KPMG Cyber Threat Intelligence Platform

SideWinder Group - Targeting Maritime Facilities Through Phishing Exploits

SideWinder (aka Razor Tiger, APT-C-17, Rattlesnake, or T-APT-04) is a nation-state sponsored threat actor with a long history of cyber espionage dating back to 2012. The group's recent campaign reveals a significant upgrade in its network infrastructure and employs spear-phishing emails with emotive lures. It has been observed targeting ports and maritime facilities in the Indian Ocean and Mediterranean Sea regions, across nations such as Pakistan, Egypt, Sri Lanka, Bangladesh, Myanmar, Nepal, and the Maldives.

Initial access is achieved by sending spear-phishing emails containing malicious documents or links that appear to be from legitimate organizations. The malicious document/link retrieves a rich text format (RTF) file which executes an embedded shellcode designed to exploit vulnerabilities in Microsoft Office such as CVE-2017-0199 and CVE-2017-11882. Shellcode within the document checks the system’s environment to ensure it’s not running in a virtualized environment and if it uses Intel or AMD processors. If the system is verified, the shellcode decodes and executes a small JavaScript payload from a remote server. The JavaScript payload contacts a malicious URL to download further stages of malware or exploit additional vulnerabilities. The malware establishes communication with the C2 server, which might use anonymizing technologies like Tor. The downloaded malware performs its intended functions, such as data exfiltration or further compromise of the target system. However, the delivery infrastructure can still be identified via an 8-byte RTF document returned by the C2 when accessed outside the geofence.

SideWinder's evolving infrastructure and payload delivery signal a persistent threat, requiring organizations to adopt vigilant and adaptive cybersecurity measures to effectively mitigate risks.

.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

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

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

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

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in
Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

SideWinder Group - Targeting Maritime Facilities Through Phishing Exploits

Indicators of Compromise: IP Addresses	
2.58.15[.]61	89.150.40[.]43
5.230.68[.]124	5.255.113[.]149
5.230.35[.]199	5.255.112[.]194
5.230.73[.]106	62.113.255[.]80
5.255.104[.]34	91.195.240[.]123
193.42.39[.]34	194.61.121[.]216
5.255.104[.]32	185.205.187[.]234

Indicators of Compromise: Domains	
hyat[.]tech	fia-gov[.]net
slic[.]live	moittpk[.]org
tref[.]tech	semain[.]tech
afmat[.]tech	shrtny[.]live
boket[.]tech	silvon[.]site
dafpak[.]org	tni-mil[.]org
dynat[.]tech	aliyumm[.]tech
fujit[.]info	ausibedu[.]org
gebre[.]tech	comptes[.]tech
govpk[.]info	mfa-govt[.]net
jotse[.]info	tnial-mil[.]net
leron[.]info	paknavy[.]store
mfacom[.]org	dgps-govtpk[.]com
nbcot[.]info	session-out[.]com
neger[.]site	newoutlook[.]live
ntcpk[.]info	paknavy-gov[.]org
numpy[.]info	download-file[.]net
pnscpk[.]com	paknavy-govpk[.]net
gruve[.]site	paknavy-govpk[.]com
defenec[.]net	almightyallah[.]live

Indicators of Compromise: Hashes
9345d52abd5bab4320c1273eb2c90161
9a1c49322a9d950c047c2edfc781b778

