DREAM

PlugX Diplomacy

Mustang Panda Campaign

Table of Contents

Executive Summary 2
Background 3
Campaign Overview 4
Technical Analysis 6
Infection Chain 7
First Stage: ZIP Container Smuggling 7
Second Stage: Dropped Files 7
Third Stage: DLL Sideloading 8
Fourth Stage: Shellcode Loader and PlugX Deployment 8
Fifth Stage: DOPLUGS Malware and Decoy 9
Distinctive Features of the DOPLUGS Variant 13
Command & Control (C&C) Infrastructure 14
Decoy Analysis 16
Lure #1: Election Information Notice | Republic of Kosovo 16
Lure #2: Regional Security Meeting Report | U.S.–Adriatic Charter 17
Lure #3: International Forum Preparatory Material | Global Buddhist Summit 18
Lure #4: Diplomatic Briefing | Cambodia–United States Engagement 19
Attribution 21
Conclusion 22
Appendix A: IOCs 23

Executive Summary

The campaign commenced with what initially appeared to be a standard diplomatic email. The subject line alluded to a policy update. The attached document was structured as an internal briefing, authored in informal language, and corresponded with actual and current geopolitical developments. For individuals engaged in government or foreign policy, it closely resembled the typical summary produced by the United States that frequently circulates after meetings, forums, or coordination calls. However, it was not authentic.

Between late December 2025 and mid-January 2026, a covert cyber espionage campaign targeted officials involved in diplomacy, elections, and international coordination across multiple regions. Rather than exploiting software vulnerabilities, the operation relied on impersonation and trust. Victims were lured into opening files that appeared to be U.S.-linked diplomatic summaries or policy documents. Opening the file alone was sufficient to trigger the compromise.

Several malicious documents explicitly mimicked American briefings, referencing U.S. partnerships, U.S.-led forums, and U.S.-associated initiatives. Others were framed as communications from foreign ministries or presidential offices that appeared to be sharing U.S. materials. The use of American attribution was deliberate. In many diplomatic settings, U.S. summaries are regarded as authoritative, timely, and dependable.

Behind these documents was a customized variant of the PlugX malware, a long-standing surveillance tool associated with Chinese state-aligned cyber operations. Once deployed, the malware enabled quiet data collection and persistent access, often without raising immediate suspicion.
The activity was identified in mid-January 2026, when one of Dream's threat-hunting AI agents flagged an anomalous archive that did not align with known benign patterns. Subsequent investigation uncovered multiple related samples sharing the same delivery mechanism, malware design, and supporting infrastructure. Together, these findings point to a coordinated intelligence operation focused on diplomatic and policy-oriented targets.

This report details the infection chain, malware functionality, and infrastructure observed in the campaign, and outlines how the activity aligns with known tradecraft associated with the China-nexus threat actor commonly referred to as Mustang Panda. At a broader level, the operation highlights a defining characteristic of modern cyber espionage. Increasingly, the most effective campaigns rely not on technical sophistication, but on credibility. In this case, the perceived legitimacy of American diplomatic materials was used as cover, turning familiar policy summaries into a vehicle for foreign intelligence collection.

Background

Mustang Panda is a longstanding threat actor with activity documented since 2012. The group has consistently relied on socially engineered delivery mechanisms and modular malware families, most notably PlugX, to gain and maintain access to victim environments. Over time, researchers have observed multiple PlugX variants that differ in loader design, encryption schemes, and supported command sets.

One such variant, commonly referred to as DOPLUGS, has been described in public reporting as a streamlined derivative of PlugX that functions primarily as a downloader rather than a full-featured remote access tool. Compared to traditional PlugX variants, DOPLUGS features a significantly reduced command set, custom RC4-based cryptographic routines, and simplified payload execution logic.

Recent reporting throughout 2024 and 2025 indicates that Mustang Panda has continued to target diplomatic and government entities, particularly in Europe and Asia, frequently leveraging shortcut-based initial access vectors, DLL search-order hijacking, and decoy documents themed around geopolitical developments. The activity documented in this report aligns with these broader trends.

Campaign Overview

All samples observed in this campaign exhibit a consistent execution chain, including PowerShell-based extraction of an embedded payload, DLL search-order hijacking, and in-memory execution of a reduced PlugX (DOPLUGS) payload. Specifically, **all four share an identically structured DOPLUGS configuration** (the sole deviation across samples is the embedded command-and-control server address).

The observed lures are themed around official meetings, elections, and international forums. In each case, the decoy content closely replicates authentic briefing notes, concept papers, or official communications associated with the referenced event.

To summarize, these are the lures identified in this campaign:

Filename	File Packing Date
Information_Note_Elections_Republic_of_Kosovo_28_December_2025.lnk	2025-12-22
Post-Meeting_Report_US-Adriatic_Charter_Partnership_Commission.lnk.zip	2025-12-23
Concept_Note_2nd_Global_Buddhist_Summit_2026.lnk	2025-12-26
Meeting_Outcome_Briefing_10_January_2026.zip	2026-01-15

