KPMG Cyber Threat Intelligence Platform

SideCopy APT - Targeting Indian Defense Organizations

Active since 2019, SideCopy is an APT serving Pakistan's interest, targeting South Asian countries, particularly India and Afghanistan. They're known to target Indian Government and defense organizations, exploiting vulnerabilities like CVE-2023-38831 in WinRAR to execute malicious payloads like AllaKore, RAT, Double Action RAT. Recently, the group deployed a Linux variant of Ares RAT, emulating the tactics of APT36, known for its focus on Indian military personnel. Alongside spear-phishing attacks, compromised domains with repurposed IP addresses are also used to spread malicious files and info-stealers.

SideCopy APT utilizes advanced social engineering to lure officials and extract confidential information. Initial access involves spear-phishing emails containing archive files with malicious LNK files linked to attacker-controlled servers. Upon file access, LNK triggers a remote HTA to drop base 64 encoded decoy PDF & DLL, and fetches information about the installed antivirus software. Upon execution, it beacons the same C2, downloads another HTA (in the TEMP folder), and drops malicious payloads. Multiple payloads like Allakore (keylogging), Ares RAT (Remote surveillance and control), PyInstaller, and NET-based tools are used for system infiltration and data theft. Establishes persistence by adding these payloads to the registry key or startup options (Windows) or via cron (Linux). Once persistence is established, the malware enumerates the device, collects data, encrypts it using RC4, and connects with the C2 server. The C2 server commands keylogging, screenshots, file download and execution and data exfiltration.

SideCopy APT has thus emerged as a cross-platform threat, targeting Indian government agencies with enticing honey-trap baits. Vigilant monitoring is crucial against their persistent and targeted threats.

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

KPMG Cyber Threat Intelligence Platform

SideCopy APT - Targeting Indian Defense Organizations

Indicators of Compromise: IP Addresses	
144.91.72[.]17	149.248.52[.]61
103.76.213[.]95	162.241.85[.]104
89.117.63[.]146	185.229.119[.]60

Indicators of Compromise: Domains	
filehubspot[.]com	afghannewsnetwork[.]com
mailupdater[.]net	freewindowssoftware[.]com
digitalfilestores[.]com	

Indicators of Compromise: Hashes
eb07a0063132e33c66d0984266afb8ae
8bee417262cf81bc45646da357541036
9e9f93304c8d77c9473de475545bbc23
9379ebf1a732bfb1f4f8915dbb82ca56
49b29596c81892f8fff321ff8d64105a
75f9d86638c8634620f02370c28b8ebd
fc5eae3562c9dbf215384ddaf0ce3b03
a52d2a0edccdc0f533c7b04e88fe8092
02c444c5c1ad25e6823457705e8820bc
d6e214fd81e7afb57ea77b79f8ff1d45
d0c80705be2bc778c7030aae1087f96e
31340ea400e6611486d5e57f0fab5af2
fe0250af25c625e24608d8594b716ecb
c872f21b06c4613954ffc0676c1092e3
ff13b07eaabf984900e88657f5d193e6
6f37dacf81af574f1c8a310c592df63f
9f5354dcf6e6b5acd4213d9ff77ce07c
ccb6723c14ebb0a12395668377cf3f7a
acec2107d4839fbb04defbe376ac4973
f759b6581367db35e3978125f4f6ff80
b6fbcae7980d4e02ce9ed9876717f385
7cba23cfd9587211e7a214a88589cf25

KPMG

KPMG Cyber Threat Intelligence Platform

SideCopy APT - Targeting Indian Defense Organizations

Indicators of Compromise: Hashes
63789cacecc1abd9669344516adb4120
9b06472e5acf2311d0af62d638a8e51a
d129b81c1d40c34ac628835e144a4740
ba2ada448b8471789c0ef3b3345597fe
6b3f45f7a6758d198a317de43d51e669
a65eb385c9019c712ea513e4c5c25152
1a1c8c0f5cafb7df661086bcb804154c
0c44da9103fb26dafc710e83e95ad1c2
61427f7a200d7a21c1cf38ffe2fd4ee5
441f580a36757cf20493029b055f581e
c46a7040ec21a423ba865233868e07306c3f358b
dfc0e3db563a426be543757aa2720fb2993667b9
a160457c20887db9181318029c704475a5aea7b2
188a54a0da9e1ad21095b0490436626c822288df
09e984201eda4680c2d238093900f879c682a87d
f671a8f290c8eb78bf4866a014363fb31099c037
08d5930079fffdb279b407d40b0607be1e3188bd
918a868196c32711c1fa2a3d04fc93bdb73eef00
685b46074c9c8a43ebee713a91a03c1554f78e13
f583975158b1dcd5b45cd40727084528d4095589
760304f51c1c4693b6ec1bb2eac1e6fa3d48b7d3
42eb5f61005ba0761b86f1ff199181946ddfb14f
768a1b12bc9d010a107e955f934f5ef5bc29708a
9467ebf01e46250d69978d8506e943b9bb60564e
e6896a37807b6a0b43b940b7d40c7e006e355cd5
db262f8bb99f795dd4178ba50251d3e8110c99b3
0152d75939164d228e20545a33f0f6e5f17e0f62
d24e7644cae64905960314747b774780e98b7859
7c81509a9b0b8cfe78e8a6db6bb9cb93fc0ab820
da99dcc6c240ea19e8a1379f53df96a823724e2b
c40ae6ecf256a8705922b7e198caa95de5c35b42
f6a4a5f9c5afc2a77decd5f848b3a2a411717760
ad3070dfeb982cc3ba90c5ab1468be7650d299b0
14a78abffa6b0912febefe51d58f780b2ce7632e

