KPMG

Threat Intelligence+

Copy no Jutsu : Sidecopy emulates Sidewinder to confuse security community

Operation Sidecopy is a Pakistani threat actor that has been targeting Southeast Asian countries, the most notable being Indian Defense and Armed Forces. The threat actor draws heavily from the Sidewinder APT group's TTPs, possibly in an attempt mislead the security community, resulting in the name, Sidecopy. It is also believed that this threat actor has links with the Transparent Tribe APT group because nearly all CnC Servers belong to Contabo GmbH.

Active from early 2019, malware modules are developed after a detailed reconnaissance of the potential victim and are constantly updated to stay ahead of counter security measures.

Sidecopy utilizes multiple infection chains to deliver commodity Remote access trojans (RATs) such as CetaRAT, Allakore and njRAT. It has been observed to use four new custom RAT families and two other commodity RATs known as "Lilith" and "Epicenter". as part of their operations. Followed by successful infection, a variety of plugins, keyloggers, credential stealers and file enumerators are deployed.

One of the more well-known plugins, "Nodachi," is written in the Goland programming language and designed for stealing files from an Indian MFA app called Kavach. The malware uses malicious LNK files as entry points, followed by a convoluted infection chain involving multiple HTAs and loader DLLs to deliver the final payloads. It is clear from the ever-evolving methods of infection, ranging from LNK files to self-extracting executables, to the use of different plugins specifically catering to the victim's infrastructure, that Sidecopy is aggressively working to infect more organizations.

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.

What is KPMG Threat Intelligence+?

The KPMG Threat Intelligence+ approach is an industry defining, research-based capability for enhanced visibility into cyber threats. Our machine ingestible feeds are the result of automated, sensor-based intelligence metrics with dedicated, expert analysis of each threat to provide you the right context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP. These feeds are additionally co-related with out industry partners and independent researchers to ensure you have the most accurate and contextual data. The intelligence is then curated from Strategic, Tactical and Operational perspective to give you 360 degree 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.

Range of services
Strategic Threat Intelligence Report
Machine Ingestible Threat Intelligence feeds
Threat Intelligence driven pre-emptive Threat Hunting Exercise
Cyber Incident Response Services

Contact us

KPMG Cyber Response Hotline : +91 9176 471 471

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

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

Sony Anthony
Partner, KPMG India
+91 98455 65222
santhony@kpmg.com

Chandra Prakash
Partner, KPMG India
+91 99000 20190
chandraprakash@kpmg.com

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

Rishabh Dangwal
Associate Director, Cyber Security
+91 78277 54752
rishabhd@kpmg.com

KPMG

Threat Intelligence+

Copy no Jutsu : Sidecopy emulates Sidewinder to confuse security community

Indicators of Compromise

IP Addresses		
167.86.83[.]29	161.97.142[.]96	173.249.50[.]230
161.97.90[.]175	144.91.65[.]100	164.68.104[.]126
149.248.52[.]61	144.91.91[.]236	173.212.224[.]110

Domains		
Amsss[.]in	imenucard[.]com	scout.fontsplugins[.]com
Appsstore[.]in	Securecheker[.]in	Eurekawatersolution[.]com
Afrepublic[.]xyz	Vedicwisdom[.]in	Vmi433658.contaboserver[.]net
Newsroom247[.]xyz	Republicofaf[.]xyz	vmi281634.contaboserver[.]net
Scouttable[.]xyz	iiieyehealth[.]com	Rarebooksocietyofindia[.]org
Securedesk[.]one	ikiranastore[.]com	Maajankidevisevasansthan[.]org
londonkids[.]in	Afghannewsnetwork[.]com	

