Double-Tap Campaign: Russia-nexus APT possibly related to APT28 conducts cyber espionage on Central Asia and Kazakhstan diplomatic relations

⋮ 1/13/2025

Introduction

On Wednesday, 27 November 2024, Russian President Putin was on a 2-day state visit in Kazakhstan to discuss with local representatives the implementation of energy projects and to counter Chinese and Western influence. Putin said he was visiting his “true ally”, yet Sekoia investigated an ongoing cyber espionage campaign using legitimate Office documents assessed to originate from the Ministry of Foreign Affairs of the Republic of Kazakhstan, that were further weaponized and likely used to collect strategic intelligence in Central Asia, including Kazakhstan and its diplomatic and economic relations with Asian and Western countries. We assess it is possible that this campaign was conducted by a Russia-nexus intrusion set, UAC-0063, sharing overlaps with APT28.

I. UAC-0063 background

UAC-0063 is an intrusion set active since at least 2021 that was first exposed by **CERT-UA** in April 2023 for conducting a cyber espionage campaign targeting several countries such as Ukraine, Israel and India, including multiple central Asian countries (Kazakhstan, Kyrgyzstan and Tajikistan). CERT-UA analysts identified spearphishing lure Word documents with malicious macros sent by a compromised official mailbox of the Embassy of Tajikistan in Ukraine.

UAC-0063 targeting suggests a focus on **intelligence collection** in sectors such as government, including diplomacy, NGOs, academia, energy, and defence, with a geographic focus on **Ukraine**, **Central Asia**, and **Eastern Europe**.

Later, in July 2024, CERT-UA published another report exposing UAC-0063 activities targeting Ukrainian scientific research institutions with new malware (dubbed HATVIBE and CHERRYSPY). The report associates the intrusion set UAC-0063 with **APT28 with medium confidence**.

As a reminder, APT28 is a well-studied intrusion set active since at least 2004, attributed by multiple governments and cybersecurity experts to **Russia’s General Staff Main Intelligence Directorate** (**GRU**) Military Unit 26165. This intrusion set is especially known for its hybrid operations on the sidelines of armed conflicts (Ukraine 2015, 2017, 2022), election manipulation (2016 US and 2017 French Presidential Election), and diplomatic crises related to Russia (TV5 Monde 2015).
Our colleagues from **Recorded Future** are tracking UAC-0063 under the alias TAG-110, assessing that its activities overlap with APT28’s strategic interests, yet without confirming the CERT-UA’s medium confidence association with APT28 based on technical elements.

II. Initial findings

In late July 2024, our attention was drawn to an article published by CERT-UA detailing the activities of the UAC-0063 intrusion set, leveraging HATVIBE and CHERRYSPY malware to conduct cyber espionage operations against government institutions. We conducted further research to identify a pattern for future Command and Control (C2) servers and to further track it through our Sekoia C2 Trackers project. We also created a set of YARA rules to detect the infection chain and the deployed malware.

On 16 October 2024, one of our YARA rules that detects malicious macros caught a malicious file uploaded to VirusTotal. The Office document titled *Rev5_Joint Declaration C5+GER_clean version.doc* seemed to be a draft version of a diplomatic join statement containing a malicious macro that prompts the user for permission for execution and lead to the compromise of the host.

Within a function in the macro, we observed the removal of the document's protection using a highly unique password. By pivoting on this password, we were able to identify **10 additional Word documents that had not yet been publicly disclosed**.

Our investigation led us to find 18 DOCX files with embedded macros, including seven blank documents that are part of the same infection chain. **Almost all documents likely originally belong to the Ministry of Foreign Affairs of the Republic of Kazakhstan**, either as correspondence letters, draft documents, or internal administrative notes. They are dated **from 2021 to October 2024** (based on both internal dates and metadata).

The most recent documents are two diplomatic letters, one from the Embassy of Kazakhstan in Afghanistan, the second from the Embassy of Kazakhstan in Belgium, both intended for the central Ministry of Foreign Affairs regarding **diplomatic cooperation and economic issues**. The both are dated early September 2024.

