KPMG Cyber Threat Intelligence Platform

TAG-74 – Strengthening Capabilities with Bisonal Backdoor

TAG-74, a Chinese cyber threat actor with clear ties to Chinese military intelligence, is known for conducting cyber-espionage operations across various sectors, including academia, aerospace & defense, government, military, and political organizations. Particularly concerning are their activities in South Korea, Japan, and Russia. Recent campaign indicate a strong focus on targeting academic institutions in South Korea, aligning with China's broader espionage objectives. Additionally, there have been observed shared capabilities and close collaboration between TAG-74 and Tick Group operations.

Initial access is achieved through Spear-phishing attachment, to deploy complied HTML(.chm) file in Victim's system. This HTML file consist of three components: first contains a legitimate executable vulnerable to DLL search order hijacking, with filenames like vias.exe, LBTWiz32.exe, and ImagingDevices.exe. The second component involves a malicious DLL loaded through DLL search order hijacking by the associated legitimate executable, creating and executing a VBE file in %TEMP% (custom ReVBShell). The third component uses an HTML file to display a decoy document, decompile the .chm file via the native Windows HTML Help (hh.exe) executable program, and execute the vulnerable legitimate executable to DLL search order hijacking, directly or via the RUN registry key. Subsequently, the Bisonal backdoor is employed, providing advanced capabilities beyond ReVBShell, with multiple instances communicating with a C2C server. Infrastructure relies on a Virtual Private Server (VPS) in South Korea, utilizing Dynamic DNS and Base64 encoding for C2C communication.

Organizations should perform network log monitoring to detect unusual file extensions, implement user privileges restrictions and strong email filtering to safeguard their environment.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

TAG-74 – Strengthening Capabilities with Bisonal Backdoor

Indicators of Compromise: IP Addresses	
92.38.135[.]92	158.247.223[.]50
141.164.60[.]28	158.247.234[.]163
148.163.6[.]214	107.148.149[.]108
45.133.194[.]135	

Indicators of Compromise: Domains	
leader.gotdns[.]ch	satreci.bounceme[.]net
visual.webhop[.]me	sarang.serveminecraft[.]net
hanseo1.hopto[.]org	formsgle.freedynamicdns[.]net
jstreco.myftp[.]biz	

Indicators of Compromise: Hashes
e8aa5c0309cbc1966674b110a4afd83a
fe5ff901c39f1b6870420fdcb8d5f10f
760a173f8bda7d5f2338d914bbf7acc1
ca7af38cebee03940f0316007c6140a1
2d9c6802e09595cd5401d76caca8f012
819a87e6907a3ecc6572d764f6b68e15
f6166e1add95269deef6e88dadb90242
155ee81a981eb83199a8b6566971bbec
5243696add287708a9df0051fd167e84
5556dd9fefcc1cace18031e89d80554e
1ce5fa5da90ef94ec665d59affe2306e
622303ba7224abf3fa79073b82e5f10f
59f7a3fe0453ca6d27ba3abe78930fdf
d113a4d93d134f14c2d4791627b0a719
fca35201477c24780e5258c633f09c8f
54e8ef4a553687f5421256f9b792327c
ae68241ecfc7ad283dddd44cff51d2c0
ccf6f2a214515d1e744c84fa1a24070d
3a63ae3afa72f6f16708e90cd88b0c23
ce15b9ea6e3474d7c7cc487f3dee064743224305
46f98b34db8a733fdfe82b42cd4998142a779107