KPMG

KPMG Cyber Threat Intelligence Platform

SideWinder Group - Targeting Maritime Facilities Through Phishing Exploits

Indicators of Compromise: Hashes
379edeaa9ed92ebe6091177417b2c751
3233db78e37302b47436b550a21cdaf9
d0d1fba6bb7be933889ace0d6955a1d7
2462db3be57df824f003f74d7a16cacb
8d7c43913eba26f96cd656966c1e26d5
d576cebe9f6cfd1d6e238e3540120dca
aced660097e6767c43f2c00033470b5f
15e0ac5a80a5849fab40cfac221c4ce4
3a6916192106ae3ac7e55bd357bc5eee
5cc784afb69c153ab325266e8a7afaf4
8f83d19c2efc062e8983bce83062c9b6
6c7d24b90f3c6b4383bd7d08374a0c6f
b67bbb2a9fdfc3e89e2ed4c32ef9eb54
056d1dc3032d04d7638c02056d5146c9
356f30ba570428a6d0896e3960de8b70
1c36177ac4423129e301c5a40247f180
d37e71880beb8f453553c778aa07718a
251ff44ae978e2140dd02f00b3f093a0
6fa501f6303fefe00c4bcd61f171f8a3
eb029e7b6d75ba082d539a4646efa55d
8202209354ece5c53648c52bdbd064f0
b7e63b7247be18cdfb36c1f3200c1dba
54b1157ce8045f2e83340dc5d756f412
5cca7559186d25707d70e91da6865fcb
6cf6d55a3968e2176db2bba2134bbe94
59f1d4657244353a156ef8899b817404fd7fedad
230911dbeaab0631c9df32fdfd8b726977866fd9
b0c489a139435bbdf7b565fa70733b7fda1c660e
d65c2f100acd9f42138661ee3620ff51471b4e1a
e127a783870701cdd20a7fc750cad4dae775d362
fcc2d69a02f091593bc4f0b7d4f3cb5c90b4b011
dbdc7073a29e53aa16340d0c3da22680168aea94
bf3bbf35ebaaa6cf622644443e034f76394e7957
79478f0831c8dbf3e5a761cd33826ec992676311

KPMG

KPMG Cyber Threat Intelligence Platform

SideWinder Group - Targeting Maritime Facilities Through Phishing Exploits

Indicators of Compromise: Hashes
38210349974efaf4d7aac78538d04aa2256e4e99
3f26b7480d1db1234b998c65fae542c6fee0ef21
97b1bf8f984ce9c17e48473409b9670741260ed5
d7086ef6bf35e1c360af522e3bc0e19fa6184b70
b8d6ec69b83954467c392b8fccdc60d4a459c718
832b42c85c885f66d32a02114ada50c24926f3a2
62657c83a39b44368c1f49b103830dc0890d768e
df0a9f12a51c88171ad1b65a462b83b2ef44c236
44c836f99f8b945830781d9580cb7f77bfafc843
85500978ed7a617eb1eaae873498523bb9cb0b28
c50caa49156a1ce5cfb2df20ab3a5292e81c54bf
33657ac7b0b7793c21a5a1ea6a78c72fa48857e1
48b9d48847ad58a55f1a8dfc5872962358dedc6e
45ecc1c56886dd29cdc7557dd8f5954f999f56a8
5120621ec0a2eecb692f8042d1f6789a8bb182d8
b3453e58af7d90949ef6843f380f5ccfa9b4943d
8e650ecbbcd710f32b859aa34feb340768ea04cb
c9a9160e6c03a5debc9f1947a74215d52c7a1af6
b4151487cff2c6f01d12d248c360846f433810a2
e4a8e4673ebfba0cea2d9755535bc93896b44183
683210af38ef15f1bacb67ddc42f085bee05cf35
53a1b84d67b8be077f6d1dd244159262f7d1a0f9
cc59e275491ab440577079d555fa215895845e8e
cedfa7843dd0d312f1d0a0dabf699de5273e7f58
1c28c495c6c8794afe594580fb2958874781698f
33f221579f95f623025b464f22a20da66be2b273
4e95a0a27ff336f1193acdd975a53a6f02ee3443
05ebfd620475269c1228f87048c237a276745f1f
b72ac58d599e6e1080251b1ac45a521b33c08d7d129828a4e82a7095e9f93e53
9572312a12605c6a6ea6447af6fc063f4196aeba523ed38ce2c5ff51c33d4831
ceb93ee3093dbf1a49918ede81055018d9c0f0945a97f904a16951010cfbce61
512a83f1a6c404cb0ba679c7a2f3aa782bb5e17840d31a034de233f7500a6cb9
006e5fe0c01712391c54319a9d1579d7208f3cfa9f49fe56a14d93f0d0e8928b
613068422c214b944c7b2e3fb60412ed99d35c9e18d53d45b16965c5a36f734a

