KPMG Cyber Threat Intelligence Platform

Nimbus Manticore – Iranian APT Targets Defense and Telecom Sectors

TLP : Clear

KPMG. Make the Difference.

Nimbus Manticore is an Iranian APT group, active since 2022, with overlaps to UNC1549, Smoke Sandstorm, and the Iranian Dream Job operations. It targets the telecom, defense, and aerospace sectors across the Middle East and Western Europe, focusing on Denmark, Sweden, and Portugal. The group uses advanced malware like MiniBrowse and MiniJunk, showing consistent targeting patterns and operational maturity aligned with IRGC strategic objectives.

Initial access is achieved via spear-phishing emails impersonating HR recruiters, luring users with fake job offers from companies like Boeing, Airbus, Rheinmetall, and flydubai. Victims are directed to a fraudulent React-based career portal hosted behind Cloudflare, with unique URLs and credentials for tracking. Upon successful login, users are prompted to download a malicious ZIP archive containing a legitimate-looking executable (Setup.exe) and a malicious DLL (userenv.dll). Executing Setup.exe initiates a multi-stage DLL sideloading chain, abusing SenseSampleUploader.exe to load a tampered xmllite.dll via low-level NT API manipulation. Persistence is achieved through scheduled tasks and registry Run key modifications, enabling the deployment of the final payload. The final payload, MiniJunk, functions as a heavily obfuscated backdoor (an evolved version of Minibike), which collects system identifiers, maintains persistence, and communicates with hardcoded HTTPS C2 servers for remote command execution and data exfiltration. Meanwhile, MiniBrowse, a stealer, is injected into Chrome and Edge to harvest credentials and exfiltrate them via HTTP POST or named pipes. Both malware components use valid digital signatures, inflated binary sizes, and advanced obfuscation to evade detection.

Nimbus Manticore's use of layered obfuscation and cloud infrastructure underscores its stealth and strategic focus, reinforcing the need for early detection and coordinated defense.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper 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

Nimbus Manticore – Iranian APT Targets Defense and Telecom Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Domains	
gocareers[.]org	rheinmetallcareer[.]com
usa-careers[.]com	airbus.usa-careers[.]com
germanywork[.]org	airbus.germanywork[.]org
airtravellog[.]com	flydubaicareers.ae[.]org
traveltipspage[.]com	arabiccountriestalent[.]com
boeing-careers[.]com	acupuncturebentonville[.]com
careers-portal[.]org	cloudaskquestionanswers[.]com
healthcarefluent[.]com	sulumorbusinessservices[.]com
rheinmetallcareer[.]org	

Indicators of Compromise: Hashes
b19a097c237d594a85986881f69f127d
96a9078d97a8b2a0cdc6632b48b8a649
0c6f48c62d56b454ebc0e1b7e044ca69
be2bd408c615997c600871970573f023
b683628884cc1d00c234ea2f4b85d153
2dab429e52096fd9eb031fc666965a5e
e8e0f2ade7294808d86b23a989b21be1
fac805be171884ddbd1396f6a59c90eb
3a85381dd880c69f40b02859cd9fd473
b319d8972115895f156807348fa9b45f
223196939e1e1ba9256f515b0a510d7a
e16c8c285b1d537be5fe32e93247c282
68abbdd75f82a22e3cf6200e13a664b3
e23637423599434a6de45b9080b7c561

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Nimbus Manticore – Iranian APT Targets Defense and Telecom Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
53d0f4a75e8acbb6255bb44242e4843f
c4b95c1ba3671c5172e7eb01178a7c39
67dbe102978e4b612237ad3ee371702f
7d216c57da81193a45c67c323d4049c3
20e80c787e129ec11de9accdd0ae4611
cef266a5ea7ba57abc576cbeb5497c97
9e0ffbefdc7dee2663eb648ecf4f5d0a1ad521ac
2901ce6828599186c8a91162c29038984c43adab
9df7c1e7cff0da299c17459fce7fff1196ca2e4e
4ad8370951516dd311ebe7e024fdad3fd00e221e
0ffecfb8f6fe484b00ba3a185a3466841ecb9015
c81055c45d790fb59ed5e7d6e8bae73c2efb0e24
ed5f66bbb5967131d069ea70fbeed8ad233f7f99
845ae4cd37f84dfcc052d6647115a7952d0f9702
468351635537473aed8b85526f4b8d342f03c63b
8b4d1cd340c95f7ddfe8e0813949d4ea34f969fc
8356a79dcd0b240dae13b90252313bde218f3acc
6b83c47142a49001e51123bfc6de8f9db32d5729
edda7fb72a1302a5658ee279ddf90e0e32779310
3515136a3c4b307c8249215143cfb958c9aaf490
e8520f70af1114d89e8e26e9acab603c84ead981
78f12a684aac664b017682915bec1490bfa304e5
ceeb1881458dc24340adcfee54be3433b8df9d00
f764a6f6b9299394285db497e15686923e5b7e55
3a391427902c4b851e09aba4b5ea5d4036fcaeaf
b467efb7c41b41beb5f0a4d0e06983d7c66be014