Another identified weaponized document is an ongoing reviewed draft for a joint statement between Germany, Kazakhstan and Central Asia leaders (Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan) following a diplomatic meeting in Astana on 16 September 2024. We found the final version of the statement published on the official German government website, providing further evidence that the bait documents were not forged.

Other documents are **administrative reports** or **briefings** regarding official meetings between Kazakhstan officials and foreign stakeholders, such as the state visit from Kazakhstan **president Tokaiev in Mongolia** in October 2024 or **his meeting with executives of US companies in New York** during the 78th session of the UN General Assembly in September 2024.
The only document which does not seem to have been issued by the Ministry of Foreign Affairs of the Republic of Kazakhstan is a **correspondence letter from the Ministry of Defense of the Kyrgyz Republic intended for military cooperation among Central Asian countries.** Its content is related to intelligence sharing about *"the previously announced special operation of the People's Republic of China against Taiwan"*. Sekoia assess it likely refers to the 2022 Chinese military exercises around Taiwan, a series of military exercises by the People's Liberation Army that encircled Taiwan in August 2022.

КЫРГЫЗ РЕСПУБЛИКАСЫНЫН КОРГОО МИНИСТРЛИГИНИН ЭЛ АРАЛЫК АСКЕРДИ
КЫЗМАТТАШТЫК БАШКЫ БАШКАРМАЛЫГЫ

ГЛАВНОЕ УПРАВЛЕНИЕ МЕЖДУНАРОДНОГО ВОЕННОГО СОТРУДНИЧЕСТІ
МИНИСТЕРСТВА ОБОРОНЫ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

MAIN INTERNATIONAL MILITARY COOPERATION DEPARTMENT OF THE MINISTRY (
DEFENCE OF THE KYRGYZ REPUBLIC

« _____ » _________ 2022 г. № _________________ Экз.№___

На № __________________ от ____________________

Срочно!

Министерствам
и загранучреждениям
Кыргызской Республик

От имени управления международного военного сотрудничеств Министерства обороны Кыргызской Республики сообщаем, что в ходе начал объявленной ранее спецоперации КНР в отношении Тайваня, на данны момент были зафиксированы множественные факты поражения военны

Last but not least, what appears to be the oldest document is an internal Kazakhstan Ministry of Foreign Affairs 2021 **administrative note alerting Kazakhstan officials about cyber espionage attempts** and general information security, a document weaponized for this purpose.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ СЫРТҚЫ ІСТЕР МИНИСТРЛІГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ОРТАЛЫҒЫ

ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ МИНИСТЕРСТВЕ ИНОСТРАННЫХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

010000, Нұр-Сұлтан қаласы,
Дінмұхамед Қонаев көшесі, 31 ғимарат
тел.: 72-01-34, 72-05-13
2021 жылғы____________________

010000, город Нур-Султан,
улица Динмухамеда Кунаева, здание 31
тел.: 72-01-34, 72-04-14
«____»________________2021г.

№ № 1-0/19534-вн от 21.07.2021

Срочно!

Руководителям загранучреждений Республики Казахстан

Настоящим сообщаем, что в Центр продолжают поступать сведения о попытках несанкционированного доступа третьими лицами к ресурсам загранучрежедений Республики Казахстан.

По этой причине, во исполнение Плана усиления защиты информации ограниченного распространения, возникает необходимость повторного ознакомления руководителей и сотрудников загранучреждений с требованиямим обеспечения информационной безопасности при работе в информационно-телекоммуникационых сетях.

В этой связи, просим Вас ещё раз ознакомиться с соответствующим инструктажем прикрепленным к документу.

Приложение: инструктаж пользователя по соблюдению требований обеспечения информационной безопасности на 6-ти листах.