KPMG

KPMG Cyber Threat Intelligence Platform

TAG-74 – Strengthening Capabilities with Bisonal Backdoor

Indicators of Compromise: Hashes
6c6c1a192ce2bea2a8fdcb8a7b8697a1f54713ae
68d65b0b5e6f1132481198a177e9fc614abefd23
89ed14844a55810776cc13477409795900d280de
77be86b6b3a505f6c28b643d94cf9d05df220849
935bd676c8ff32805c67520193fa8a7301518369
04833839a29a7bb504bf2fad147548784d4611b9
5032c84e767ada99be8730d434ab06c0c8981505
636c36eb965b38021cf3cb02c98b41c0d0445293
ddbc119024cf55cac4920b49779c6d2dfaa6ad15
cf5a676f0e673c9a2eac47d462571083cdb896a5
7a29e8b959994183296d12603a54f5e117b4ff4c
ae5039ece2a3cbedc0817455408a80844faf7d4b
dfff4b97c0462252f2a6fa66a46e9e84edc72a41
a31332d8e142d883391c624b53484987bbe3bbbf
e1b36c1f9a0d7f524e760d7acac99e4268a48257
0baa92fe526b6989c7a340a1b8f6e44d4a1b219b
03d4cd888a415d8d409c02e13d1753002eef79e1
aa4ad5341a9258330abd732cbab3721d76764f1ff21a8f960622661d701a1a71
ae0f641dc9d33ee50990971104ef1c598e216693700be6b74bb1e9ef373af97c
6a59421fd225d90439b6a933458718cf43dbe518c63979e8980bc070c070558a
df7d584d56af6fcf3cca31ed0d3a4d34abd2c1019b8d223a230f8a78075a7d9a
078a8026f32b8d05258285dc527408388c651f6c3eaebc45f8bb3f4b42248631
beb09817608daba003589292a6cca2f724c52f756df2ef0e230380345d702716
ba07ee6409908384172511563e6b9059cf84121fcb42c54d45c76ec67cb36d7c
bf1d1f5157756529d650719cc531ec2de94edb66ae1dabd00ed6f4b90a336d9c
2dd7c9ea32f5b2a4d431fc54aa68cd76837f80bb324ef2e4e1e5134e467e35af
56c9235e55b1a6371762159619e949686d8de2b45a348aeb4fd5bed6a126f66a
dda47ba7a41c9a2f041cc10f9b058a78e0019315c51cc98d0f356e2054209ae5
cf5bbbcb3f4d5123c08635c8fd398e55e516893b902a33cd6f478e8797eea962
b3a8ea3b501b9b721f6e371dd57025dc14d117c29ce8ee955b240d4a17bc2127
9d10de1c3c435927d07a1280390faf82c5d7d5465d772f6e1206751400072261
0eea610ec0949dc602a7178f25f316c4db654301e7389ee414c9826783fd64c0
8073593a7311bc23f971352c85ce2034c01d3d3fbbe4f99a8f3825292e8f9f77
e1748e7e668d6fc7772e95c08d32f41ad340f4a9acf0e2f933f3cbeba7323afa

KPMG

KPMG Cyber Threat Intelligence Platform

TAG-74 – Strengthening Capabilities with Bisonal Backdoor

Indicators of Compromise: Hashes
0d6893c7a3a7afc60b81c136b1dcdfb24b35efab01aac165fe0083b9b981da7c
77fbb82690c9256f18544e26bb6e306a3f878d3e9ab5966457ac39631dfd2cb0
8f50f49e77ddcc7ef639a76217b2eb25c48f9ce21ae8341050d0da49b89b7b34
465c7c6a0f23ba5f928fc0d0cdc4d9f6ec89e03dcedafc3d72b3b3c01a54a00c
11cd4b64dcac3195c01ffc937ae1eb77aa2f98d560a75347036d54a1cf69a5fd
01e5ebc2c096d465800660a0ad6d62208a5b2b675e3700f3734fac225b1d38bd
a88ca28b0948e810d4eb519db7b72a40cfe7907ce4c6a881a192880278f3c8b5
89f250599e09f8631040e73cd9ea5e515d87e3d1d989f484686893bcecc1a9bc
0ea0b19c562d20c6ac89a1f2db06eedcb147cde2281e79bb0497cef62094b514