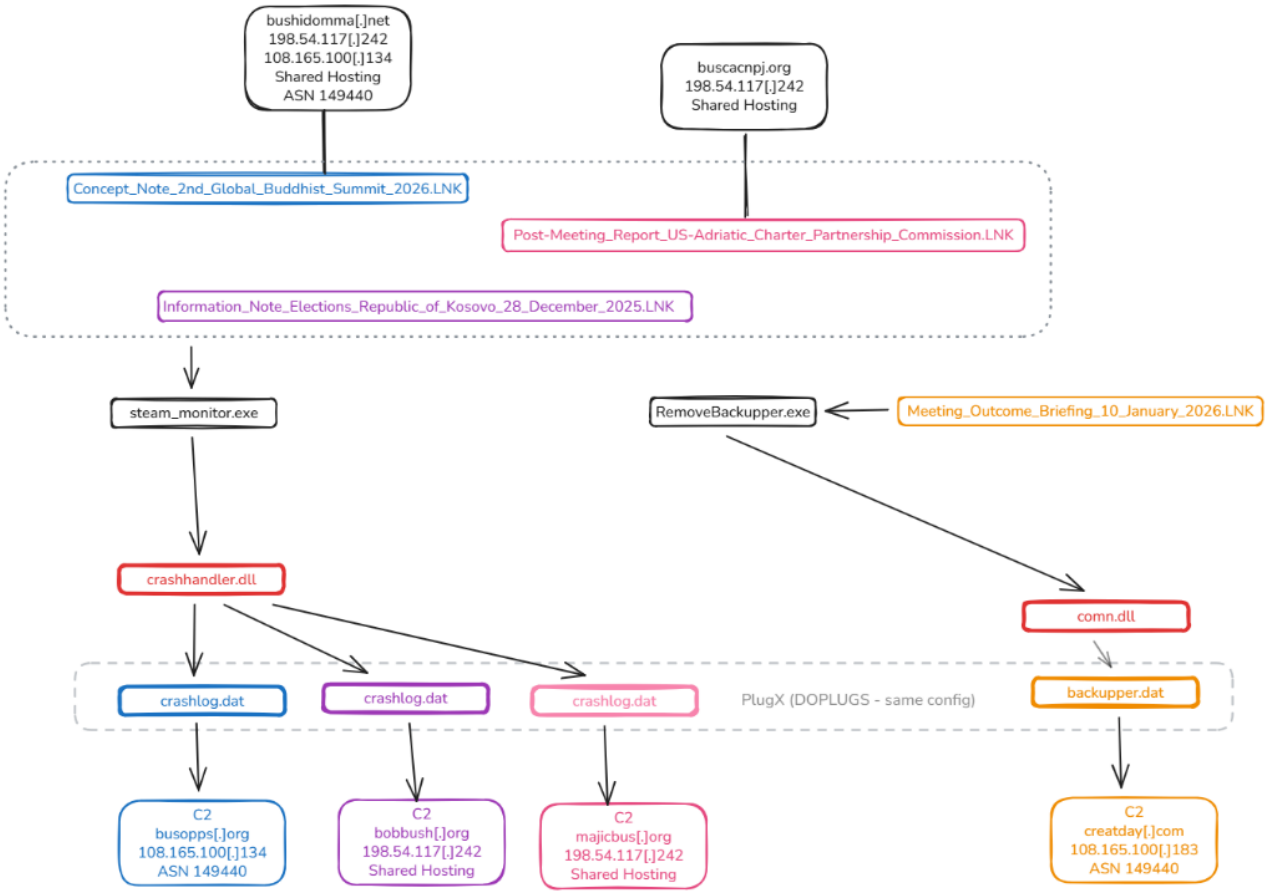


Figure 1: The campaign lures.

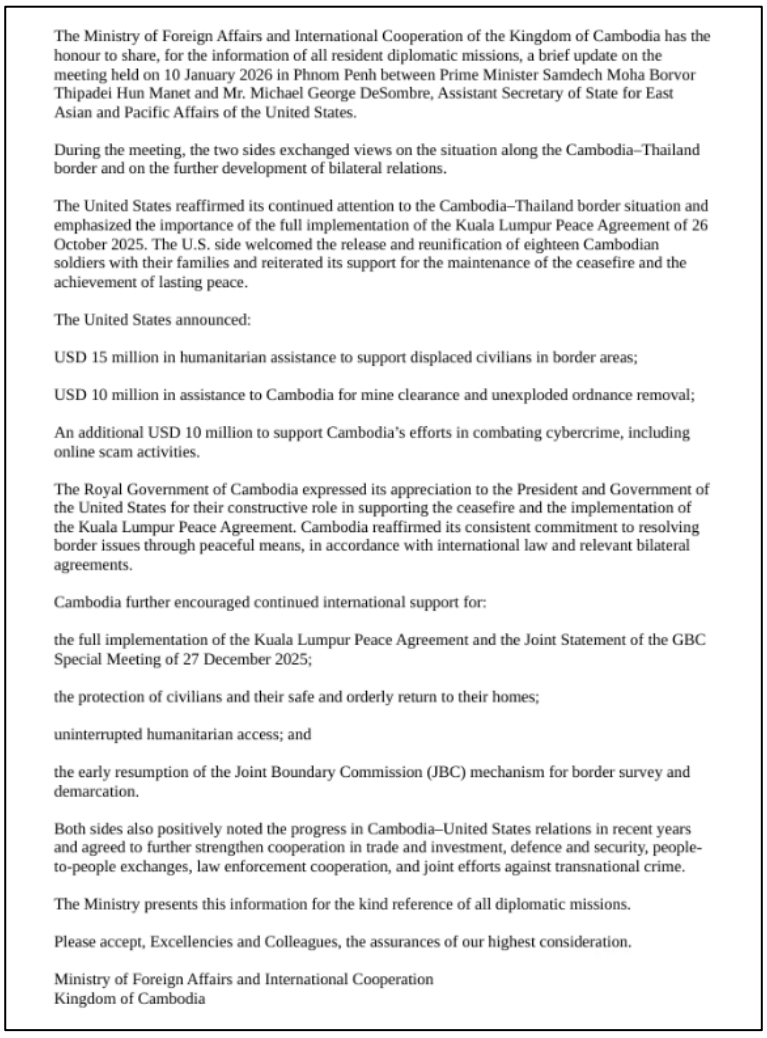
Technical Analysis

Recently, one of Dream's Threat Hunting AI agents identified a suspicious file named: *Meeting_Outcome_Briefing_10_January_2026.lnk*.

Initial analysis revealed that the file is a ZIP container packed on January 15th, 2026, and that it contains a single Windows shortcut.

Executing the shortcut triggered a PowerShell command sequence that extracted and executed an embedded payload. This initial finding prompted a deeper technical analysis of the file contents and execution flow.

Using the artifacts and behaviors observed in this initial sample as pivot points, we identified multiple related samples that shared the same delivery technique, execution logic, and underlying malware components.



The Ministry of Foreign Affairs and International Cooperation of the Kingdom of Cambodia has the honour to share, for the information of all resident diplomatic missions, a brief update on the meeting held on 10 January 2026 in Phnom Penh between Prime Minister Samdech Moha Borvor Thipadei Hun Manet and Mr. Michael George DeSombre, Assistant Secretary of State for East Asian and Pacific Affairs of the United States.

During the meeting, the two sides exchanged views on the situation along the Cambodia–Thailand border and on the further development of bilateral relations.

The United States reaffirmed its continued attention to the Cambodia–Thailand border situation and emphasized the importance of the full implementation of the Kuala Lumpur Peace Agreement of 26 October 2025. The U.S. side welcomed the release and reunification of eighteen Cambodian soldiers with their families and reiterated its support for the maintenance of the ceasefire and the achievement of lasting peace.

The United States announced:

USD 15 million in humanitarian assistance to support displaced civilians in border areas;

USD 10 million in assistance to Cambodia for mine clearance and unexploded ordnance removal;

An additional USD 10 million to support Cambodia's efforts in combating cybercrime, including online scam activities.

The Royal Government of Cambodia expressed its appreciation to the President and Government of the United States for their constructive role in supporting the ceasefire and the implementation of the Kuala Lumpur Peace Agreement. Cambodia reaffirmed its consistent commitment to resolving border issues through peaceful means, in accordance with international law and relevant bilateral agreements.

Cambodia further encouraged continued international support for:

the full implementation of the Kuala Lumpur Peace Agreement and the Joint Statement of the GBC Special Meeting of 27 December 2025;

the protection of civilians and their safe and orderly return to their homes;

uninterrupted humanitarian access; and

the early resumption of the Joint Boundary Commission (JBC) mechanism for border survey and demarcation.

Both sides also positively noted the progress in Cambodia–United States relations in recent years and agreed to further strengthen cooperation in trade and investment, defence and security, people-to-people exchanges, law enforcement cooperation, and joint efforts against transnational crime.

The Ministry presents this information for the kind reference of all diplomatic missions.

Please accept, Excellencies and Colleagues, the assurances of our highest consideration.

Ministry of Foreign Affairs and International Cooperation
Kingdom of Cambodia

Figure 2: A sample of a PDF lure originated throughout the campaign.

