

"Excuse me, how will the conflict between Russia and Ukraine affect the situation on the peninsula?" Analysis of the recent targeted attack activities of APT organization Kimsuky

2022-05-05 NSFOCUS APT , KimAPosT , Kimsuky , TBS , Ukraine read: 79

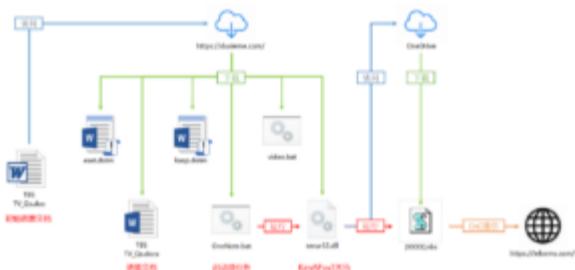
## I. Overview

Recently, NSFOCUS Fuying Lab captured multiple phishing documents and related Trojan programs named "TBS TV\_Qs.doc". After analysis, the series of malicious files are all part of the recent cyber attack activities of APT organization Kimsuky, and its direct targets are likely to be military experts in charge of the peninsula issue.

Relevant in-field attack payloads show that Kimsuky's attack has lasted for at least one month. When Fuying Lab captured the attack, related online services still existed and the attack process was still complete. Based on the obtained attack payload, it is likely that the attacker has achieved his main attack purpose.

## 2. Process analysis

The Kimsuky attack activity captured this time starts with a malicious document, downloads different anti-virus software countermeasures by visiting a specific URL, tries to run the known Kimsuky Trojan program KimAPosT, and finally uses the malicious file stored in the OneDrive network disk. The code performs a specific attack behavior.



The main process of Kimsuky's targeted attack

The Kimsuky organization began to test and use a similar attack process in 2021, and in this process, it improved the bypass strategy and added some anti-analysis methods. Compared to other Kimsuky known attack flows, this flow has more flexibility in final attack code delivery.

## 3. Activity Analysis

The Kimsuky attack activity captured this time has the following characteristics:

1. The content of the decoy document is some form of interview questions, covering the impact of the Russian-Ukrainian conflict on North Korea and South Korea, North Korea's ballistic missile test, China-South Korea relations, South Korea's new president, the denuclearization of the peninsula, how to put pressure on North Korea and other international politics topic;
2. The decoy file is named "TBS TV\_Qs.doc", which corresponds to the content form, indicating that the decoy is trying to disguise as TBS interview material.

### Kimsuky Decoy Document Contents

本次捕获的Kimsuky攻击活动，带有以下时间特征：

1. 截至发现时（2022年4月27日），攻击流程中使用的各远程链接仍可解析；
2. 本次攻击中使用的话题诱饵为俄乌冲突（2022年2月24日）相关内容；
3. 本次攻击中出现的使用的KimAPosT木马，其CnC地址可以直接关联至一个早期（2022年3月12日）KimAPosT木马；
4. 截至发现时（2022年4月27日），攻击流程最终阶段代码已不具备实际攻击能力。

由此可以推断，本次事件是一场出现在2022年3月初，持续了一个月以上的，针对专注半岛问题研究人员的Kimsuky攻击活动。根据诱饵内容，其直接目标很可能是与TVB有合作关系的军事评论员或关联群体。截至2022年4月27日，Kimsuky攻击者可能已经完成了主要攻击过程，将最终攻击代码替换为仅包含受害者统计功能的非入侵代码。

## 四、组件分析

本次Kimsuky定向攻击活动中出现的功能性vbs脚本、bat脚本等攻击组件较多。本节仅展示主要组件或木马程序。

### 4.1 恶意文档TBS TV\_Qs.doc

名为“TBS TV\_Qs.doc”的office文档是Kimsuky本次攻击过程中的初始载荷。

该文档使用内置的宏代码执行恶意行为，因此，为欺骗受害者启动文档的编辑功能，该文档打开后呈现如下内容：

Kimsuky初始恶意文档内容

如果受害者依照提示启动了内置宏，恶意宏代码将分别在文档打开时与文档关闭时执行不同的操作。

宏代码运行后，文档首先尝试获取远程链接https[:]//dusieme.com/panda/TBS TV\_Qs.docx中的内容并打开，该内容为用于欺骗受害者的诱饵文档。

主要恶意代码集中在宏的AutoClose函数中。关闭文档时，该文档将根据受害者系统中反病毒软件的安装情况执行对应的操作。该文档检测的反病毒软件名称与对应操作见下表：