Инструктаж ЗУ.pdf

Старший специалист
по защите информационных ресурсов **А. Садыков**

Исп: А.Садыков
Тел.: 7203782
тел.+7 701 6260343

III. HATVIBE and CHERRYSPY infection chain

The infection chain related to this campaign includes the malware HATVIBE and CHERRYSPY. It has previously been partially documented in open source. In May 2023, Bitdefender highlighted HATVIBE and CHERRYSPY malware that have been used in a cyber espionage campaign targeting Asia, since at least late 2022. A few days later, CERT-UA also reported on these malware, linking them to the probable compromise of the official email account of the Tajikistan Embassy in Ukraine, which had been used to target Kazakhstan, Kyrgyzstan, Mongolia, Israel, and India.

Over a year later, in July 2024, CERT-UA disclosed that Ukraine's scientific research institution has been compromised again via an employee's email account, proving that this campaign was still ongoing at that time. Last, in November 2024, Recorded Future shed light on the scale of this campaign, reporting 62 confirmed unique victims across Central Asia, East Asia, and Europe since July 2024.

Although the infection chain was already partially documented, **the ten documents identified by Sekoia exhibit a previously unknown malicious code**, while retaining a similar execution structure.

For this analysis, we will focus a Word document titled *Rev5_Joint Declaration C5+GER_clean version.doc* (MD5: 35fee95e38e47d80b470ee1069dd5c9c), which is a commented draft of a joint declaration between the Heads of Central Asia countries and the Chancellor of Germany.

This document was weaponized on 13 September 2024 with a malicious macro aimed at creating another malicious document. This second document is automatically opened in an hidden Word instance by the initial macro, to drop and execute a malicious HTA (HTML Application) file embedding a VBS backdoor nicknamed "HATVIBE" by the CERT-UA. As this infection chain is pretty unique, we named it Double-Tap and decided to take a look at it.

Double-Tap infection chain leading to HATVIBE execution

When the *Rev5_Joint Declaration C5+GER_clean version.doc* document is opened, the user is prompted to execute a malicious macro. When executed, this macro does several things such as:

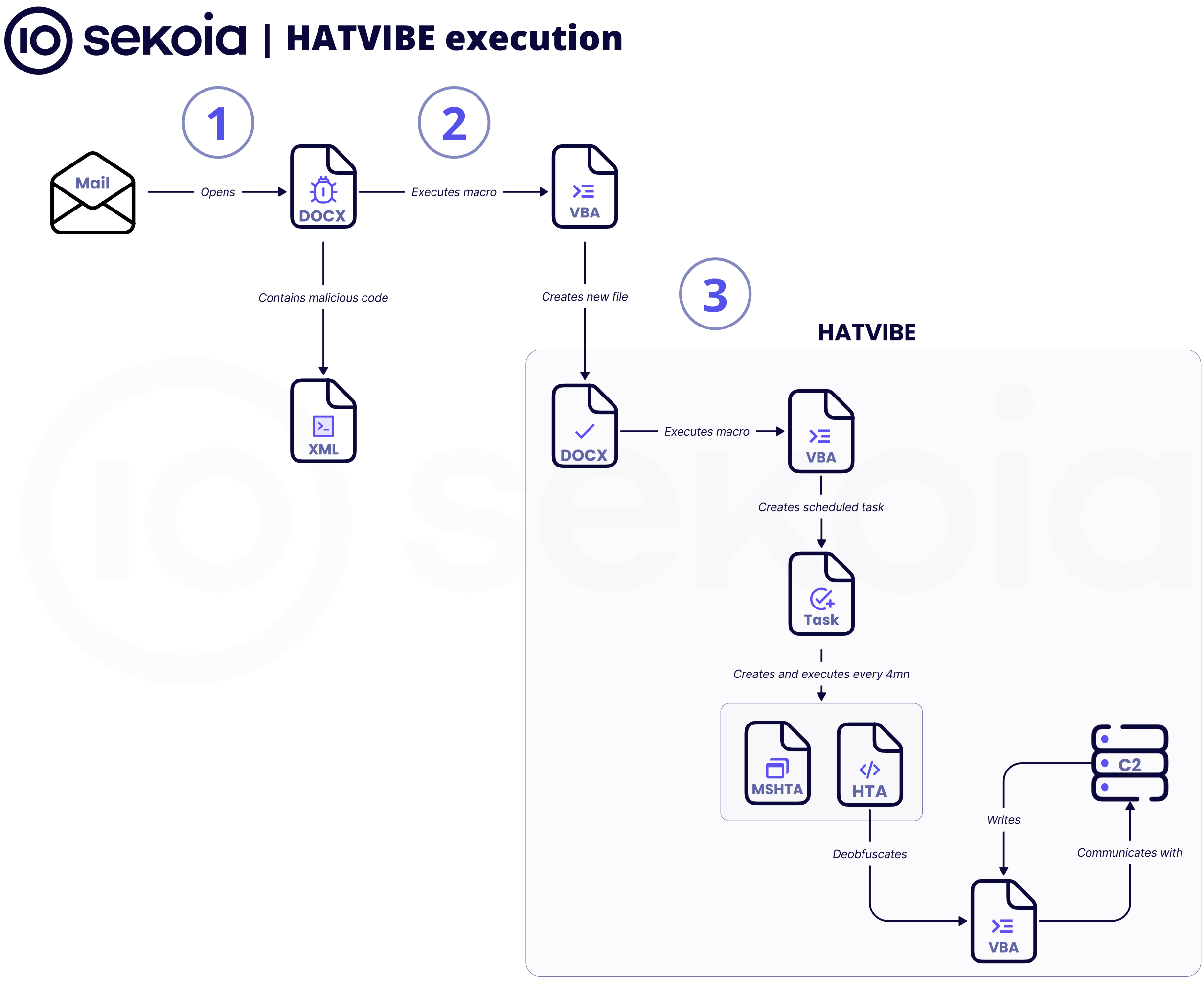
- It downgrades the security settings which ask the user to execute macros by altering the HKCU\Software\Microsoft\Office\[VERSION]\Word\Security\AccessVBOM registry key. This will lead to the execution of the malicious macro of the second document without user confirmation.
- It unprotects the document with a hardcoded password to delete shapes implemented by the attacker over it and saves it. The use of shapes is a quite common social engineering technique as it pushes the target to activate the macro in order to see the document's content.
- It creates a second blank document under C:\Users\[USER]\AppData\Local\Temp\. This second document is populated from variables present in the settings.xml of the first document and weaponised by adding a malicious macro to it. This malicious macro is also extracted from the settings.xml of the first document.
- Then, it launches in a hidden Microsoft Word instance this second malicious document, which will execute its macro completely silently as the AccessVBOM registry key has been previously altered.

The macro embedded in the second document is much more straightforward. It gets malicious VBA code to execute from variables in its settings.xml file. And then executes two methods from this code:

- The first method extracts the contents of an HTA file embedding HATVIBE variables in its settings.xml and saves it under C:\Users\[USER]\AppData\Local\Settings\locale (without any extension).
- The second method creates a scheduled task named "Settings\ServiceDispatch" by using RegisterTaskDefinition. This task aims to execute the HTA containing HATVIBE's code every four

minutes by launching mshta.exe.

The full chain can be summarised in the scheme below:



What makes this Double-Tap infection chain quite unique is that it employs many tricks to bypass security solutions such as storing the real malicious macro code in the settings.xml file and creating a scheduled task without spawning schtasks.exe for the second document or using, for the first document, an anti-emulation trick aimed to see if the execution time has not been altered, otherwise the macro is stopped.

Focus on HATVIBE

The HTA launched by the scheduled task contains the VBS backdoor named “HATVIBE” by the CERT-UA. The aim of this backdoor is to receive VBS modules for execution from a remote C2 server. Once received, HATVIBE uses a simple XOR algorithm to decrypt each module, contact it between two <script> tags before adding it to the HTML body of the HTA file, leading to the automatic execution of the received module.

The modules seem to be chained together and each module appears to be received from different C2 endpoints such as “/setup.php”, “/local.php” or “/upset.php”. During our analysis and after sending a PUT request to “/setup.php”, we received a first VBS module to execute. This module aims, once executed, to send another PUT request to “/local.php”.

