Hive Pro®

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## ACTOR REPORT

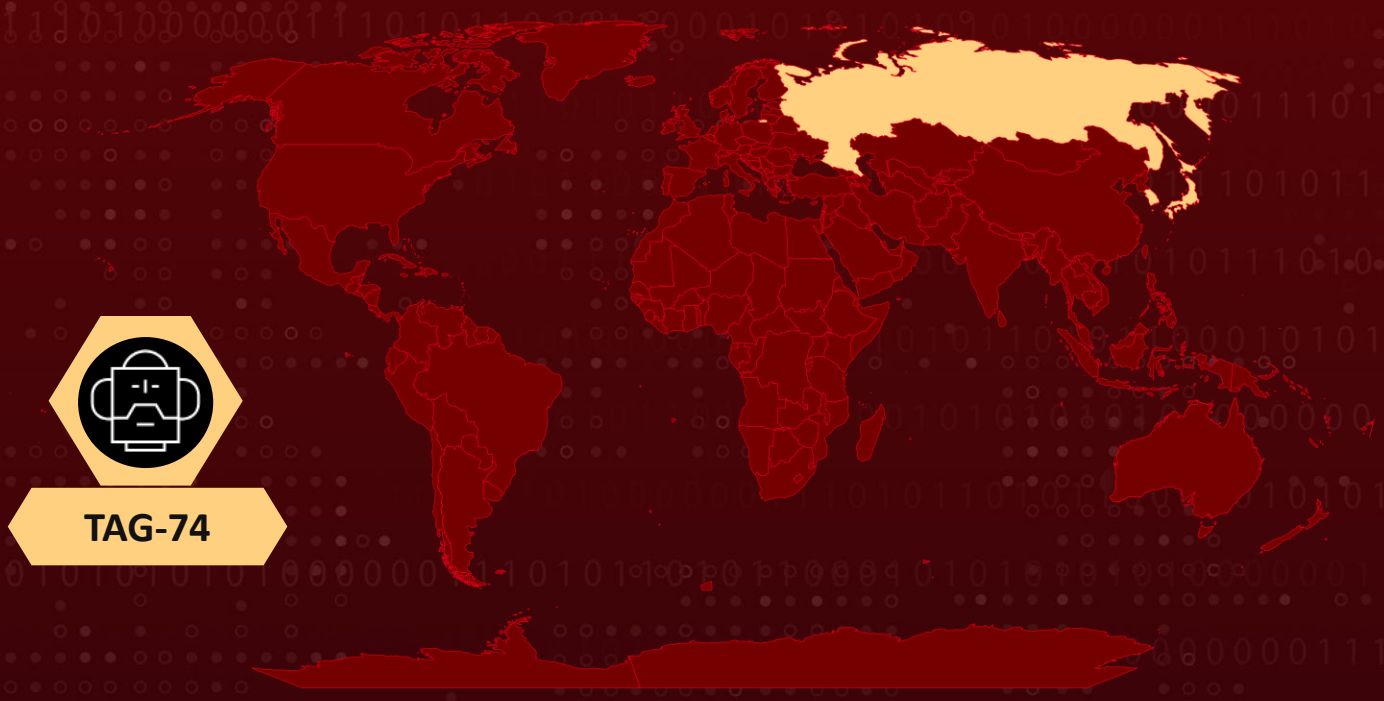
# TAG-74's Multi-Year Campaign Targets South Korean Organizations

| Date of Publication | Admiralty code | TA Number |
| --- | --- | --- |
| September 27, 2023 | A1 | TA2023390 |

# Summary

**First Appearance:** May 2023
**Actor Name:** TAG-74
**Target Industries:** Academic, aerospace, defense, government, military, and political organizations
**Target Region:** South Korea, Japan, and Russia
**Malware:** Bisonal, ReVBShell

## Actor Map



# Actor Details

**#1** Chinese state-sponsored cyber espionage has been identified as partaking in a "multi-year" campaign with a specific focus on South Korean academic, political, and governmental organizations. Within this campaign, the threat actor TAG-74 has displayed a notable preference for targeting South Korean academic institutions. TAG-74 is a Chinese state-sponsored threat activity group primarily dedicated to intelligence gathering activities.

**#2** TAG-74 utilizes social engineering attacks, employing Microsoft Compiled HTML Help (CHM) files as lures. These CHM files are used to deliver a modified version of an open-source Visual Basic Script backdoor known as "ReVBShell." This backdoor, in turn, is used to deploy the Bisonal remote access trojan.

**#3** The techniques associated with this TAG-74 campaign involve the use of .chm files that trigger a DLL search order hijacking execution chain. This chain is designed to load a customized version of the open-source VBScript backdoor, ReVBShell. Additionally, multiple instances of the customized backdoor, Bisonal, have been identified communicating with TAG-74 infrastructure. Bisonal is likely employed to provide additional capabilities once initial access is established through ReVBShell.