检测反病毒软件名称	对应厂商	对应操作
bdagent.exe, epsecurityservice.exe	Bitdefender	无
mbam	Malwarebytes	无
nortonsecurity.exe	Norton	无
equi.exe, ekrn.exe	ESET	下载并植入模板文档，来自 <a href="https[:]//dusieme.com/panda/ca.php?na=dot_eset.gif">https[:]//dusieme.com/panda/ca.php?na=dot_eset.gif</a>
avpui.exe, avp.exe, msseces.exe	Kaspersky	下载并植入模板文档，来自 <a href="https[:]//dusieme.com/panda/ca.php?na=dot_kasp.gif">https[:]//dusieme.com/panda/ca.php?na=dot_kasp.gif</a>
eppwsc.exe, a2guard.exe	Emsisoft	下载并运行vbs文件，来自 <a href="http://dusieme.com/panda/ca.php?na=vbs_kasp.gif">http://dusieme.com/panda/ca.php?na=vbs_kasp.gif</a>
sophos,	Sophos	执行上述操作产生的%appdata%\temp.vbs文件
tmwscsvc, ntrtscan, tmrhea, pccntmon.exe, coreserviceshell	TrendMicro	写入开机启动项OneNote.bat，来自 <a href="https[:]//dusieme.com/panda/ca.php?na=start2.gif">https[:]//dusieme.com/panda/ca.php?na=start2.gif</a>
sbamsvc.exe, epag.exe, scs.exe, ccsvchst	Vipre	写入开机启动项OneNote.bat，来自 <a href="https[:]//dusieme.com/panda/ca.php?na=start4.gif">https[:]//dusieme.com/panda/ca.php?na=start4.gif</a>
avastui, avgui.exe, v3l,	Avast	写入开机启动项OneNote.bat，来自 <a href="https[:]//dusieme.com/panda/ca.php?na=start3.gif">https[:]//dusieme.com/panda/ca.php?na=start3.gif</a>
agentsvc.exe, psuaservice	Panda	下载并运行vbs文件，来自 <a href="https[:]//dusieme.com/panda/ca.php?na=video.gif">https[:]//dusieme.com/panda/ca.php?na=video.gif</a>

[https\[:\]//dusieme.com/panda/ca.php?na=videop.gif](https://dusieme.com/panda/ca.php?na=videop.gif)

写入开机启动项OneNote.bat，来自

[https\[:\]//dusieme.com/panda/ca.php?na=start1.gif](https://dusieme.com/panda/ca.php?na=start1.gif)

下载并运行vbs文件，来自

[https\[:\]//dusieme.com/panda/ca.php?na=video.gif](https://dusieme.com/panda/ca.php?na=video.gif)

—  
—  
写入开机启动项OneNote.bat，来自

[https\[:\]//dusieme.com/panda/ca.php?na=start1.gif](https://dusieme.com/panda/ca.php?na=start1.gif)

表1 Kimsuky恶意文档检测的反病毒软件与对应操作

可以看到，该恶意文档通过远程服务器dusieme.com提供的vbs、bat、dotm等类型的文件，对常见反病毒拦截策略进行了绕过。

随后，该文档进一步检测以下进程名称字符串：

进程名称字符串

equi.exe

ekrn.exe

avpui.exe

avp.exe

wrsa.exe

v3l

avira

avguard.exe

antivirservice

avscan.exe

tmwscsvc

nrttscan

tmrhea

pccntmon.exe

coreserviceshell

bdagent.exe

epsecurityservice.exe

表2 Kimsuky恶意文档检测的进程名称字符串

当运行环境中不存在以上进程时，文档尝试从[https\[:\]//dusieme\[.\]com/panda/ca.php?na=secur32.gif](https://dusieme[.]com/panda/ca.php?na=secur32.gif)处下载数据，并保存至%localappdata%\Microsoft\OneDrive\secur32.dll。该secur32.dll文件是下一阶段的木马程序，由上述绕过策略中注册的开机启动项运行。

最终，恶意文档还会尝试连接远程链接[https\[:\]//dusieme\[.\]com/panda/r.php](https://dusieme[.]com/panda/r.php)，将检测到的反病毒软件名称与其他运行信息上传到该位置。

#### 4. 2 诱饵文档TBS TV\_Qs.docx

名为”TBS TV\_Qs.docx”的文件是初始恶意文档打开时从[https\[:\]//dusieme\[.\]com/panda/TBS TV\\_Qs.docx](https://dusieme[.]com/panda/TBS TV_Qs.docx)处下载的文档。该文档用于欺骗受害者，使其认为文档运行正常。

该文档携带如下内容：

Kimsuky诱饵文档内容

可以看出该文档记录了某种形式的采访问题，涵盖了俄乌冲突对朝韩两国的影响、朝鲜弹道导弹实验、中韩关系、韩国新总统、半岛无核化、如何向朝鲜施压等敏感政治话题。结合文档名称，可以推测Kimsuky本次攻击活动的目标为专注半岛问题的研究人员，很可能是受TVB邀请的军事评论员或关联群体。

