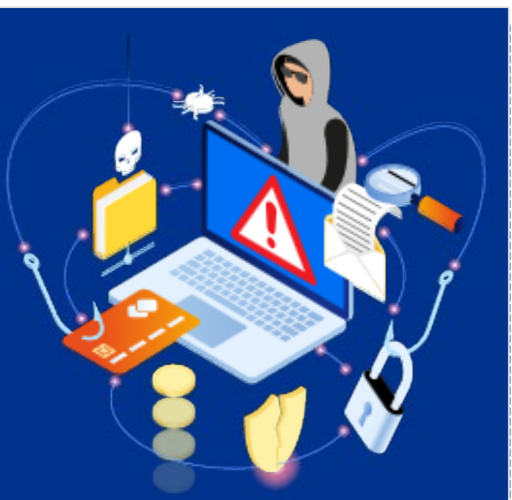
KPMG Cyber Threat Intelligence Platform

UNC1549 – Iran's Cyber Intrusion into Aerospace and Defense



UNC1549 (aka Smoke Sandstorm, Tortoiseshell), is a threat actor that has been publicly linked to Iran's Islamic Revolutionary Guard Corps (IRGC), has been active since at least June 2022, and continues to operate as of February 2024. The focus of this activity on defense, aerospace, and aviation-related entities is noteworthy, particularly in light of recent tensions between Iran and Israel due to the Israel-Hamas war. The campaign is targeting aerospace and defense entities in the Middle East, including Israel and UAE, along with Turkey, India, and Albania.

UNC1549 gains initial access through spear-phishing emails or social media with links to fake websites related to Israel-Hamas war or fake job offers. Backdoor payloads like MINIBIKE/MINIBUS arrive via compressed archives, often concealed within legitimate applications such as Microsoft OneDrive. These payloads often communicate with C2 servers using Microsoft Azure cloud infrastructure. Persistence is established via registry key manipulation or search-order-hijacking (SoH) techniques. To evade detection, attackers utilize tactics like hosting C2 infrastructure on Microsoft Azure and employing deceptive domain naming schemes. Conducts reconnaissance within the target network, observing security processes and virtual machines to identify valuable assets and potential targets for discovery. Credential harvesting occurs through fake job websites housing malicious payloads aimed at stealing users' credentials. By establishing communication with their C2 infrastructure, attackers maintain control over compromised devices and exfiltrate data.

UNC1549 highlights the importance of proactive defense strategies, combining user education and technological advancements. To secure digital environments effectively, organizations must remain adaptive, emphasizing the need of enhanced cybersecurity protocols.

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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

UNC1549 – Iran's Cyber Intrusion into Aerospace and Defense

Indicators of Compromise: Domains	
1stemployer[.]com	xboxplayservice[.]com
vsliveagent[.]com	cashcloudservices[.]com
birngthemhomenow.co[.]il	jupyternotebookcollections[.]com
notebooktextcheckings[.]com	

Indicators of Compromise: Hashes
01cbaddd7a269521bf7b80f4a9a1982f
054c67236a86d9ab5ec80e16b884f733
1d8a1756b882a19d98632bc6c1f1f8cd
2c4cdc0e78ef57b44f11f7ec2f6164cd
3b658afa91ce3327dbfa1cf665529a6d
409c2ac789015e76f9886f1203a73bc0
601eb396c339a69e7d8c2a3de3b0296d
664cfda4ada6f8b7bb25a5f50cccf984
68f6810f248d032bbb65b391cdb1d5e0
691d0143c0642ff783909f983ccb8ffd
710d1a8b2fc17c381a7f20da5d2d70fc
75d2c686d410ec1f880a6fd7a9800055
909a235ac0349041b38d84e9aab3f3a1
a5e64f196175c5f068e1352aa04bc5fa
adef679c6aa6860aa89b775dceb6958b
bfd024e64867e6ca44738dd03d4f87b5
c12ff86d32bd10c6c764b71728a51bce
cf32d73c501d5924b3c98383f53fda51
d94ffe668751935b19eaeb93fed1cdbe
e3dc8810da71812b860fc59aeadcc350
e9ed595b24a7eeb34ac52f57eeec6e2b
eadbaabe3b8133426bcf09f7102088d4
ef262f571cd429d88f629789616365e4
816af741c3d6be1397d306841d12e206
c5dc2c75459dc99a42400f6d8b455250
05fcace605b525f1bece1813bb18a56c
4ed5d74a746461d3faa9f96995a1eec8