**#4** ReVBShell is configured to enter a sleep mode for a specified duration, a command that can be issued remotely and edited as needed from a server. Additionally, it employs Base64 encoding to obfuscate the command-and-control (C2) communication, making it more challenging to detect and analyze.

**#5** It has been observed that this customized variant of ReVBShell is highly likely to be shared by both TAG-74 and another closely associated threat activity group, **Tick Group** (aka BRONZE BUTLER, Stalker Panda, and Stalker Taurus). There has been prior evidence suggesting the presence of shared capabilities and close collaboration between Tick Group and TAG-74-linked activities.

**#6** TAG-74's has consistent focus on South Korean targets for an extended duration and its apparent alignment with the Northern Theater Command, it is likely that the group will continue to maintain a high level of activity in its persistent endeavors to collect intelligence from strategic targets within South Korea. Additionally, there is the possibility of the group expanding its operations to include countries such as Japan and Russia in its intelligence-gathering efforts.

## Actor Group

| NAME | ORIGIN | TARGET REGIONS | TARGET INDUSTRIES |
|---|---|---|---|
| TAG-74 | China<br>**MOTIVE**<br>Cyber-espionage | South Korea, Japan, and Russia | Academic, aerospace, defense, government, military, and political organizations |

# Recommendations

**Configure IDS/IPS for Alerting and Blocking:** Set up your Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), or other network defense mechanisms to generate alerts for connection attempts to and from external IP addresses and domains. Block these connections to prevent malicious activity.

**Block Low-Legitimate-Use Attachments:** Organizations should evaluate the feasibility of blocking file attachments such as .chm files and other formats with low legitimate use at email gateways and through application deny lists. These types of files are frequently abused and have limited legitimate use in most environments.

**Regular Log Analysis:** Conduct regular log analysis to promptly generate alerts and subsequently block identified Command and Control (C2) communications. This helps in the timely detection and remediation for active intrusions.

**Block Traffic Involving DDNS Domains:** Due to the prevalence of dynamic domain name system (DDNS) domains in network intrusion activity, consider implementing measures to block and log all TCP/UDP network traffic involving DDNS subdomains. Utilize technologies like DNS Response Policy Zones (RPZ) or similar mechanisms for effective blocking.

# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0005<br>Defense Evasion |
| TA0007<br>Discovery | TA0011<br>Command and Control | TA0010<br>Exfiltration | T1566<br>Phishing |
| T1566.001<br>Spearphishing Attachment | T1059<br>Command and Scripting Interpreter | T1059.005<br>Visual Basic | T1204<br>User Execution |
| T1204.002<br>Malicious File | T1547<br>Boot or Logon Autostart Execution | T1547.001<br>Registry Run Keys / Startup Folder | T1574<br>Hijack Execution Flow |
| T1574.001<br>DLL Search Order Hijacking | T1218<br>System Binary Proxy Execution | T1218.001<br>Compiled HTML File | T1480<br>Execution Guardrails |
| T1518<br>Software Discovery | T1518.001<br>Security Software Discovery | T1132<br>Data Encoding | T1132.001<br>Standard Encoding |
| T1071<br>Application Layer Protocol | T1071.001<br>Web Protocols | T1573<br>Encrypted Channel | T1573.001<br>Symmetric Cryptography |
| T1041<br>Exfiltration Over C2 Channel | | | |