Infection Chain

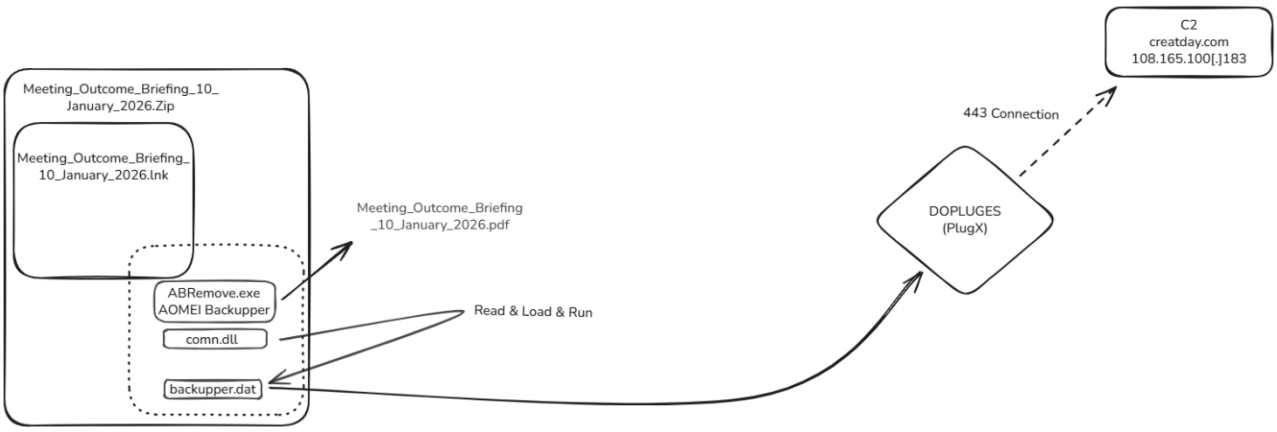


Figure 3: The infection chain diagram.

First Stage: ZIP Container Smuggling

The first stage consists of a ZIP archive containing a single LNK file that visually presents itself as a legitimate looking PDF document through icon spoofing and descriptive metadata.

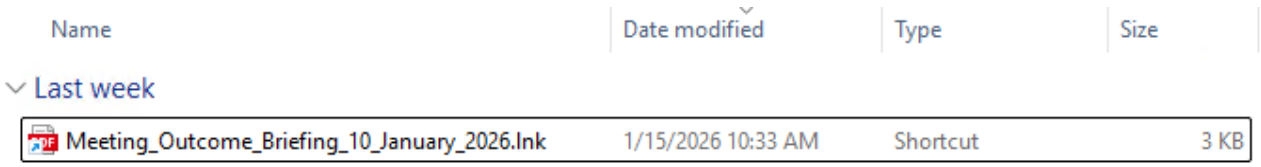


Figure 4: A sample of the ZIP archive content.

Once a user attempts to open the file, the LNK executes *powershell.exe* with a hidden window. The embedded PowerShell logic recursively searches for the ZIP archive, reads it as raw bytes, and extracts a payload beginning at a fixed byte offset. The carved data is written to disk using an obfuscated invocation of the *WriteAllBytes* method.

The extracted data is treated as a TAR archive and unpacked using the native *tar.exe* utility, demonstrating consistent use of living-off-the-land binaries (LOLBins) throughout the infection chain.

Second Stage: Dropped Files

Extraction of the embedded TAR archive results in the following files being written to the user's *%APPDATA%* directory:

- A legitimate signed executable vulnerable to DLL search-order hijacking (*RemoveBackupper.exe*)

- A malicious DLL responsible for loader execution (*comn.dll*)
- An encrypted data file containing the PlugX payload (*backupper.dat*)

Third Stage: DLL Sideloading

The executable observed in the initial sample, *RemoveBackupper.exe*, is a legitimate component of AOMEI Backupper, a backup and recovery software suite developed by the Chinese software company AOMEI Technology.

RemoveBackupper.exe is vulnerable to DLL search-order hijacking. When executed from a user-writable directory, it loads the locally present comn.dll before the legitimate library.

The malicious comn.dll exports a function expected by the host executable and uses this entry point to initiate malicious execution. This sideloading technique enables arbitrary code execution without exploiting software vulnerabilities and is a recurring component in Mustang Panda operations.

The *comn.dll* loads the *backupper.dat* using *VirtualAlloc,* changes the memory region to executable, and executes the payload.

Fourth Stage: Shellcode Loader and PlugX Deployment

backupper.dat contains shellcode at the start of the file, which redirects execution to a decryption routine.

```
03528C0E  84C0            TEST AL,AL
03528C10  F8              CLC
03528C11  49              DEC ECX
03528C12  41              INC ECX
03528C13  5A              POP EDX
03528C14  52              PUSH EDX
03528C15  04 00           ADD AL,0
03528C17  58              POP EAX
03528C18  50              PUSH EAX
03528C19  5A              POP EDX
03528C1A  B9 008C0800     MOV ECX,88C00
03528C1F  8032 E5         XOR BYTE PTR DS:[EDX],0E5
03528C22  83C2 01         ADD EDX,1
03528C25  83E9 01         SUB ECX,1
03528C28  83F9 00         CMP ECX,0
03528C2B ^75 F2           JNZ SHORT 03528C1F
03528C2D  50              PUSH EAX
03528C2E  FC              CLD
03528C2F  F5              CMC
03528C30  87DB            XCHG EBX,EBX
03528C32  F8              CLC
03528C33  58              POP EAX
03528C34  FFD0            CALL EAX
03528C36  F9              STC
03528C37  90              NOP
```

Figure 5: A decryption routine within backupper.dat.

The rest of the file is then decrypted with a hardcoded XOR key (0xE5 in this case) and then executed from memory; this key is different for each variant.

The XOR-decrypted content is a valid PE header (4D5A – MZ), but also a valid set of x86 Assembly instructions, leading to a function that loads the final PlugX payload.

```
034A000E  4D              DEC EBP
034A000F  5A              POP EDX
034A0010  E8 00000000     CALL 034A0015
034A0015  5B              POP EBX
034A0016  52              PUSH EDX
034A0017  45              INC EBP
034A0018  55              PUSH EBP
034A0019  8BEC            MOV EBP,ESP
034A001B  81C3 290B0000   ADD EBX,0B29
034A0021  FFD3            CALL EBX
034A0023  C9              LEAVE
034A0024  C3              RETN
```

Figure 6: a call to the next phase of the final payload loading.