The received payload from “/local.php” can take two forms. The first one is another VBS module to decrypt and execute inside the HTA file. The second one is a file to write on the disk, without execution.

We tried multiple times to receive any kind of payload from the “/local.php” endpoint. However, each attempt was a failure. According to the CERT-UA and Recorded Future, HATVIBE downloads and ultimately starts a more complex Python backdoor named CHERRYSPY.

A potential overlap with APT28-related Zebrocy campaigns

Zebrocy is the name of a backdoor and an alleged APT28 subgroup, which conducted between 2015 and 2020 cyber espionage campaigns on Central Asian states targeting government bodies, including defence and diplomatic entities. Zebrocy campaigns shared parts of the infrastructure, victimology and interests with APT28, according to cybersecurity vendors, including Kaspersky.

The Double-Tap campaign demonstrates some similarities with old Zebrocy infection chains, including the use of VBA scripts to drop a backdoor. Zebrocy and UAC-0063 notably share the following elements:

- a Double-Tap document technique (a Word document that executes another one);
- a C2 using a PHP backend;
- a Windows registry key modified to bypass security mechanisms (AccessVBOM);
- the creation of scheduled tasks to ensure persistence.

Based on the common victimology, areas of activity, and technical similarities, Sekoia analysts assess with medium confidence that **UAC-0063 is related to the GRU-operated APT28 intrusion set**, as assessed by CERT-UA.

IV. From Kazakhstan to Central Asia: a focus on a broader strategic espionage

After analysing the uncovered spearphishing Word documents regarding the subject and recipient, Sekoia analysts assess that all files were **legitimate documents issued from the Foreign Affairs of the Republic of Kazakhstan**, then weaponized to be used as spearphishing bait for **diplomatic-related entities in Central Asia**.

Those documents may have been exfiltrated through a cyber operation conducted earlier by the same intrusion set, within the same campaign. Yet, we do not have technical evidence to confirm this possibility. The documents may have also been obtained by another intrusion set through cyber operation, open source collection or by a physical operation (stolen laptop by intelligence agents), and then handed to the operators of this campaign to be weaponized.

If there is no technical evidence that Kazakhstan is the final target, we still assess it’s a realistic possibility that it is one of the prime targets in a cyber espionage campaign aiming at Central Asia, conducted by UAC-0063 (as assessed by the CERT-UA). This hypothesis is supported by the theme of the bait document and by the specific geopolitical context.

Kazakhstan geopolitical context

In recent years, geopolitical shifts have increasingly driven Kazakhstan to distance itself from Russia and pursue closer economic and strategic ties with other powers, notably Western states and China. Since the Russian invasion of Ukraine in February 2022, **Kazakhstan**, the leading Central Asian power and former part of the Soviet Union, **has maintained a balanced stance on the war in Ukraine** by supporting Ukraine's territorial integrity without openly condemning the Russian invasion.

This stance, aiming to **gain influence on both Russian and Western states**, also brings **economic opportunities** to Astana, which aims to become the key trade link between China and Europe. Indeed, Kazakhstan is well-positioned to benefit from the "Middle Corridor" in Central Asia, a network of roads, railways, and maritime routes that has gained new economic momentum due to the war in Ukraine.

Astana also developed its **economic relations with Central Asian states**, such as the new Talibans-ruled **Afghanistan** to which Kazakhstan resumed discussions by removing the Talibans from its list of terrorist organizations. In October 2024, president Tokaiev visited **Mongolia** during which both states signed a "Joint Declaration on Strategic Partnership", an agreement including a joint Earth observation satellite system, marking Kazakhstan's first satellite export.
Another notable development is that Kazakhstan is on the verge of **constructing its first civilian nuclear power plant** with France (EDF), Russia (Rosatom), China (CNNC), and South Korea (KHNP) competing for the project. This initiative has significant economic and geopolitical implications and is likely a point of interest for Russian intelligence.