Hashes
5e804c0a24a5f471635bed760fee8bba15a3d69fc6ddac306ef0da364b58aa34
91cbd850c6ac25ad762eb256ab432c45af78737cb3fb042f6fd8b3ece9a96dfb
Ee58d8ecc5dce13f4eee1e6164654f82a5eb339dc3c6e023b69ea7d6df5b930f
75033494867c133e7470c348cc36da13b18aa20d13612619540a9a909aa29f48
4d6488a7db35e0447f6fe44e94f26773cf8666c7071ec27257daeca7bd72bab1
De6d22103f4d655614d5c8cb7fa6350486edc08a80da48b20a3c83ec45bb7aba
df542d57b80c6bb0cdfff0e009ed410e4241d91624cb7b38c1b806bd6df103d8
54759951089f44a3918e164b8bf29c8f388cfd41f9930f81b8103852947fed93
b220804279422bd5e6150e93bea68ead6648f92fc192fe26df9ff77efda1b319
a55d19aabd1b56c5d583311da142314df09400b7a1eea4dcd49474524a8f879b
24469a7f1f33cdecf507824a773814b5f3190c81acaf04d06c168ccbf71b2ee8
49796c18a09c100118b7d678dc76bea283a70d6ba695224db9364ff740597103
124677d655b829892bfe73877ca2a2289bbf623cf404ae50f73f255866205adc
16e153921beabc0bc5bc1b161e19afb14e39cfe9991dcd04f20a923ed1d27989
bb5733aaea12b3d0f38eccb5725fc0fa5e56d0a6462f0eb4228c3d34a177e1d6
7f800784b00354dd15eee129317a63bd3f7bb25622e898c873603e5b142cbb09
b74e20c912e5c1529ec73bcd89776d4f81e56663edcfaccc82ecac50e34d5284
df47ca45bdf2f910a0ebae49d29549240066f77d0abb735cf1afe41368cb0d85
e16153ee38bc971c4fd94f4d35996d0ef41a33bb53d5028170da48712904a3e7

KPMG

Threat Intelligence+

Copy no Jutsu : Sidecopy emulates Sidewinder to confuse security community

Indicators of Compromise

Hashes
1a2cf862d210f6d0b85fbf71974f3e1fbe1d637e2ef81f511ea64b55ed2423c7
8a10797ac7f84d09cfb4cb3a6a1e75473dc81dab757c0000036a861575216e5c
907f594f49e498f0526684e03afd76e953b46b2c4947dd260f90f2665b7ff875
c54cde89abbc781c3c435b2bc2a71189a78f34cd4dfa3a0e804eea407d14c944
caed359105265eac5e9628548c95a898c3f8d0e427354eaa6ec3a2acb3515c83
a8c75aaf566c230b2e006e36209bda758864ef990b5e324c338f12ec3b1e9d3d
d11fdc8146e3ed7669601b5a787843542711f6f4d0a728aecbf855a787e1b148
c073355b2b6b41fa7bba206e872df1439f63c8bb4bcd85dd4e5e076e4e466f0a
772dd3668bb5449a6e83b94103335f890423e1f7206963f79f4b3b77ea9d4bcd
f0431adfc5921c02cfdcd4b86a1f5b56fe4763556227686ffff41e2a602af93a
74ce70dd77d6f8a8c22ec4ce9af76c2a9d2c39f858a3b0610b6d1598aea38548
fb48d1a60ad9dd2325ea161cacf84355185fc33aed8b08a415d0098cb1c4560a
660427971b04313c2ebf2410f9ba4f67c5f1d8ecc472be6c709546a12dc97f7d
f034db8f1e05edaa8b5c9fcd6f2987cb8cbb480a3793b9d67c3ff1d3c25f2b68
a00813028306c519829ca3b2f16357124aa77b998c9c6cc6f16c00c24503eace
0b68637be6ecc8f66bd68dd5a4b669f15aeeeb66a873e7b8caaad575b4215aca
0409094e0075f146a84cae1df4404262cb0de371863d1b3dde45b0b69f8c354c
3534eec1bcc94e717060c4fd4ed249cff77b6ce20c3be45061c8d9717c53da44
e2428029a07f6964fb945acda1f3f72852f5fc9c85924420fa0bee63d2370659
4749dc156be23be1e49dc2e48bfd370048c3d46e2be08b8b108088c5ea695fdb
931f50af89987aaf7f4e85516e42ccdd7d3c9bba2d51b13324fef184b14d96ef
d96014c5357a338aa2659822bea02d1901985a84a0bee8dce11686993df015c7
6ed9dc3f18d676b66cf4bb583c31137267ea6b8652f14eb44df47a49b45da3d8
f927d3aec7a84b45d8b6e4f871cf4d4c462143079b31f7d07214754cfb04cb0a
0a52ba42fae2876b014c5343935df94de0659272df2ec9a018a3015fbaa7f5d2
f0bbc9b2ae7ad32636c6c0ca2b95eab4b3e0498daac5175b44cb42b369fc7366
72b0004a0d4551a43d5ce30a6cc733806ac0fa2220cb42857cb40f183eec31ef
6e7cb476f8ad98f64ec4b3633aa600aeb0dfe20d964b22c2dba35b7e3fe6d944
3972fe894765a9262e401d7e5e9a23d042655265bf8f4944b91ddbfcbbdba45a
65ae52ac448a011701c4f077449112329b79f23f758524dd753dfe757c52f508
05c129e088486b1b9c8f8728fdd8081363f6c58f2db5fe2e34cf01913bdf08dc
f889d2358eec85212659b0d273e5e892e610e114c990bfde93c9d607d85f58b0
234defc7e28089ce81141907ceb16f3c80b12b6c19a4516d97f049ec66af633d
bb1e62f812c67a049d7148e609f9abc4047e07ba942446628cc7149f517afd34