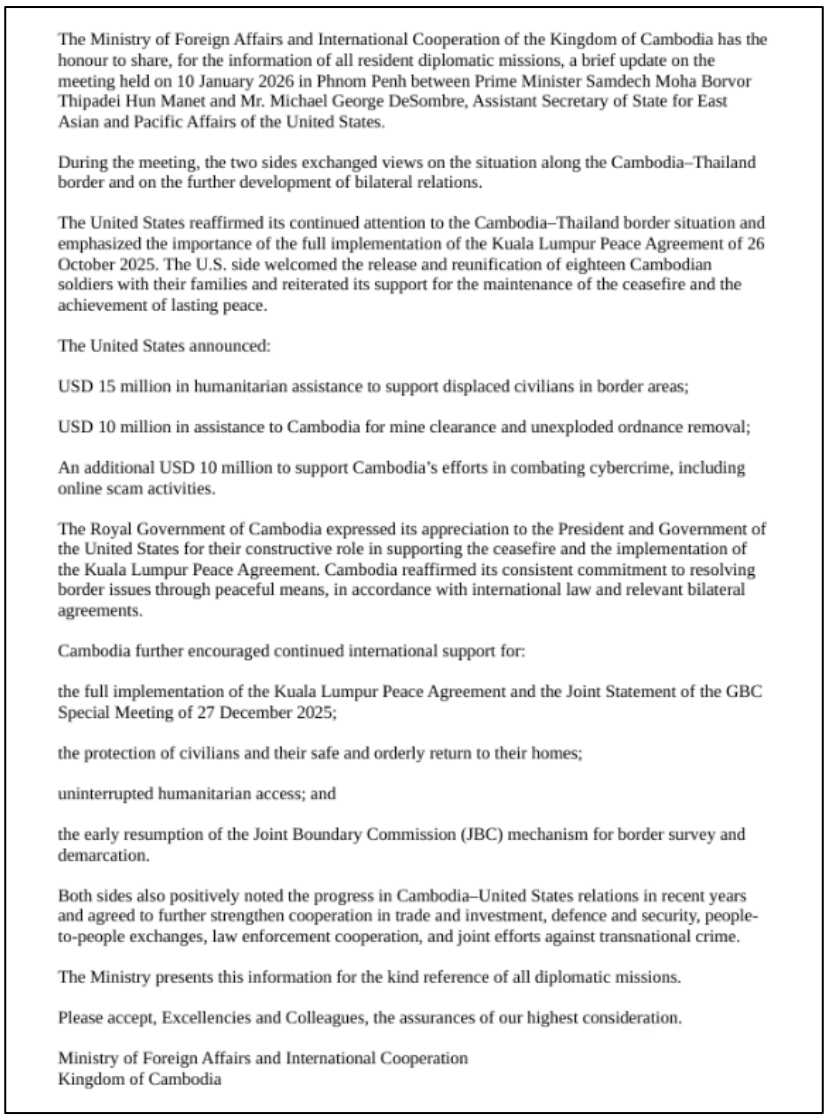
The loader function is highly obfuscated, using the Control Flow Flattening (CFF) technique, which increases the complexity for the reverse-engineering process by eliminating syntactic cues and forcing semantic recovery through opaque, non-linear state transitions.

The loader function performs the following sequence of operations:

- Resolve: Finds kernel32/ntdll via the PEB and resolves APIs (like *VirtualAlloc* , *LoadLibraryA*) using ROR13 hashing.
- Map: Allocates memory based on *SizeOfImage* and copies PE sections to their intended virtual addresses.
- Fix: Adjusts absolute addresses via Base Relocations and resolves the Import Address Table (IAT).
- Execute: Jumps to the DLL Entry Point.

Fifth Stage: DOPLUGS Malware and Decoy

Following execution, the legitimate executable displays a decoy PDF document to the user, which is written to a temporary directory, and runs the final payload which in our case is PlugX, specifically – DOPLUGS variant.



The Ministry of Foreign Affairs and International Cooperation of the Kingdom of Cambodia has the honour to share, for the information of all resident diplomatic missions, a brief update on the meeting held on 10 January 2026 in Phnom Penh between Prime Minister Samdech Moha Borvor Thipadei Hun Manet and Mr. Michael George DeSombre, Assistant Secretary of State for East Asian and Pacific Affairs of the United States.

During the meeting, the two sides exchanged views on the situation along the Cambodia–Thailand border and on the further development of bilateral relations.

The United States reaffirmed its continued attention to the Cambodia–Thailand border situation and emphasized the importance of the full implementation of the Kuala Lumpur Peace Agreement of 26 October 2025. The U.S. side welcomed the release and reunification of eighteen Cambodian soldiers with their families and reiterated its support for the maintenance of the ceasefire and the achievement of lasting peace.

The United States announced:

USD 15 million in humanitarian assistance to support displaced civilians in border areas;

USD 10 million in assistance to Cambodia for mine clearance and unexploded ordnance removal;

An additional USD 10 million to support Cambodia's efforts in combating cybercrime, including online scam activities.

The Royal Government of Cambodia expressed its appreciation to the President and Government of the United States for their constructive role in supporting the ceasefire and the implementation of the Kuala Lumpur Peace Agreement. Cambodia reaffirmed its consistent commitment to resolving border issues through peaceful means, in accordance with international law and relevant bilateral agreements.

Cambodia further encouraged continued international support for:

the full implementation of the Kuala Lumpur Peace Agreement and the Joint Statement of the GBC Special Meeting of 27 December 2025;

the protection of civilians and their safe and orderly return to their homes;

uninterrupted humanitarian access; and

the early resumption of the Joint Boundary Commission (JBC) mechanism for border survey and demarcation.

Both sides also positively noted the progress in Cambodia–United States relations in recent years and agreed to further strengthen cooperation in trade and investment, defence and security, people-to-people exchanges, law enforcement cooperation, and joint efforts against transnational crime.

The Ministry presents this information for the kind reference of all diplomatic missions.

Please accept, Excellencies and Colleagues, the assurances of our highest consideration.

Ministry of Foreign Affairs and International Cooperation
Kingdom of Cambodia

Figure 7: The dropped Meeting_Outcome_Briefing_10_January_2026.pdf

This malware (DOPLUGS) has no hardcoded API function names; instead, the names are stored as encrypted stack strings and decrypted every time they are called using different arithmetic operations:

```
qmemcpy(v80, "WnhMpojZtpmxTr|u|r", 18);
*(_DWORD *)v83 = &v80[19];
v26 = -1578947332;
v27 = &v80[18];
while ( v26 != 988261337 )
{
  *v27++ = 0;
  v26 = -1578947332;
  if ( v27 == *(_BYTE **)v83 )
    v26 = 988261337;
}
v47 = 0;

v48 = -2065342327;
while ( v48 != 956393596 )
{
  if ( v48 == -1228600702 )
  {
    v49 = (~v80[*(_DWORD *)v83] & 0x34 | v80[*(_DWORD *)v83] & 0xCB)
        ^ ((-12 - v83[0]) & 0x34 | (v83[0] + 11) & 0xCB);
    v80[*(_DWORD *)v83] = ~v49 & 0xB | v49 & 0xF4;
    v47 = *(_DWORD *)v83 + 1;
    goto LABEL_140;
  }
  *(_DWORD *)v83 = v47;
  v48 = 956393596;
  if ( v47 < 0x12 )
    v48 = -1228600702;
}
```

Figure 8: The hardcoded stack string with its decryption routine.

There are over 50 encrypted stack strings in this DOPLUGS sample; each is encrypted with different keys and arithmetic operations.