Kazakhstan targeting for broader intelligence gathering

All geopolitical topics evoked above are highly likely to be subject of interest for the Russian intelligence service, thus likely **explaining most of the weaponized document's theme**.

Thus, we assess that our findings indicate a **part of a global cyber espionage campaign** targeting Central Asian countries, especially Kazakhstan external relations. It concurs with Bitdefender, CERT-UA and Recorded Future assessments.
The objective of this partially uncovered campaign is likely to gather strategic and economic intelligence on Kazakhstan's relations with Western and Central Asian countries, aiming to preserve Russia's influence in a region historically within its sphere of control. Ultimately, Russia's objectives are to ensure Kazakhstan remains politically aligned, to counter the influence of competing powers, and to secure its own economic and strategic foothold in the region.

V. Detection opportunities

There are several valuable detection opportunities when analysing the previously outlined infection chain.

Registry change

Upon the initial opening of the Microsoft Word document, a registry key modification occurs to enable persistent macro execution. This modification involves adding the "AccessVBOM" value set to 1 to the relevant registry path, which varies based on the Microsoft Office version:

```
Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\*\Word\Security
```

This technique has been well-known among attackers for many years, particularly during the rise of macros as malicious entry points. This setting enables macros to execute without prompting the user for permission. In the context of this campaign, it is essential to run the second Microsoft Word document and its macro seamlessly, without user interaction.

Collecting Microsoft Windows events related to registry changes is crucial for detecting such modifications. We provide below a Sigma detection rule for identifying these changes:

```
detection:
  registry:
    registry.value:
      - AccessVBOM
      - VbaWarnings
    registry.data.strings: 'DWORD (0x00000001)'
  cmdline_vbom:
    process.command_line|contains|all:
      - 'reg'
      - 'add'
      - '\SOFTWARE\Microsoft\Office\'
      - 'AccessVBOM'
  cmdline_warning:
    process.command_line|contains|all:
      - 'reg'
      - 'add'
      - '\SOFTWARE\Microsoft\Office\'
      - 'VbaWarnings'
  condition: registry or 1 of cmdline_*
```

Scheduled task

Another detection opportunity arises from using the “mshta.exe” binary, which is executed with a payload connecting to the attacker’s command and control (C2) server. When run from a previously created scheduled task, this behaviour stands out, as it is uncommon in most environments. This can also be correlated with an mshta.exe process initiating a network request to the Internet.

By relying on Windows Event Logs or EDR telemetry to monitor process parent-child relationships, we created a Sigma detection rule to identify executions from the scheduled task:

```
detection:
  selection:
    process.name: mshta.exe
    process.command_line: '*'
    process.parent.name: svchost.exe
    process.parent.command_line|contains|all:
      - "-k"
      - "netsvcs"
```

```
      - "-p"
      - "-s"
      - "Schedule"
  condition: selection
```

This pattern can be supplemented with a second detection to identify network connections initiated by “mshta.exe”:

```
detection:
  selection:
    process.name: mshta.exe
    process.command_line: '*'
    event.type: connection
  condition: selection
```

The infection chain employed to deliver **HATVIBE** leverages commonly known, albeit relatively old, techniques. Utilising macros and a living-off-the-land binary such as “mshta.exe” continues to prove effective, even for cyber espionage intrusions targeting specific organisations. For defenders, these offer real opportunities to intercept the onset of an attacker’s intrusion: against our customers’ telemetry we did not find any false positives for those two rules.

Conclusion

Based on a finding through our YARA trackers, we were able to document the HATBIVE infection chain from the Russia-aligned intrusion set UAC-0063. Our investigation extended Bitdefender, CERT-UA, and Recorded Future initial findings with exclusive IOCs, indicating that this campaign is still ongoing as of November 2024.

HATVIBE presents technical similarities and victimology that overlap with APT28-related Zebrocy campaigns, allowing us to assess with medium confidence that UAC-0063 is related to APT28 and GRU cyber activities.