# Indicator of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd,<br>11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd,<br>a88ca28b0948e810d4eb519db7b72a40cfe7907ce4c6a881a192880278f3c8b5,<br>89f250599e09f8631040e73cd9ea5e515d87e3d1d989f484686893bececc1a9bc,<br>0ea0b19c562d20c6ac89a1f2db06eedcb147cde2281e79bb0497cef62094b514,<br>aa4ad5341a9258330abd732cbab3721d76764f1ff21a8f960622661d701a1a71,<br>8f50f49e77ddcc7ef639a76217b2eb25c48f9ce21ae8341050d0da49b89b7b34,<br>ae0f641dc9d33ee50990971104ef1c598e216693700be6b74bb1e9ef373af97c,<br>465c7c6a0f23ba5f928fc0d0cdc4d9f6ec89e03dcedafc3d72b3b3c01a54a00c,<br>6a59421fd225d90439b6a933458718cf43dbe518c63979e8980bc070c070558a,<br>df7d584d56af6fcf3cca31ed0d3a4d34abd2c1019b8d223a230f8a78075a7d9a,<br>078a8026f32b8d05258285dc527408388c651f6c3eaebc45f8bb3f4b42248631,<br>c643598b4ee0e9b3b70dae19437bbec01e881a1ad3b2ec1f6f5c335e552e5d6e,<br>9425666e58b200306935c36301d66a4bf2c831ad41ea0ee8984f056257b86eb6,<br>a16997954b64499479b4721c9f742b5d2875496f2035e1c654b06694981041b2,<br>0d0acd7e7257a715c10dded76acb233adc8fdfe32857eda060bd1448e8b54585,<br>0ea02fddf2ec96d4aee8adaffda2dd5fab0ea989b0c3f8c1577a1be22ee9153a,<br>e3cdaa9bfba6bfac616b7f275c1e888b8910efcb8a3df071f68ad1e83710bd61,<br>9fdb528949a2b80ac40cb7d3333bdff5d504294cc3d90cf353db72b8beffd2b2,<br>607f324c3427916d67369e40af72aa441f3ca7be1e0ec6c53c3558fc7a1c4186,<br>8efc5db8c678bdf27dacbf033842c2ef676c979afdc4561cb8d315d2d488491f, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | beb09817608daba003589292a6cca2f724c52f756df2ef0e230380345d702716,<br>ba07ee6409908384172511563e6b9059cf84121fcb42c54d45c76ec67cb36d7c,<br>bf1d1f5157756529d650719cc531ec2de94edb66ae1dabd00ed6f4b90a336d9c,<br>2dd7c9ea32f5b2a4d431fc54aa68cd76837f80bb324ef2e4e1e5134e467e35af,<br>56c9235e55b1a6371762159619e949686d8de2b45a348aeb4fd5bed6a126f66a,<br>dda47ba7a41c9a2f041cc10f9b058a78e0019315c51cc98d0f356e2054209ae5,<br>Cf5bbbcb3f4d5123c08635c8fd398e55e516893b902a33cd6f478e8797eea962,<br>b3a8ea3b501b9b721f6e371dd57025dc14d117c29ce8ee955b240d4a17bc2127,<br>9d10de1c3c435927d07a1280390faf82c5d7d5465d772f6e1206751400072261,<br>0eea610ec0949dc602a7178f25f316c4db654301e7389ee414c9826783fd64c0,<br>8073593a7311bc23f971352c85ce2034c01d3d3fbbe4f99a8f3825292e8f9f77,<br>e1748e7e668d6fc7772e95c08d32f41ad340f4a9acf0e2f933f3cbeba7323afa,<br>0d6893c7a3a7afc60b81c136b1dcdfb24b35efab01aac165fe0083b9b981da7c,<br>77fbb82690c9256f18544e26bb6e306a3f878d3e9ab5966457ac39631dfd2cb0 |
| IPv4 | 45.133.194[.]135,<br>92.38.135[.]92,<br>107.148.149[.]108,<br>141.164.60[.]28,<br>148.163.6[.]214,<br>158.247.223[.]50,<br>158.247.234[.]163 |
| Domains | alleyk.onthewifi[.]com,<br>anrnet.servegame[.]com,<br>asheepa.sytes[.]net,<br>attachdaum.servecounterstrike[.]com,<br>attachmaildaum.servecounterstrike[.]com,<br>attachmaildaum.serveblog[.]net,<br>bizmeka.viewdns[.]net,<br>bucketnec.bounceme[.]net,<br>chsoun.serveftp[.]com, |

| TYPE | VALUE |
| --- | --- |
| Domains | ckstar.zapto[.]org,<br>daecheol.myvnc[.]com,<br>eburim.viewdns[.]net,<br>eduin21.zapto[.]org,<br>elecinfonec.servehalflife[.]com,<br>foodlab.hopto[.]org,<br>formsgle.freedynamicdns[.]net,<br>formsgle.freedynamicdns[.]org,<br>fresh.servepics[.]com,<br>global.freedynamicdns[.]net,<br>global.freedynamicdns[.]org,<br>hairouni.serveblog[.]net,<br>hamonsoft.serveblog[.]net,<br>hanseo1.hopto[.]org,<br>harvest.my-homeip[.]net,<br>hometax.onthewifi[.]com,<br>hwarang.myddns[.]me,<br>jaminss.viewdns[.]net,<br>janara.freedynamicdns[.]org,<br>jeoash.servemp3[.]com,<br>jstreco.myftp[.]biz,<br>kanager.bounceme[.]net,<br>kcgselect.servehalflife[.]com,<br>kjmacgk.ddnsking[.]com,<br>kookmina.servecounterstrike[.]com,<br>ksd22.myddns[.]me,<br>kumohhic.viewdns[.]net,<br>kybook.viewdns[.]net,<br>leader.gotdns[.]ch,<br>likms.hopto[.]org,<br>logindaums.ddnsking[.]com,<br>loginsdaum.viewdns[.]net,<br>mafolog.serveminecraft[.]net,<br>mailplug.ddnsking[.]com,<br>minjoo2.servehttp[.]com,<br>mintaek.bounceme[.]net,<br>munjanara.servehttp[.]com,<br>necgo.serveblog[.]net,<br>pattern.webhop[.]me,<br>pixoneer.myvnc[.]com,<br>plomacy.ddnsking[.]com,<br>proeso.servehttp[.]com,<br>prparty.webhop[.]me,<br>puacgo1.servemp3[.]com,<br>saevit.servebeer[.]com, |