KPMG

KPMG Cyber Threat Intelligence Platform

SideWinder Group - Targeting Maritime Facilities Through Phishing Exploits

Indicators of Compromise: Hashes
9ce32ce5e2b70fec7f749e7868d89a4e3e739fed9c75cd6c4ec6eafde4c3711a
142c6a4c7e9efbf6f3176df3ff218449bb4f7b2a69d60060e6339f1c3cc95d93
e21396bf5f9936310b4f53273db330a9620d78c1c744277b0e9126f0afdbc29d
0826f532664b25a60d6ff5f98f82b2a618b86dda21f7badd6b5ea7165f5ed44d
0e51c4f52b63e7ce231959168dbc4270b4fa451c58e3bd2081441e7d83915361
121648be6641269d626d4d2ad79d234c99b121e0e0588909c05ba870308d9bc9
15ce7d3c879975ca81777cf58f47409283e34ec1fe8e966fde608bc7eda16646
170ccf1225154fa0cd92a14219f0b912479cc4095203646c38a31bb78baafe9f
1a88ef58675971eb18eeb267b1be90594cd6c7ebddf1c67d66729fa3e68de323
4db0a2d4d011f43952615ece8734ca4fc889e7ec958acd803a6c68b3e0f94eea
4e3c4ea383e6ed5c00672e08adabe24fc142cd05c86830a79c15c90412a2f588
53cc8f46f10e4b3958834d75b15db3aa0d8c86a63b8bd3e6ac180c05ce27d748
542fb0e314df639a7eef7ff077ddfd9574e70fb5ed5cbaf31c44d97f77e0c43c
55a0bbde3e32c559715cdc9c7d30d003b9e14725a6369d30edef20c1ed6dd994
60017e193cfd0df017eb8d0cc5f4bfc49593d90430a3e89a287f6afb83672236
62f40035834c9811b5dcbfa3cbe0fd4e51d8678f3aca8fb0644b0a3043a1a362
7dca552bc38f54716c80eb2c4f1f35cf6e5b12a78a5cec8bf335453c1b433cfd
7dcf935a24039dff2d084f41ab8ca318b28c53c01f9de069f087b3be15457ba9
89d4d85592bf0b5e8b55c2d62c9050bfa8c3017f9f497134dbacbb2a0f13a09e
8af93bed967925b3e5a70d0ad90eae1f13bc6e362ae3dac705e984f8697aaaad
8b4259cb1619bcbf3f6760f0982d0a1d3c67aa26738a3d6f6788bf6c2a5410e5
921496822997485059ad137e7cd25060cbe6abc9466f2e33c1d7df01630737f4
931aee9ba0e51804cb354a3a41830721e41a0fab6758aa19a43eaf1abe621b4d
9d02bf092fdcf44a51ae6e264ec3e3e57afbe79622c92a797e33fb62ed495cda
a11fab6de2c5111833e9e4a6f69ce5dded17085a3d8ae21c7fcfa00d7e113c9b
a3283520e04d7343ce9884948c5d23423499fa61cee332a006db73e2b98d08c3
a45258389a3c0d4615f3414472c390a0aabe77315663398ebdea270b59b82a5c
a703c6772e8bcf7cd0aef05ecbee4c7f7f39371d45b42bf1030df2be5261717c
acbfbf6fd00fa347a52657e5ca0f5cc6cbcf197a04e2d3fd5dc9235926b319d7
b565bd60e9182746de76feeebe7f85902e22ee3a22d5d55a278be7340923806e
e1ae44d26899969d520789e23c777d6c07785da23454664ad12b2783946a617c
f1cdd47f7a2502902d15adf3ac79c0f86348ba09f4a482ab9108ad98258edb55
bc9d4eb09711f92e4e260efcf7e48906dca6bf239841e976972fd74dac412e2f
cd09bf437f46210521ad5c21891414f236e29aa6869906820c7c9dc2b565d8be