Example of some of the decrypted strings:

Encrypted	Decrypted
WnhMpojVhzp	WinHttpOpen
WnhMpojZwqpx	WinHttpConnect
WnhMpojZtpmxTr|u	WinHttpCloseHandle
WnhMpojK}~zY}gs	WinHttpQueryData
WnhMpojHmzldTvsu	WinHttpQueryHeaders
WnhMpojK}|{tjv@t	WinHttpReceiveResponse
WnhMpojJ}qzOybgt	WinHttpSendRequest

This DOPLUG variant shares similarities with previously seen variants, such as the usage of a custom RC4 encryption/decryption routine and the same C2 commands.

```
v6 = v12 + 1;                           // RC4 PRGA step
v8 = (unsigned __int8)(v12 + 1);        // used as S-box index
v9 = *(_BYTE *)(a1 + v8);
result = v9 + v11;
v10 = (unsigned __int8)(v9 + v11);      // second index for swap
*(_BYTE *)(a1 + v8) = *(_BYTE *)(a1 + v10);
*(_BYTE *)(a1 + v10) = v9;
*(_BYTE *)(a3 + v13) = *(_BYTE *)(a2 + v13) & ~*(_BYTE *)(a1 + (unsigned __int8)(*(_BYTE *)(a1 + v8) + v9))
                     | *(_BYTE *)(a1 + (unsigned __int8)(*(_BYTE *)(a1 + v8) + v9)) & ~*(_BYTE *)(a2 + v13);//
                                        // output[k] = input[k] XOR keystream
                                        // keystream byte is pulled from S[ (S[i] + old_S[i]) & 0xFF ]
                                        // XOR is implemented as (x & ~y) | (y & ~x)
v4 = v13 + 1;
```

Figure 9: The custom RC4 encryption and decryption routine.

These are the C2 commands present in all samples we've analyzed in this campaign.

Command ID	Functionality
0x7002	Shell Execution
0x1007	Beacon/Timeout Config
0x3004	Download & Execute Payload
0x1005	Self-Cleanup / Uninstall

The C2 configuration is stored within the executable and has the following structure:

Offset	Size	Description
0x00	4 bytes	RC4 Key Length
0x04	N bytes	RC4 Key in ASCII
0x04+N	padding	Padding to 16 bytes alignment
0x10	~ 2200 bytes	RC4 Encrypted Config

Once decrypted, the C2 configuration has another layer of encryption, XOR with a sliding key (starting with 0x15 or 0x16), and has the following structure:

Offset	Size	Description

0x00	8 bytes	C2 Address Length
0x08	2 bytes	Flag
0x0A	2 bytes	Port
0x0C	6 bytes	Padding
0x12	22-24 bytes	XOR Encrypted C2 Address

Distinctive Features of the DOPLUGS Variant

We believe this campaign specifically utilizes the DOPLUGS variant of PlugX. This assessment is based on the unique characteristics of DOPLUGS that are present in the samples analyzed.

1. Extreme Obfuscation

The sample uses more than 50 encrypted stack strings, with every API call protected by custom XOR encryption. It employs multiple position-dependent encryption keys, using different algorithms for different strings, which significantly increases the time and effort required for reverse engineering because each string may need a new algorithm to be analyzed. In addition, it avoids static imports almost entirely, relying only on `kernel32.dll` with all other APIs resolved dynamically at runtime.

2. Control Flow Flattening (CFF)

State machine obfuscation: Functions use magic constants and goto jumps, which increases the complexity for the reverse-engineering process by eliminating syntactic cues and forcing semantic recovery through opaque, non-linear state transitions.

3. Multi-Layer C2 Config Encryption

The C2 configuration encryption is multilayer, combining RC4 and XOR.

4. Reduced C2 Command Set

Standard PlugX variants operate as comprehensive RATs with complete backdoor functionality delivered through a modular plugin architecture. In contrast, DOPLUGS functions exclusively as a downloader.

DOPLUGS implements only four backdoor commands, a reduction from the extensive command sets found in "traditional" PlugX variants.

Command & Control (C&C) Infrastructure

Network indicators extracted from the analyzed samples reveal a compact and reused command-and-control infrastructure spanning a small number of autonomous systems. Across the campaign, multiple domains resolve to the same IP addresses or exhibit coordinated hosting transitions, indicating deliberate infrastructure management rather than opportunistic use.

The following C&C domains were observed across multiple samples:

2. **creatday[.]com** → 108.165.100[.]183 (ASN 149440)
3. **busopps[.]org** → 108.165.100[.]134 (ASN 149440)
4. **majicbus[.]org** → 198.54.117[.]242 (shared hosting)
5. **bobbush[.]org** → 198.54.117[.]242 (shared hosting)
6. **buscacnpj[.]org** → 198.54.117[.]242 (shared hosting)
7. **bushidomma[.]net** → 108.165.100[.]134 → 198.54.117[.]242

Several domains initially resolved to infrastructure within **ASN 149440** before transitioning behind **Cloudflare**, and in some cases later moving to shared hosting at **198.54.117[.]242**. This migration pattern is observed for **creatday[.]com** and **busopps[.]org**, both of which progressed from direct hosting to Cloudflare-fronted infrastructure.

The domain **bushidomma[.]net** demonstrates the most complete lifecycle, resolving first to ASN 149440, later migrating to shared hosting, and subsequently transitioning behind Cloudflare. In contrast, **majicbus[.]org**, **bobbush[.]org**, and **buscacnpj[.]org** were observed exclusively on shared hosting, suggesting late-stage infrastructure reuse rather than initial deployment nodes.

Collectively, these patterns indicate a controlled, centrally managed C&C setup, with infrastructure recycled and repositioned over time rather than abandoned. This approach is consistent with operational security practices observed in prior PlugX campaigns, where Cloudflare is used to obfuscate backend hosting and shared infrastructure is repurposed across multiple payloads or delivery waves.

Additional infrastructure characteristics further reinforce this assessment:

- All identified domains were registered through the same registrar (**Namecheap**, registrar ID 1068).
- Domain registration dates are tightly clustered around **23 December 2025**.

- Multiple domains became operational within a narrow time window, suggesting coordinated provisioning rather than ad hoc acquisition.

To conclude, the reuse of domains, overlapping hosting providers, synchronized registration timing, and repeated migration patterns strongly suggest centralized infrastructure planning in support of this campaign, rather than unrelated or opportunistic activity.

Decoy Analysis

Lure #1: Election Information Notice | Republic of Kosovo

(Information_Note_Elections_Republic_of_Kosovo_28_December_2025.lnk)

The earliest observed lure is presented as an official election-related information notice purportedly originating from the Office of the President of Kosovo, announcing the parliamentary elections that were held on 28 December 2025.

The decoy document mirrors the language and presentation typically used in official government communications and would likely be relevant to recipients engaged in European diplomatic, political, or election-monitoring activities.

This is reminiscent of previous public reporting on Mustang Panda activity targeting European diplomatic and governmental entities using diplomacy-themed lures.