#### 4.3 恶意模板文档eset.dotm

该恶意模板文档被初始恶意文档从[https\[:\]//dusieme\[.\]com/panda/ca.php?na=dot\\_eset.gif](https://dusieme[.]com/panda/ca.php?na=dot_eset.gif)下载使用，用于替换Normal.dotm模板文件，绕过ESET反病毒程序。

该模板文档带有恶意宏代码，用于下载[https://dusieme\[.\]com/eset/d.php?na=battmp](https://dusieme[.]com/eset/d.php?na=battmp)处的批处理文件并执行。

#### 4.4 恶意模板文档kasp.dotm

该恶意模板文档被初始恶意文档从[https\[:\]//dusieme\[.\]com/panda/ca.php?na=dot\\_kasp.gif](https://dusieme[.]com/panda/ca.php?na=dot_kasp.gif)下载使用，用于替换Normal.dotm模板文件，绕过Kaspersky反病毒程序。

该模板文档带有恶意宏代码，用于执行前述过程中下载的批处理文件c:\users\public\videos\video.bat。

## 4.5 木马程序secur32.dll

名为secur32.dll的文件是初始恶意文档最终从[https\[:\]//dusieme\[.\]com/panda/ca.php?na=secur32.gif](https://dusieme[.]com/panda/ca.php?na=secur32.gif)下载的木马程序，被设置为由开机启动项执行。

该木马程序是已知Kimsuky木马程序的变种，绿盟科技将其暂称为KimAPosT。

该木马的主要功能包含两个部分，分别由两个线程实现。

木马的一个线程会持续寻找类名为“49B46336-BA4D-4905-9824-D282F05F6576”的窗口，并将该其隐藏。该类名对应安博士杀毒软件的实时检测窗口，因此该线程的实际功能为隐藏安博士告警提示。

木马的另一个线程主要用于将内置的一个vbs脚本释放至%TEMP%\[4字节随机字符].vbs并运行。

该KimAPosT变种与原版木马的主要区别在于使用自制的动态API加载函数处理加密的API字符串。

## 4.6 最终攻击载荷[XXXX].vbs

该最终载荷是vbs脚本，同样曾出现在Kimsuky已知活动中。与早期版本相比，该版本改变了部分代码逻辑。

该vbs脚本中记录了一个指向OneDrive网盘的远程链接，直接访问该链接将获取以下内容：

## Kimsuky vbs中url的对应内容

实际上该链接中的内容并未被直接使用，Kimsuky攻击者可能希望使用这种方式误导分析人员。

该脚本随后对上述onedrive链接进行拆分，重组为一个新的链接：

[https://api.onedrive\[.\]com/v1.0/drives/1C11C1E4D824C4B5/items/1C11C1E4D824C4B5%21106?select=id%2C%40content.downloadUrl&authkey=%21AGK9y7IsivaLcUU](https://api.onedrive[.]com/v1.0/drives/1C11C1E4D824C4B5/items/1C11C1E4D824C4B5%21106?select=id%2C%40content.downloadUrl&authkey=%21AGK9y7IsivaLcUU)

脚本访问该链接，获取以下回复：

## Kimsuky vbs实际访问url的对应内容

该回复中的1drv链接中存储着最终的恶意脚本，脚本内容被加密，逻辑与初始恶意文档中出现的算法相同。

以往的同类攻击事件中，最终恶意脚本的主要功能包括统计受害者用户名、下发vbs代码或批处理文件、窃取受害主机内容。

然而，截至本次活动被发现时，最终恶意脚本已被替换为仅包含统计功能的简单代码：

Kimsuky vbs实际执行的代码内容

该代码将受害者计算机用户名发送至指定地址https[:]//ielsems[.]com/cic/macro.php中。

关联样本显示，该域名ielsems[.]com早在2021年就已被攻击者使用，出现在类似的攻击流程当中。

## 五、总结

随着近期国际形势的激烈变化，多个APT组织再次进入活跃状态。

Kimsuky的本次定向攻击活动早有预谋，相关攻击流程和工具在经过一年以上的较长测试周期后才投入使用，并在静默运行数周后才最终暴露。

如果防御方能够及时跟进此类APT组织新攻击流程，在其测试期间发现并补充检测策略，则可以在其发动攻击时作出良好的应对。

**版权声明** The copyright holder of all contents of the "Technology Blog" on this site is NSFOCUS Technology Group Co., Ltd. ("NSFOCUS"). As a platform for sharing technical information, NSFOCUS looks forward to interacting with the majority of users, and welcomes the full text to be forwarded with the source (NSFOCUS-Technical Blog) and website indicated. For any form of use other than the above, it is necessary to apply for copyright authorization to NSFOCUS (010-68438880-5462) in advance. For unauthorized use, NSFOCUS reserves the right to pursue responsibility. At the same time, if a legal dispute is caused by the unauthorized use of blog content, the user shall bear all legal responsibilities and has nothing to do with NSFOCUS.

Spread the word. Share this post!

**Meet The Author**

NSFOCUS