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Nimbus Manticore – Iranian APT Targets Defense and Telecom Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
d84a9f9ad37561f870eb3375a7b324dd4b591b91
e812a52b63a45f6862bde5b65b2bdbea04de84b1
0502825fefef4d7150fd002413c5b638e2794935
c1ecaadde03b80cc6722f0b6ff289fdedd594abc
d5a9b90ee4584ed5c60914f3978a6c49671de912
bdeb5634d8d1eb1c1c870672ab9eb1f8411c25d5
2910168bdc05fb8279ae8eddb396144980d1d47d
64893ae79f18d6f2b67c7b1e83e57a8deb4e2f0c
037ba18395f80d7ff481f95412a3367d8553233b
d67a8fc7af7113d147f049a9b8c430f3563e984d
75a60296945a84d0952df5d1d07b21d90c5eb088
daa59b1a6e4ae62bfa91722fc0b2c26799864834
5bc4469b2466f4f26565538c82e0d5e08bc7037e
744390c471b9fe24831983ae7a23e9dd163e638a
6d66923725e711023d12ac092e5a961f52add6c6
41dfa13a9ea89d13da3a692795d00973724a2fab
b9b3ba39dbb6f4da3ed492140ffc167bde5dee005a35228ce156bed413af622d
53ff76014f650b3180bc87a23d40dc861a005f47a6977cb2fba8907259c3cf7a
b405ae67c4ad4704c2ae33b2cf60f5b0ccdaff65c2ec44f5913664805d446c9b
5985bf904c546c2474cbf94d6d6b2a18a4c82a1407c23a5a5eca3cd828f03826
0e4ff052250ade1edaab87de194e87a9afeff903695799bcbc3571918b131100
8e7771ed1126b79c9a6a1093b2598282221cad8524c061943185272fbe58142d
f54fccb26a6f65de0d0e09324c84e8d85e7549d4d04e0aa81e4c7b1ae2f3c0f8
054483046c9f593114bc3ddc3613f71af6b30d2e4b7e7faec1f26e72ae6d7669
95d246e4956ad5e6b167a3d9d939542d6d80ec7301f337e00bb109cc220432cf
9b186530f291f0e6ebc981399c956e1de3ba26b0315b945a263250c06831f281

KPMG

KPMG Cyber Threat Intelligence Platform

Nimbus Manticore – Iranian APT Targets Defense and Telecom Sectors

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
23c0b4f1733284934c071df2bf953a1a894bb77c84cff71d9bfcf80ce3dc4c16
0b2c137ef9087cb4635e110f8e12bb0ed43b6d6e30c62d1f880db20778b73c9a
6780116ec3eb7d26cf721607e14f352957a495d97d74234aade67adbdc3ed339
41d60b7090607e0d4048a3317b45ec7af637d27e5c3e6e89ea8bdcad62c15bf9
4260328c81e13a65a081be30958d94b945fea6f2a483d051c52537798b100c69
a37d36ade863966fb8520ea819b1fd580bc13314fac6e73cb62f74192021dab9
5d832f1da0c7e07927dcf72d6a6f011bfc7737dc34f39c561d1457af83e04e70
ffeacef025ef32ad092eea4761e4eec3c96d4ac46682a0ae15c9303b5c654e3e
c22b12d8b1e21468ed5d163efbf7fee306e357053d454e1683ddc3fe14d25db5
4da158293f93db27906e364a33e5adf8de07a97edaba052d4a9c1c3c3a7f234d
061c28a9cf06c9f338655a520d13d9b0373ba9826a2759f989985713b5a4ba2b
bc9f2abce42141329b2ecd0bf5d63e329a657a0d7f33ccdf78b87cf4e172fbd1
e69c7ea1301e8d723f775ee911900fbf7caf8dcd9c85728f178f0703c4e6c5c0
e77b7ec4ace252d37956d6a68663692e6bde90cdbbb07c1b8990bfaa311ecfb2
b43487153219d960b585c5e3ea5bb38f6ea04ec9830cca183eb39ccc95d15793
1b629042b5f08b7460975b5ecabc5b195fcbdf76ea50416f512a3ae7a677614a
f8a1c69c03002222980963a5d50ab9257bc4a1f2f486c3e7912d75558432be88
954de96c7fcc84fb062ca1e68831ae5745cf091ef5fb2cb2622edf2358e749e0
afe679de1a84301048ce1313a057af456e7ee055519b3693654bbb7312083876
9ec7899729aac48481272d4b305cefffa7799dcdad88d02278ee14315a0a8cc1
3b4667af3a3e6ed905ae73683ee78d2c608a00e566ae446003da47947320097f
a4f5251c81f080d80d1f75ad4cc8f5bc751e7c6df5addcfca268d59107737bd0
cf0c50670102e7fc6499e8d912ce1f5bd389fad5358d5cae53884593c337ac2e
3b58fd0c0ef8a42226be4d26a64235da059986ec7f5990d5c50d47b7a6cfadcd
7c77865f27b8f749b7df805ee76cf6e4575cbe0c4d9c29b75f8260210a802fce
d2db5b9b554470f5e9ad26f37b6b3f4f3dae336b3deea3f189933d007c17e3d8