REPUBLIKA E KOSOVËS - PRESIDENTJA
REPUBLIC OF KOSOVO - THE PRESIDENT
REPUBLIKA KOSOVO - PREDSEDNICA

20 November 2025
Prishtina, Republic of Kosovo

H.E. Roberta Metsola
President of the European Parliament

H.E. Kaja Kallas
High Representative of the European Union for Foreign Affairs and Security Policy
Vice-President of the European Commission

Your Excellencies,

As part of my constitutional mandate as President of the Republic of Kosovo, I have officially set and announced the 28th of December 2025, as the date for the forthcoming early parliamentary elections in the Republic of Kosovo. In line with the recommendations of the EU electoral experts, I have therefore decided to grant the Central Election Commission the longest possible deadline for the upcoming elections provided for in the Constitution of the Republic of Kosovo, rather than the shortest.

In line with a well-established practice, I officially invite the European Union to deploy an independent and impartial Electoral Expert Mission, to monitor and assess the upcoming elections. We kindly ask that the Mission's mandate place particular focus on gender equality and the participation of women throughout all stages of the electoral process, as well as monitor the rights and accessibility of persons with disabilities to the polling stations.

I am confident that the support and active engagement of the EU institutions will significantly strengthen the confidence of our citizens and international partners in this electoral process. This is particularly important for safeguarding the credibility, integrity, and transparency of the elections. Considering this, I hope that the European Union will mandate an Electoral Expert Mission for the upcoming elections in the Republic of Kosovo.

Please accept, Your Excellencies, the assurances of my highest consideration.

Sincerely,

Vjosa Osmani Sadriu
President of the Republic of Kosovo

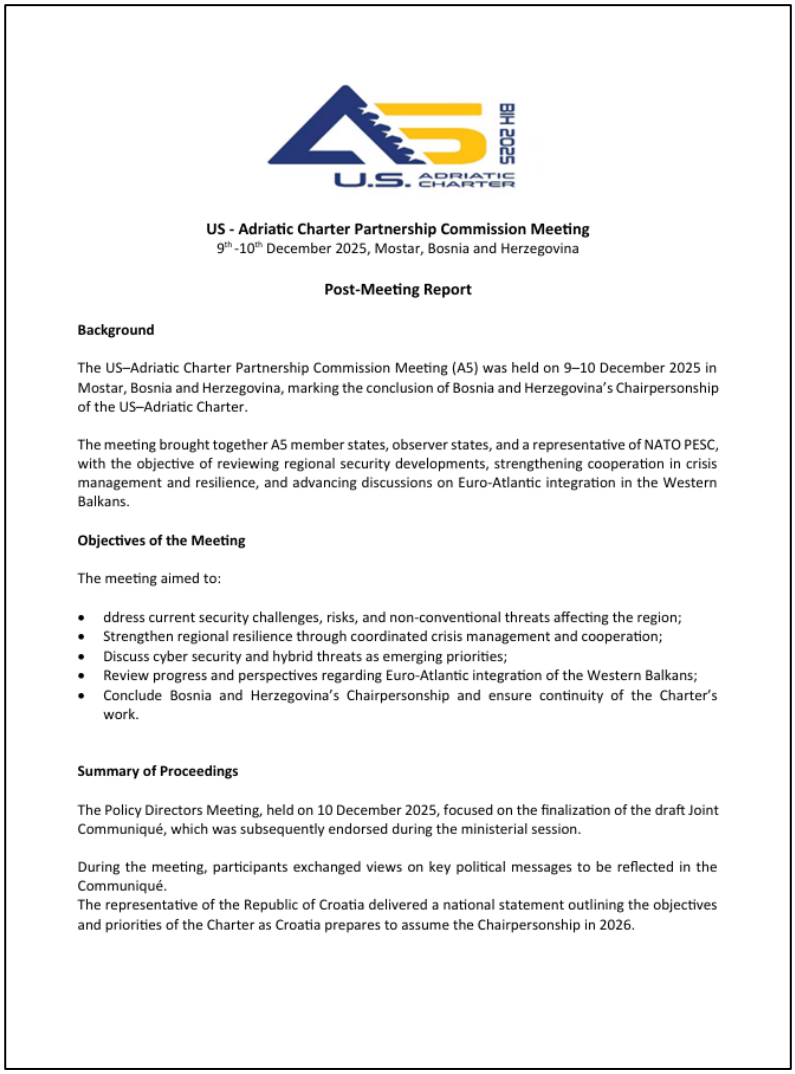
Figure 10: The dropped Information_Note_Elections_Republic_of_Kosovo_28_December_2025.pdf

Lure #2: Regional Security Meeting Report | U.S.–Adriatic Charter

(Post-Meeting_Report_US-Adriatic_Charter_Partnership_Commission.lnk.zip)

This subsequent lure references a post-meeting report associated with the U.S.–Adriatic Charter Partnership Commission, masquerading as material connected to a meeting hosted under the auspices of the Bosnian Ministry of Foreign Affairs.

The referenced engagement aligns with publicly documented meetings held in December 2025 involving representatives from the United States and Western Balkan states.



US - Adriatic Charter Partnership Commission Meeting
9th-10th December 2025, Mostar, Bosnia and Herzegovina

Post-Meeting Report

Background

The US–Adriatic Charter Partnership Commission Meeting (A5) was held on 9–10 December 2025 in Mostar, Bosnia and Herzegovina, marking the conclusion of Bosnia and Herzegovina's Chairpersonship of the US–Adriatic Charter.

The meeting brought together A5 member states, observer states, and a representative of NATO PESC, with the objective of reviewing regional security developments, strengthening cooperation in crisis management and resilience, and advancing discussions on Euro-Atlantic integration in the Western Balkans.

Objectives of the Meeting

The meeting aimed to:

- ddress current security challenges, risks, and non-conventional threats affecting the region;
- Strengthen regional resilience through coordinated crisis management and cooperation;
- Discuss cyber security and hybrid threats as emerging priorities;
- Review progress and perspectives regarding Euro-Atlantic integration of the Western Balkans;
- Conclude Bosnia and Herzegovina's Chairpersonship and ensure continuity of the Charter's work.

Summary of Proceedings

The Policy Directors Meeting, held on 10 December 2025, focused on the finalization of the draft Joint Communiqué, which was subsequently endorsed during the ministerial session.

During the meeting, participants exchanged views on key political messages to be reflected in the Communiqué.
The representative of the Republic of Croatia delivered a national statement outlining the objectives and priorities of the Charter as Croatia prepares to assume the Chairpersonship in 2026.