KPMG

KPMG Cyber Threat Intelligence Platform

UNC1549 – Iran's Cyber Intrusion into Aerospace and Defense

Indicators of Compromise: Hashes
f58e0dfb8f915fa5ce1b7ca50c46b51b
0a739dbdbcf9a5d8389511732371ecb4
36e2d9ce19ed045a9840313439d6f18d
aaef98be8e58be6b96566268c163b6aa
c3830b1381d95aa6f97a58fd8ff3524e
c51bc86beb9e16d1c905160e96d9fa29
a5fdf55c1c50be471946de937f1e46dd
ec6a0434b94f51aa1df76a066aa05413
89107ce5e27d52b9fa6ae6387138dd3e
cb5f9111abc6c74f507fd6a6c3c6608279105177
39f4849cc0b18d3d40b2e010d914d1602cc2ad26
d767cc57e49571bf0886c71f84ce35003e1561a1
e7416baccd1e6cd2260d9a94f81ab4e51c7d752a
98c9882f79dec194e8b549e8dbb88af1170673da
8840e0d44be9e9c779606f0f712e9d136680cfa0
a93ffd73353a9b9f6d865562d92bb6f14a9e1628
f02d553ac98e14df9b04b86aa56dcb87b8c7162d
a53b68a8dfac4438c66393065c2f9a1607bae4c4
7f307bc0c220dff65d809f3b5f06d959a331fc8f
7ba787b9840169db4c6863eee4387bd908fc0cc2
c5fa1dc0a76bed67f1a1a9bc943b39ef6e4ed104
9958083f74f9895c67b47abde61ae002a997e4a3
b7f3a570426417c7cc013a248bea945cac57d898
deb66759d359b165a37c926d916cc0d4198986a5
6ea6238a661bfd4465379889e5a750823593c30f
3c8b1a7148f9e5278b50f5f9bbcafabb938c38c8
338be8e1d845b9a51d6382fa83cba49b708732a4
f0f37af7a4a31718b1e55bd23916f4d3b4d3a7cb
852d0e2a8f1b4933f5ea4cc966f4344226cacba9
89443c286910456773f7d82998e74fbeb4e4b119
88af8a53758afde88aa5326e69ca3d4e745c2cfb
ff1c547f22708d27688d412006c9c0b357d2eac5
0ead4133b81cb9f68077df1f3cb9c3ca26a04cc4
a3218432f34aaeabe253d07efab27bb7fff2061c

KPMG

KPMG Cyber Threat Intelligence Platform

UNC1549 – Iran's Cyber Intrusion into Aerospace and Defense

Indicators of Compromise: Hashes
d9d513e6ddfe9e83df4540deed3c421f80c5ec41
9acb977f13fce7ec38275887ddbbc0f42532e907
44b6974fd91cfeee47b51f37b658f64726d56713
612d7bf177a89aa2078238318d484bea209e43f0
5ce26492b2d536f709b68c70771896c2dee7c97b
3cbd593f9a01bf68a7a3421565f22e791a3bf3d9
0d40b2b9ff14e8db7bd2f17c40160e7af9b2bcfc
ae99ef9475cf553e3396419f08faec8b7965cb1fdd2f08d42dd190e376c445e0
042f44b403997dda7e6dd769847722798b7d0e5e7cd981468444a3cbe56f5705
0bbe40e99636478e07fc2c8cc73262348009072c3286e2a705ba0e4cbc0c25cd
75623550fd5722a448739d81e8ac9be70ec9bb4c3bc8fcc61b11125afc660dfc
985967e245d8fbc722e30371c9ed48c3269ceaa6b9b9b80caf2b95c920c856c2
b01a2eac8cb4f8882e46b997b93c4f0bc0722dd4ac9d5725c7652dc2d9ad6b64
4c2091325eedc12f25e3b4b98af681ca0e4ea5abcb461c74e148c7db0f4ef185
be86b8559a84d97aa1cc9852e60a553f5164477bacfc69b7f3453ad37fb6fd2a
45d4c5562be69cc50e6b0728701a6c22dac9b3268a762276bbab67e5938ad90b
93b2e45c13ba5c785dfd9e21ad2f6fe7289470e8504a89ae4c352858f8510749
73bf3a5877a7fe16544d15670e3ece034e4826323ba555b3527ad4d061f44ec4
8e2429d70989bbdd2ea8842dce7c3d790ebe148490ee519b47767557f4a4a733
eb112ff6ca57aef272e81ff9f23b767095fb1b2ea8013cc9182d1586f12062b2
1c3180f60e4140ccd2ee8dcb793b5a81a7782c14e63bffd7ebd21272486737c3
457be9e546e54f54b26921dd57d426d2dc413ca1c7939ce00a5dc8efea257ef3
78065411e7e8eb205ddae7215a229b7c93bdca5d628670f89caa982238ac7eb6
326c0fa053a70138df4b84d82169191be143beff6eca498069d11e76e9872b38
ab0b602665b609392eacdcbfc6c1981f216c19f21e2156a55cf9998eab02227b
f2a797524acea6dc1247d170b84f64e79a5af2f8d0f80d865c014b30027e4048
27679b5a935882d53a50630b65c438252da32a645879f73efbda9739490000f5
4c2412b71242a6405ab33b3687223e43a421202b4837f6ede1ee80ecb3d31856
bdb460527ac7ef739a013083d2268381a1464b845a05b39a5b3d88ef89941c8b
fc95b67fa0664bf2d542f07120a3b51d47ff8eb55a94d00e16827eea26483206
10e9d1eaf24ad3c63578d89f8b887adb47700aae02da1532c4842428725e77d6
26ca51cb067e1fdf1b8ad54ba49883bc5d1945952239aec0c4840754bff76621
720afa3e1216a9eb68b66858d50de0326f52afa279ef9ee0521aee98b312382f
23f6cefdce551431675506cb1c438feb2c66d38d1c77ebefe0fd5042e677ff80