The theme of spearphishing weaponized documents indicates a cyber espionage campaign focused on collecting strategic intelligence on diplomatic relations between Central Asia states, especially on Kazakhstan’s foreign relations, by Russian intelligence. This focus is coherent with Moscow’s strategic interests, which aim to preserve Russia’s influence in a region historically within its sphere of control.

Thank you for reading this blog post. Please don’t hesitate to provide your feedback on our publications. You can contact us at tdr[at]sekoia.io for further discussions, always good to have feedbacks from peers.

Appendix

C2

Domain	Domain	First seen

Domain	Domain	First seen
background-services[.]net	2.58.15[.]158	03/09/2024
lookup[.]ink	Cloudflare	17/09/2024
download-resourses[.]info	213.159.79[.]56	22/10/2024
[no domain]	38.180.207[.]137	04/10/2024
[no domain]	38.180.206[.]61	02/10/2024

Weaponized documents

- 06e4084e2d043f216c0bc7931781ce3e1cea4eca1b6092c0e34b01a89e2a6dea
- 3b87dc25a11b6268019d5eae49a6b93271dfdc262f2607cfefa35d196f724997
- 47092548660d5200ea368aacbfe03435c88b6674b0975bb87a124736052bd7c3
- 6edf3d03bd38c800d5d1e297d59c2496968202358f4be47e1f07e57a52485e0c
- c61e9326421d05d62cafd6c04041ab1a8f57c0a21d424b9ca04b6a1fc275af19
- e3a0be8852d77771dc3f44f3e9a051e7fe56547b569aad5a178ae44ef31713b9
- e440bad60823642e8976528bd450364ce2542d15a69778ff20996eb107158b8d
- efc99e6f3cdd10313c52a8ad099424e3f39ab85b75375b8db82717d61c7f0118
- fd78051817b5e2375c92d14588f9a4ba1adc92cc1564e55e6150ae350ed6c889