KPMG

Threat Intelligence+

Copy no Jutsu : Sidecopy emulates Sidewinder to confuse security community

Indicators of Compromise

Hashes
353b9177483c499c806a604299ef28e655f5647e039a408e4226bec650bea2d2
6afbb8029cb52890b4d8893029b789dcbcd86aace059e50c4c6ed12dc4364a4a
62124b7d418a3defd0b33e3c15c4cee7c88808d2c7712768c25c304011652d4c
3da037462cda8dd0e32999798c70bbc699d2d6fff34d9dbc20066c4aa2c67543
9d7edfa9834f4c5b5b35c04c7906993c330fc0a29382a69f9601793211ccf253
cf16c7ece034eca4d6489f77d87a7100ba3b4721678bde3bf2e54a01dd4ecc51
f08fdfc993072272f4b3945800d50558e03ae532af7099b8d86e467cb522f0bf
01f14a8749b2022fb72334b9d10a06a5ef8921f3f38fe4a3f78ca78cf23d3e5e
5b3f238fa7392e6e5a35d41f0b3f2eff7fce70547d0572df7ef8bf46e07d9a9a
3dfa7180dcd674b26539687313e2e80d705f52dbe74163c40ae050e60488382a
1afb690159f041ce4f0af3618ebd1cef4597d3d94bd249c4644b8e359f46199d
f17fd9ff93d1b3db6c3e4463d5ca5c11b99827890c58721d2860df75d4323705
84609f9e443225a23cca8ab6be910c207d220bb430fd543d0724eaae8f7df592
c79ab21cf7fc23b9a096c4d9aa5b7cd02d968b8dfc58b137c2df44b1e55307b6
a90605c2c755558778d3200d52496229951c0cbb7d13b2ce8f75d9ea7d738bf1
6d4f18ec7564d4e1abcd0c6e4697f9cd029fba5fb4889d647dacd938d9aabb65
2545fcbee4cdb94cac171f8242bcfe1b2cdd048864c6f47ce0386d701918104e
7d6822107e82ad3fee7b901e4e74bc9f885892da1a1378e63f8cdeaf651b4f49
7bf2d1167b4cd57a72aa1c34b2c3f978ed42569ff0494411af164b1ead715466
2bcd8fd2292b57cb0e093bd723d70560aa49c50bc3f34e9f1ff9ba66ac3f5cee
B0942f024982da62053fa5c469b02ccdc2ceb16290a07bb2eae01d9a42b55452
3f34c61025b5cf46075d79e68efb5da0f4ac01c113d8c1aaff3903ccd9a0fa3e
fa02de1f2dbd29f19e8ab0ff2931b063bd8f8ccadf0d7e321f0a02d2e2f86419
73a2df93ded57d1ddcdc9091eeded169668d8abbe7e8e35b7a737c01fceffa59
1e488c21314be1a976218e39c90ee17902636508e6e97754152b3bb14f5af062
c5b93a7a94b80d1548f09bce173ef20b5675cf39f479d923e670ba0112b3ef13
59fcc32fc7f64db71b868cd5bb674da5604cb5da032c8329e7183437c2d3936f
19e680eaa52c0ad14274b04141a8e172d2ec1a01a3f429263090a990120ad9df
353b9177483c499c806a604299ef28e655f5647e039a408e4226bec650bea2d2
6afbb8029cb52890b4d8893029b789dcbcd86aace059e50c4c6ed12dc4364a4a

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.