KPMG Cyber Threat Intelligence Platform

Silver Dragon - Covert Multi Stage Espionage

TLP : Clear

KPMG. Make the Difference.

Silver Dragon is a Chinese-aligned APT group operating under APT41, active since at least mid-2024. Its operations maintain a clear cyber-espionage focus consistent with historical APT41 activity. The group has recently added new capabilities, including custom malware that uses Google Drive as a covert C2 channel to hide traffic within legitimate cloud activity. Silver Dragon primarily targets government ministries and public-sector entities, with observed operations across Southeast Asia and parts of Europe.

Silver Dragon uses multiple infection vectors, phishing based LNK delivery, AppDomain hijacking and Windows service DLL hijacking to gain initial access. The latter two rely on a RAR archive containing an installation batch script and encrypted payload components. In the phishing chain, victims receive LNK files with embedded PowerShell that extracts malicious payloads, drops a decoy PDF and abuses GameHook.exe for DLL sideloading BamboLoader. In the AppDomain hijacking chain, the installer copies a malicious dfsvc.exe.config and loader DLLs, redirecting dfsvc.exe to a .NET loader (MonikerLoader). MonikerLoader decrypts ComponentModel.dll using an ADD-XOR routine, reflectively loads it, and executes shellcode in memory. In the Service DLL hijacking chain, the script deploys BamboLoader and registers it as a service DLL by hijacking legitimate services through registry edits and service recreation. Across all chains, the decrypted shellcode loads a Cobalt Strike beacon for C2 and lateral movement. After compromise, the actor installs tools such as SilverScreen for covert screenshots, SSHcmd for SSH-based command execution, and GearDoor, a .NET backdoor using Google Drive for encrypted tasking, plugin execution, and file exfiltration.

Silver Dragon's highly modular and loader intensive tactics show the group's mature capabilities while highlighting the need for behavior driven detection and strong defense-in-depth.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version as per the OEM and secure it with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

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

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Silver Dragon - Covert Multi Stage Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Domains	
oicm[.]org	wikipedla[.]blog
bigflx[.]net	mindssurpass[.]com
ampolice[.]org	copilot-cloud[.]net
protacik[.]com	revitpourtous[.]com
splunkds[.]com	exchange4study[.]com
zhydromet[.]com	onedriveconsole[.]com

Indicators of Compromise: Hashes
00bd4de2bde0461accdd2e79279b08c2
2edd53b59f01931888d9d237871aa808
61bb113beecd0166ac2f2e8e027645fe
9fd54246d78eacdb02d8d830a27f95bc
0d1f1d68ae32ee8d51f8ec8f2676bfeb
e43f35f6cbb86a283bf2d8051d73b31c
8ee654d826ca5243e2ed1bc4d07f86be
ae72b2c870eb5cb9e01183c3cd301c7c
5f1928e8a644dab9fb294374362b045e
791de86ffaf47666e3dcf26c8f943f25
ccc1631e700763c4c31cd7540f2bf608
b0bae77341da2871b8354cbe22b39cf6
7728646e661df092f1e71735a711f05a
2a7042102cae68fce699e33cd78d847d
2524f644a0d731c252079870ec7c882e
cbdd29728b03f1da10e3dafd1bc5df30
1c66d075c3df801f92a24d99b3f69de3

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Silver Dragon - Covert Multi Stage Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
a5c9a0a0f09683ccdcc56b9ff284162a
ae98807d74d87edfc35140d507420874
14e9ef06501f14449e56fcb3471273ed
658a1cb18ad9a3450093ade1ef29f94e
e4b79d14ebbca9240e9d763ce90fe0e6
e3dcb68059e854af3b99bd4d1dc02e53
a53331b3562f12c84cb59c24d7641251
876e6bca4c322db479d00152a5c8231a
b2f9bf291261499f60fbaaaa2b50a4ae
5a654a8a336156d637abd8cedc2bb977
da1ac5b2ee326a66bfb233c89c1f1aac
0012f9f7bc6db810618fb914bfa87171
876e6bca4c322db479d00152a5c8231a
876e6bca4c322db479d00152a5c8231a
30bf9d8012bfe749eb6a5bed61e1c28605f92c1e
aac46d75d2f8fa09dd1d163cc47de944ff0438a3
79c18cf8ec7c5ee74f4d8d72503bedc2421c431e
5d8652119a6d99df52eda35924efa1d80f74de88
69c9474d942e314d6f71be59cbd936e765a7938b
62d2491ea2465f9d87afbc7ed1f5af8ca6601190
52da3171aafb4c3dda874b3ef4426c4b9813d487
d501f2ae86465f97470f2456b3e0c7b4cf7c4503
e0eb70574201880708664ff8db11dae75e6cf9d5
de50ee5a264d9b96028ab8c6a263ac302e3443d3
12e6dae26e015e5b50c8da16e63351cf2eb6b7a7