| TYPE | VALUE |
| --- | --- |
| Domains | safety.viewdns[.]net,<br>samgiblue.servegame[.]com,<br>sarang.serveminecraft[.]net,<br>satreci.bounceme[.]net,<br>sejonglog.hopto[.]org,<br>signga.redirectme[.]net,<br>skparty.myonlineportal[.]org,<br>steering.viewdns[.]net,<br>stjpmsko.serveblog[.]net,<br>surveymonkey.myddns[.]me,<br>themiujoo.viewdns[.]net,<br>tsuago.servehalflife[.]com,<br>tsuagos.servehalflife[.]com,<br>unipedu.servebeer[.]com,<br>visdpaka.servemp3[.]com,<br>visual.webhop[.]me,<br>wwl1764.ddnsking[.]com |
| Filenames | SearchFilterHost.exe,<br>msfltr32.exe,<br>MySnake.EXE,<br>KOREA MARITIME & OCEAN UNIVERSITY.chm,<br>SPM_(협력사)_사용자매뉴얼_v2.1.chm,<br>세종대학교 DID 연락처 Ver1.0(202103 현재).chm,<br>서울기독대 전자출결-웹페이지 교수자-메뉴얼 Ver1.0.chm,<br>2022년도_기초과학연구역량강화사업_착수보고회_개최_계획 Ver1.1.chm,<br>국토위 위원명단(사진)_Ver_1.2.chm,<br>비젠테크_Seculetter_제품소개서_2021 v1.4.chm,<br>통일부 남북경협관련 법인 연락처_Ver2.1.chm |

## References

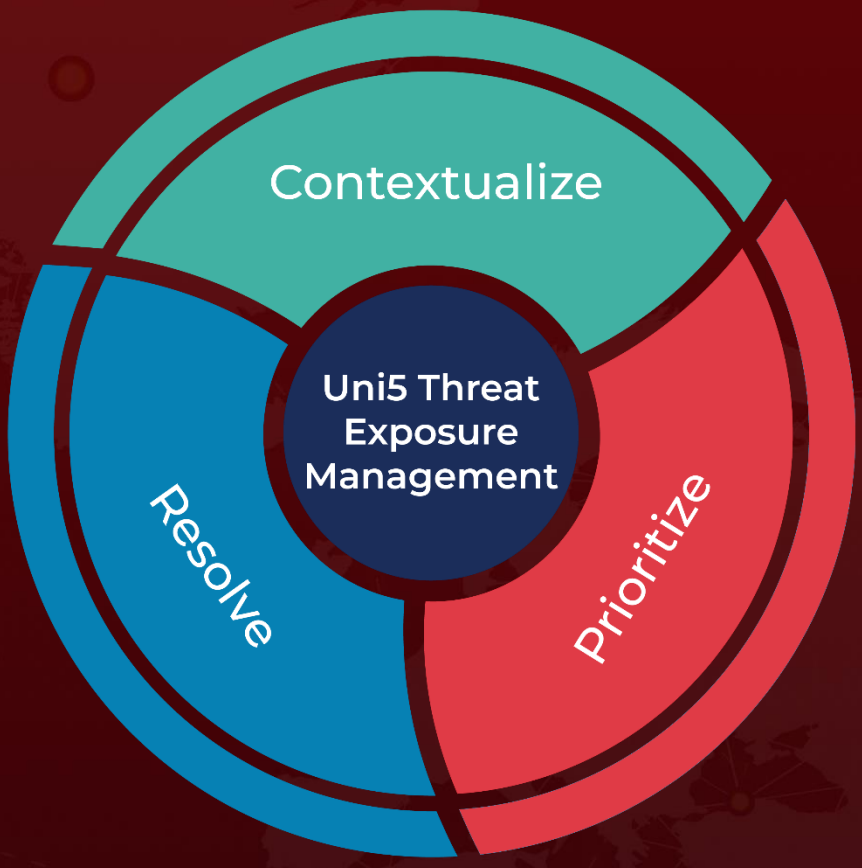

https://go.recordedfuture.com/hubfs/reports/cta-2023-0919.pdf

https://www.hivepro.com/tick-launches-attack-on-east-asian-data-loss-prevention-software-company/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**September 27, 2023 . 7:15 AM**



More at www.hivepro.com