Deobfuscated HATVIBE VBA code

YARAs

```
rule apt_UAC0063_HATVIBE_loader_obfuscated_VBA {
    meta:
        malware = "HATVIBE"
        intrusion_set = "UAC-0063"
        description = "Detects obfuscated HATVIBE HTA file"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
        hash =
"332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725"
    strings:
        $ = "<HEAD><HTA:APPLICATION ID=\"" ascii
        $ = "<span id=" ascii
        $ = "<script Language=\"VBScript.Encode" ascii
    condition:
        filesize < 1MB
        and all of them
}
```

```
rule apt_UAC0063_HATVIBE_loader_deobfuscated_VBA {
    meta:
        malware = "HATVIBE"
```

```
        intrusion_set = "UAC-0063"
        description = "Detects obfuscated HATVIBE HTA file"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
        hash =
"0fa7e3ffb8a9ca246cc1f1e3f6118ced7a7b785de510d777b316dfcefdddb0be"
    strings:
        $ = "window.resizeTo 0,0" ascii
        $ = ".InnerHTML =" ascii fullword
        $ = "Chr(Asc(Mid(" ascii fullword
        $ = "Xor Asc(Mid(" ascii fullword
        $ = "Mod Len(" ascii fullword
        $ = "\"script>"
    condition:
        3 of them
}
```

```
rule apt_UAC0063_HATVIBE_loader_malicious_xml_content1 {
    meta:
        intrusion_set = "UAC-0063"
        description = "Detects some suspected APT28 document settings.xml"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
        hashVariantA =
"e8c0f309df515733ad8233b409d6b64d005f88bf1d549567365c2b21a90cf05c"
        hashVariantB =
"51ca8b4aa5744148ed049a529b2676eb95229aedc213b874c0c78ff82c7de559"
    strings:
        $subVariantA_1 = "Sub baads()" nocase ascii
        $subVariantA_2 = "Sub goods()" nocase ascii
        $subVariantB_1 = "Sub pop()" nocase ascii
        $subVariantB_2 = "Sub push()" nocase ascii
        $docOpen = "docUment_oPen" nocase ascii
        $localAppData = "%LOCALAPPDATA%" nocase ascii
        $mshta = "mshta.exe" nocase ascii
        $scheduledTask = "Schedule.Service" nocase ascii
        $docVar = "<w:docVar w:name="
    condition:
        filesize < 5MB
        and (
            all of ($subVariantA_*)
            or
```

```
            all of ($subVariantB_*)
        )
        and $docOpen
        and $localAppData
        and $mshta
        and $scheduledTask
        and $docVar
}
```

```
rule apt_UAC0063_Stage_1_Malicious_Macro_compiled {
    meta:
        intrusion_set = "UAC-0063"
        description = "Detects malicious VBA file based on password"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
        hash = "a502b51d44a3e2e59218618ab7a30971"
    strings:
        $ = "oikmseM#*inmowefj8349an3" ascii
    condition:
        uint32be(0) == 0xd0cf11e0 and
        filesize < 50KB and
        all of them
}
```

```
rule apt_UAC0063_Stage_1_Malicious_Macro_clear {
    meta:
        intrusion_set = "UAC-0063"
        description = "Detect clear version of the malicious Stage 1 Macro
by UAC-0063"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
        hash = "6f5a9ce100dd650dedbc3e68f74c3b97"
    strings:
        $ = ".RegWrite"
        $ = "< TimeValue("
        $ = "Word.Application"
        $ = "ActiveDocument.Name"
        $ = "While Now"
    condition:
        all of them and filesize < 3KB
}
```

```
rule apt_UAC0063_Stage_2_Malicious_Macro_clear {
    meta:
        intrusion_set = "UAC-0063"
        description = "Detect clear version of the malicious VBA by UAC-
0063"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
    strings:
        $ = "appdir = CreateObject"
        $ = "svc.NewTask("
        $ = ".RegisterTaskDefinition"
        $ = ".Variables.Count"
        $ = "Schedule.Service"
    condition:
        all of them and filesize < 3KB
}
```

```
rule apt_UAC0063_Settings_xml_containing_VBE {
    meta:
        intrusion_set = "UAC-0063"
        description = "Detects settings.xml file containing a VBE in hex"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
        hash = "e3f6d079d99eeb54566fc37fa24ff6f7"
    strings:
        $start = "<w:settings"
        $vbe_head = "23407e5e"
        $vbe_tail = "5e237e40"
        $var = "w:val="
    condition:
        filesize < 50KB
        and $start
        and $vbe_head
        and $vbe_tail
        and #var > 100
}
```

```
rule apt_UAC0063_HATVIBE_vbe {
    meta:
        malware = "HATVIBE"
        intrusion_set = "UAC-0063"
```

```
        description = "Detects the HATVIBE header in VBE"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
        hash = "78db9584ff4f7cd8f006eb6c12cac575"
    strings:
        // On Error Resume Next / window.resizeTo 0,0 / window.moveTo
-2000,-2000
        $header = "#@~^EwwAAA==6
P3MDKDP\"+k;:.PH+XY@#@&Skx9GhcD+kr\"+:W,!S!@#@&SkUNKARsW-n:WPR+Z!T~ +Z!T"
    condition:
        $header
}
```

```
rule apt_UAC0063_HATVIBE_decoded {
    meta:
        malware = "HATVIBE"
        intrusion_set = "UAC-0063"
        description = "Detects decoded HATVIBE's VBE"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
    strings:
        $ = "window.resizeTo 0,0"
        $ = "window.moveTo -2000,-2000"
        $ = ".InnerHTML ="
        $ = "& Chr(Asc(Mid("
    condition:
        all of them
}
```

```
rule apt_UAC0063_HATVIBE_module_decoded {
    meta:
        malware = "HATVIBE"
        intrusion_set = "UAC-0063"
        description = "Detects decoded HATVIBE's modules received through
HTTP"
        source = "Sekoia.io"
        creation_date = "2024-12-03"
        classification = "TLP:GREEN"
    strings:
        $ = "Mid(http_obj.reponseText,1"
        $ = "innerHTML = strHTML"
        $ = "http_obj.Open \"PUT"
```

```
        $ = "<script Language=VBScript"
    condition:
        2 of them
}
```