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Silver Dragon - Covert Multi Stage Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
ffd50936f8c0daf4531e0d12e93a81e917f7d747
8e5a5d99bba0d65d0e9fccfab06a052c85f2c912
8d543c5d1d1b8fa56c3fad1183e189880e934ec6
e963bebc16649ab219db780247505bc4cfa58e8f
9e2929816b418ff2eadae689bfde146d54e6f81a
64a94ff99d6569aaf7f78fb9aaab9c390fc6b1ae
8dbff1ef04ab461be37cdc8d9c947aff28b897fb
838b34d83e147c894fc56581b8fa2e74b3bf74fa
42598b390f4229710c2eac73b3f926c0c4f485c8
441ca1c9471c4de7417fe89e69bf120325c3a0f8
a294c76a2da9548c51fb662b42c0ab24126162d9
2885ad69943a957d3cefed7e4aa5b8ba704f8aec
49f4656ec33284e9d5d787c252f9b31cbc1d9e13
c093b163f86d35c7cc3f2966d4a5ec5f8ce77980
431bf1320725857a786895ded08837053ddf6967
02aff0938ab03440abc5c6a0b4a3fced24bbd019
ebb415e0d98e1367e66c964df5b0c0b766604b98
9160cda21fce14b188c0d33395ff7fb7170725a9
c093b163f86d35c7cc3f2966d4a5ec5f8ce77980
c093b163f86d35c7cc3f2966d4a5ec5f8ce77980
166e777cb72a7c4e126f8ed97e0a82e7ca9e87df7793fea811daf34e1e7e47a6
19139a525ee9c22efd6a4842c4cd50ab2c5f9ee391e5531071df0bb4e685f55d
2f787c1454891b242ab221b8b8b420373c3eb1a0c1fdcb624dd800c50758bbb0
3128bdb8efaaa04c0ba96337252f4cc2dc795021cbc410f74ace9dde958bac1d
3a2df7a2cfeca5ba315a29cf313268a53a22316c925e6b9760ead8f4df0d1f75

KPMG

KPMG Cyber Threat Intelligence Platform

Silver Dragon - Covert Multi Stage Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
3e2a0bafbd44e24b17fd7b17c9f2b2a3727349971d42612d55bbc1732082619a
43f8f94ca5aa0af7bfb0cc1d2f664a46500a161b2d082b48b516d084ef485348
44e769efed3e4f9f04c52dcd13f15cead251a1a08827a2cb6ea68427522c7fbb
4f93be0c46a53701b1777ab8df874c837df3d8256e026f138d60fc2932e569a8
51684a0e356513486489986f5832c948107ff687c8501d64846cdc4307429413
5341c7256542405abdd01ee288b08e49dcb6d1782be6b7bea63b459d80f9a8f5
568c67564d62b09d1a1bc29a494cf4bf31afddcafcf78592b178c63f23ccfcae
5ad857df8976523cb3ad2fdf30e87c0e7daa64135716b139ffdcd209b98e1654
72e4b6540e32b8b7aac850055609bc5afc19e29834e9aa6be29a8ea59a2c9785
7384462d420bdc9683a4cac2a8ad19353a2aa7d2244c91e9182345777e811e33
740a09fcdefa5a5f79355b720f54ff09efa64062229fb388adbccd9c829e9ff0
74a11a07d167f8f5c0baa724d1f7708985c81d0ac3d0e4d7ef3f3220c335e009
7f89a4d5af47bc00a9ad58f0bcbe8a7be2662953dcd03f0e881cc5cbf6b7bca8
85a03d2e74ae84093a74699057693d11e5c61f85b62e741778cbc5fc9f89022f
8c29f9189a9ad75a959024f59e68c62d42a6fd42f9eacf847128c7efe4ef7578
948468aba5c851952ebe56a5bf37904ed83a6c8cb520304db6938d79892f0a1b
967b5c611d304385807ea2d865fa561c15cde0473dd63e768679a4f29f0e4563
a6b5448ba45f3f352f5f4c5376024891adda1ef8ebf62a8fe63424fa230c691d
b93560c4d18120e113fb8b04a8aa05f66a12116d1fbf18a93186f6314381e97e
bcbe2f0a8134c0e7fce18d0394ababc1d910e6f7b77b8c07643434cd14f4c5d6
bd699ed720e2bd7085b3444cb8f4d36870b5b48df1055ec6cc1553db3eef7faf
c4de1f1a8cb3b0392802ee56096ddb25b6f51c51350ce7c45e14d8c285765300
ddaca57f3d5f4986da052ca172631b351410d6f5831f6af351699c6201cc011b
e3b016f2fc865d0f53f635f740eb0203626517425ed9a2908058f96a3bcf470d
bcbe2f0a8134c0e7fce18d0394ababc1d910e6f7b77b8c07643434cd14f4c5d6
bcbe2f0a8134c0e7fce18d0394ababc1d910e6f7b77b8c07643434cd14f4c5d6

Follow us on:
kpmg.com/in/socialmedia