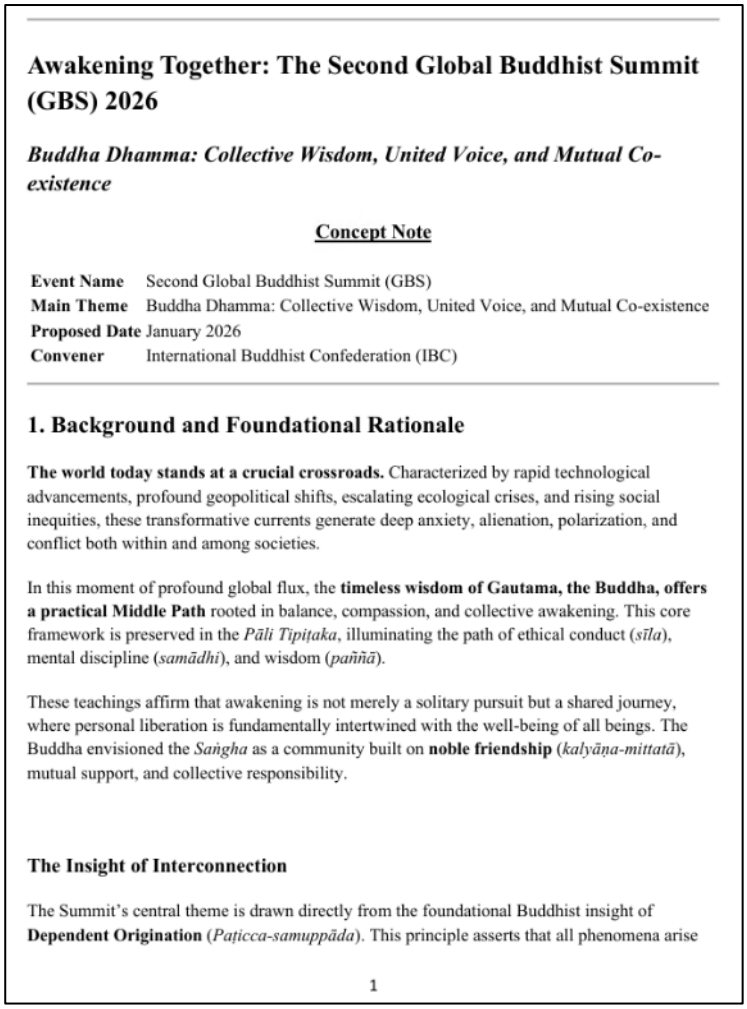
Figure 11: A sample of the Post-Meeting_Report_US-Adriatic_Charter_Partnership_Commission.pdf

Lure #3: International Forum Preparatory Material | Global Buddhist Summit

(Concept_Note_2nd_Global_Buddhist_Summit_2026.lnk)

The next lure is styled as preparatory material associated with the 2nd Global Buddhist Summit, an international forum scheduled to take place in New Delhi on 24–25 January 2026. At the time this report is being written, the event has not yet occurred.

The decoy content is framed as a concept note intended for participants or stakeholders involved in the summit, an event at which Buddhist scholars and religious leaders are expected to be in attendance. Given the expected participation of prominent Buddhist leaders and scholars, including figures of geopolitical sensitivity, this lure would plausibly appeal to recipients involved in religious, cultural, or policy-related engagement with South Asia.



Awakening Together: The Second Global Buddhist Summit (GBS) 2026

Buddha Dhamma: Collective Wisdom, United Voice, and Mutual Co-existence

Concept Note

Event Name	Second Global Buddhist Summit (GBS)
Main Theme	Buddha Dhamma: Collective Wisdom, United Voice, and Mutual Co-existence
Proposed Date	January 2026
Convener	International Buddhist Confederation (IBC)

1. Background and Foundational Rationale

The world today stands at a crucial crossroads. Characterized by rapid technological advancements, profound geopolitical shifts, escalating ecological crises, and rising social inequities, these transformative currents generate deep anxiety, alienation, polarization, and conflict both within and among societies.

In this moment of profound global flux, the **timeless wisdom of Gautama, the Buddha, offers a practical Middle Path** rooted in balance, compassion, and collective awakening. This core framework is preserved in the *Pāli Tipiṭaka*, illuminating the path of ethical conduct (*sīla*), mental discipline (*samādhi*), and wisdom (*paññā*).

These teachings affirm that awakening is not merely a solitary pursuit but a shared journey, where personal liberation is fundamentally intertwined with the well-being of all beings. The Buddha envisioned the *Saṅgha* as a community built on **noble friendship** (*kalyāṇa-mittatā*), mutual support, and collective responsibility.

The Insight of Interconnection

The Summit's central theme is drawn directly from the foundational Buddhist insight of **Dependent Origination** (*Paṭicca-samuppāda*). This principle asserts that all phenomena arise

1

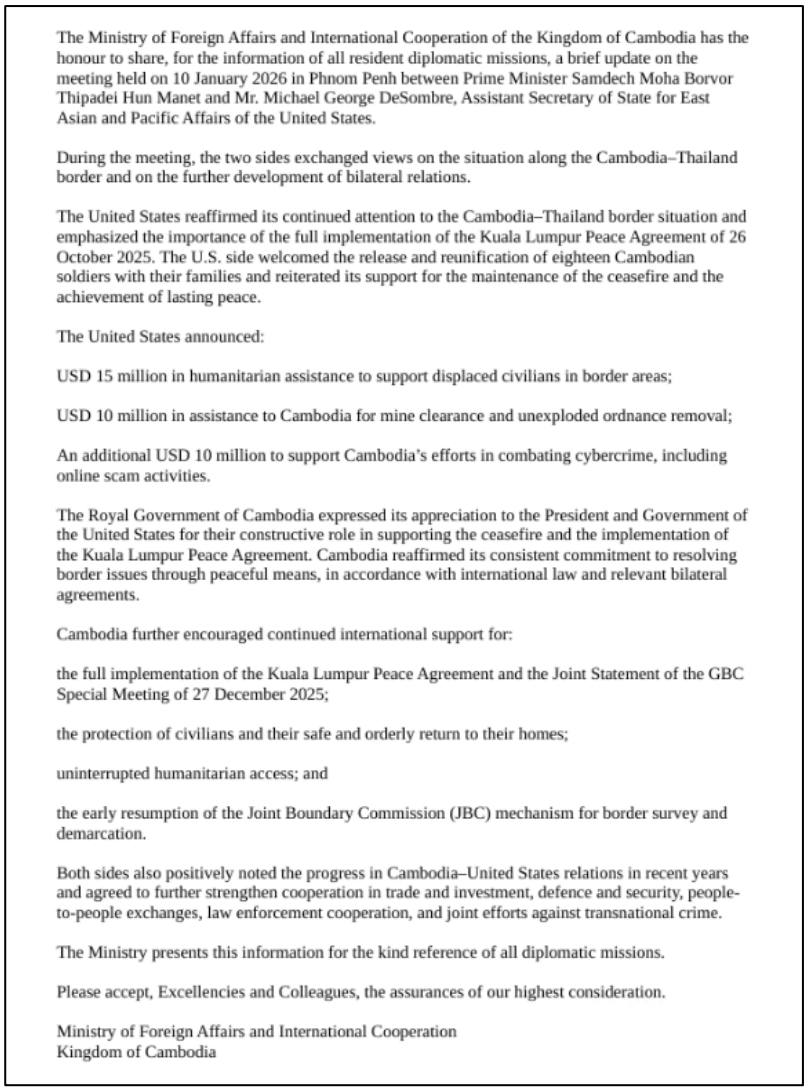
Figure 12: Concept_Note_2nd_Global_Buddhist_Summit_2026.pdf

Lure #4: Diplomatic Briefing | Cambodia–United States Engagement

(Meeting_Outcome_Briefing_10_January_2026.lnk)

The most recent lure masquerades as a post-meeting diplomatic briefing associated with an engagement involving Cambodia and the United States. The decoy content closely resembles material issued by the Cambodian Ministry of Foreign Affairs and International Cooperation, both in structure and tone.

The referenced meeting took place on 10 January 2026 and relates to diplomatic discussions in the context of the ongoing Cambodia–Thailand border dispute. The content of this document suggests it was designed to appear relevant to diplomats and policy professionals focused on Southeast Asia.



The Ministry of Foreign Affairs and International Cooperation of the Kingdom of Cambodia has the honour to share, for the information of all resident diplomatic missions, a brief update on the meeting held on 10 January 2026 in Phnom Penh between Prime Minister Samdech Moha Borvor Thipadei Hun Manet and Mr. Michael George DeSombre, Assistant Secretary of State for East Asian and Pacific Affairs of the United States.

During the meeting, the two sides exchanged views on the situation along the Cambodia–Thailand border and on the further development of bilateral relations.

The United States reaffirmed its continued attention to the Cambodia–Thailand border situation and emphasized the importance of the full implementation of the Kuala Lumpur Peace Agreement of 26 October 2025. The U.S. side welcomed the release and reunification of eighteen Cambodian soldiers with their families and reiterated its support for the maintenance of the ceasefire and the achievement of lasting peace.

The United States announced:

USD 15 million in humanitarian assistance to support displaced civilians in border areas;

USD 10 million in assistance to Cambodia for mine clearance and unexploded ordnance removal;

An additional USD 10 million to support Cambodia's efforts in combating cybercrime, including online scam activities.

The Royal Government of Cambodia expressed its appreciation to the President and Government of the United States for their constructive role in supporting the ceasefire and the implementation of the Kuala Lumpur Peace Agreement. Cambodia reaffirmed its consistent commitment to resolving border issues through peaceful means, in accordance with international law and relevant bilateral agreements.

Cambodia further encouraged continued international support for:

the full implementation of the Kuala Lumpur Peace Agreement and the Joint Statement of the GBC Special Meeting of 27 December 2025;

the protection of civilians and their safe and orderly return to their homes;

uninterrupted humanitarian access; and

the early resumption of the Joint Boundary Commission (JBC) mechanism for border survey and demarcation.

Both sides also positively noted the progress in Cambodia–United States relations in recent years and agreed to further strengthen cooperation in trade and investment, defence and security, people-to-people exchanges, law enforcement cooperation, and joint efforts against transnational crime.

The Ministry presents this information for the kind reference of all diplomatic missions.

Please accept, Excellencies and Colleagues, the assurances of our highest consideration.

Ministry of Foreign Affairs and International Cooperation
Kingdom of Cambodia

Figure 13: Meeting_Outcome_Briefing_10_January_2026.pdf

In summary, taken together, the recurring use of diplomatic, governmental, and international policy themes suggests that the lures are designed to be relevant to individuals who routinely engage with such material as part of their professional responsibilities. Given the nature of the documents and their framing, it is reasonable to conclude that the campaign is primarily aimed at recipients operating in government, diplomatic, policy, or related institutional environments. This assessment is derived solely from the observable content and context of the lures, rather than from any inference of the attacker's intent.

Attribution

The combination of delivery techniques, loader architecture, malware characteristics, lure theming, and overlapping infrastructure observed in this campaign aligns with publicly documented activity attributed to Mustang Panda.

In addition to these factors, this attribution is further supported by the identification of the PlugX payload deployed as the DOPLUGS variant. Public reporting has consistently demonstrated a strong correlation between DOPLUGS and Mustang Panda operations, with this variant being overwhelmingly associated with activities linked to Mustang Panda. The observed reduced command set, custom encryption routines, and downloader-focused functionality closely aligned with characteristics documented in previous analyses of Mustang Panda's DOPLUGS campaigns.

Conclusion

Overall, the activity documented in this report demonstrates that Mustang Panda continues to operate using its characteristic tradecraft, combining timely geopolitical lures with well-established delivery mechanisms and tooling. The repeated use of the same infection chain-shortcut-based initial access, PowerShell-mediated payload extraction, and signed-binary DLL side-loading reflects a continued reliance on proven techniques to support consistent execution across multiple themed campaigns.

The correlation between actual diplomatic events and the timing of detected lures suggests that analogous campaigns are likely to persist as geopolitical developments unfold. Entities operating in diplomatic, governmental, and policy-oriented sectors should consequently regard malicious LNK distribution methods and DLL search-order hijacking via legitimate executables as persistent, high-priority threats rather than isolated or fleeting tactics. Ongoing surveillance for shortcut exploitation, loader reuse, and low-noise PlugX variants such as DOPLUGS remain essential for prompt detection and response.

Appendix A: IOCs

#	Lure	Identifier	Filename
1.	#4	50746ddd81a5dbc5cec793209ab552125fff9c7184aa5bcfe22d6c3b267f67f1	Meeting_Outcome_Briefing_10_January_2026.zip
2.	#4	d0576b39bb6c05ea0a24d3a3d5d7cb234454fefc65860f21a97757582adc7650	Meeting_Outcome_Briefing_10_January_2026.lnk
3.	#4	84d6a8b47edadf5725d9937d8928a90d190e0c98b5b4d1a4c58e97cddcd36768	comm.dll
4.	#4	f988d58e4a32b908ff7a557d740c6860c59807832c7626774330dcaed65ead14	backupper.dat
5.	#4	creatday[.]com	
6.	#4	108.165.100[.]183	
7.	#3	784a914bd1878ad68a6cf3f693da5ddcc2f04b794204333098ad749b7e372fd4	Concept_Note_2nd_Global_Buddhist_Summit_2026.lnk
8.	#3	busopps[.]org	
9.	#3	108.165.100[.]134	
10.	#3	bushidomma[.]net	Delivery Infrastructure
11.	#3	2c3708a103b257fa75fcb34948c817fd564d4479f1e267b33c5b08f0d4c7634f	crashhandler.dll
12.	#3	e9d8f28fd0aef3bc3f5b28a41b3f342165b371db9aefd7d03f2aba4292009d3e	crashlog.dat
13.	#1	42c3b9cad6c8383699eba4f82d51908c0d61e9ea454bc40447cf20475ce20ff0	Information_Note_Elections_Republic_of_Kosovo_28_December_2025.lnk
14.	#1	bobbush[.]org	
15.	#1	198.54.117[.]242	
16.	#1	e9033abcbf9512e7c56243ce79f447473b9ae09cfcd3c70add3a6e302679f64e	crashhandler.dll
17.	#1	eb10443a2f0b9a25d01a84426a6a8532b0e7c9157abda55b94c98a1fd2d45562	crashlog.dat
18.	#2	b1606ca49aa15eadb039f33d438697973b203693d0003e467e1f33b36d10a530	Post-Meeting_Report_US-Adriatic_Charter_Partnership_Commission.lnk

19.	#2	majicbus[.]org	
20.	#2	198.54.117[.]242	
21.	#2	843b22df66f87a587be77145da163f9615fe8164a5ea17f9e33562ff43894fbf	crashhandler.dll
22.	#2	6788365386ccd34d1db681c61ef07ef4d2faea5672571b77a76dc48f327afaa9	crashlog.dat
23.	#2	buscacnpj[.]org	Delivery Infrastructure