KPMG

KPMG Cyber Threat Intelligence Platform

SideCopy APT - Targeting Indian Defense Organizations

Indicators of Compromise: Hashes
0837020963d7c6d9ab59d44fd6739c4017ba4f2d
259f5ea19c5efaf628dbe4f33cbd2ea616a70a02
15741f7037339735ec22bef88a52cd5bedbf54a2
be4985d41c7edc8434d136decf678c9ed05af4128631b4b4ac4444248348af96
d3e245fd45e0373f147c1de8645dff6b1098c4ae469330f429a5902621a2eb85
5716244ce0f3bbae24b79db810e80cd5001b320e6608a838284b22889143ca66
295093ab3aa27403ba43894bfd9fa27a00661523ac626b991d18658cf21e391b
7d95e03424edfb67b067c1a4bf1dca2fac9a4eafb68f69b0594b633a3ccc5a51
6ffed1bb706a5eb205294f9287a9182d71e293b3b131415bfbe24b99e28ccd67
32c629af8f602f18b9bf4b557e9ecf6cfd81c62dc1fa103e269a3fa1e7233526
29465f87bd3e6731668f3d3020924db55dae04d8cec335088d49072013900685
be1df638f11f98f73610729008afe0fd9802becbccaddfd3706ffea10d17933e
47358f1f45fcf25b33d79ebf23770afd5cf6217fd58b44a87e9ff62db8c703a1
fe82d48663ca2c246c9dca724a1b641b5e35d0ec83bd5aba4246be9dd4b59427
c328cec5d6062f200998b7680fab4ac311eafaf805ca43c487cda43498479e60
5893b58d6a6a772f8ecd491a4dace11007fd1aac90e5f4a0363288d1376e1ce5
6935999ee4b2f88cf74ec299c24a212a2c4b0f95105fb773e920d88153eab3c3
9cbdcd0316bf10c4d9b969671dbc342bf71844f0e5d31b4a289951fe18ab3d57
b3e0e462c97cb6c737fc3f02588c09a66afcc28fd5f6bb7948e0aaea36ed84ce
c900af25405a5f4062ea99e88cef0ce26dc287899a4431896a7baffd31691d09
3d7eaa1f572e1b16f68d54d47e73fe38ae63bbe27fdff94ed3a1bab1febe62ff
1122e444eb6726986882c60c2158b11829d895a53b48cd7129c3fe0d74bb2c74
03fbbe79af672f9e4f62fb1be3c62bfc0bc6382f6f4f860e909419a20d679d5f
d225c8a14a04af6fd9004bdb11653ba23aca5d908b753f64c492facee9a9dcf3
9645299e58c7521d811fbdcdbd57db45160191db7c7b73eae5d97e4530136da8
61b898f4254d8c6d3d375584a1109367f9e86d221e2d404bf6768fb81b1b48b5
a9407fdee890615e8e4f4927deb0c32795e848ce58e66dab56bf3b7188bc0b25
db403abf7dcc5bccbedbb53eceef76bd02b440c1114a0b64e665eac1e44fa993
57e72c7c81df7d971db2977b51bc37447b641466917e7ed8f92efa3b0eb23f0d
7efea614cd6eaf338da6d788029fff8b7a62e17ca8dcf58c5932db045c358dc6
91185752db6a3b0fab5531d0190ba7c67df242ee8304a0a07d9f2de814b2f02b
c7ab0b7004a757216b47bf61bd099c4e3e95436262fa2b067ec2c469f9fb1f65
3e094ecf780687c38cd3fe7533a2db276b1ee7724c2300dacbaaba25510b7971
b51bc30fccbc0297400b05ea4b573463846c55114a35060b09d38c53cf8d1c69

KPMG

KPMG Cyber Threat Intelligence Platform

SideCopy APT - Targeting Indian Defense Organizations

Indicators of Compromise: Hashes
0acfb2159191abf2998fedb2bf8679a0dce4cc41b324db72615b751f198150f0
0d11eddaf91966691b06ea164eca834848c5cc6276ef8a29ec67cad71ba386e7
8e9a414713b7b73c9d6b3e5fa6d8d9d201b80123f812c8263a0ece4ce58ce90d
eb1b12729274f84798bf83b779528095686f67330d80e39cb45791a7c6979910
ba06e43aeaad50e7196a44d8422eee85deba75754f891102bcd9bd6255b1e6ca
047f1575fe8b90e50168307e6547a76e873a1c8ff08d4e7b837c383751172f3e
c89806e27ecefa3a05ba84b2dd46b148aef007ffa0ef80f6b34621d7777fbd65
bca2ae73987fd0f3f9c7cd984c55b3a0881333ced9a666f375d684d72f082acb
d3b0efc4efbef68c3a4bbc9a71b95ed186b3511141597a38071c51e1a9ad01b0
f81d1c47a666d4ec32e69b3e1312dda62c932298e32cc42d5c0c6543589d96be
3ed1dc92e8399f062e5e62e5483a87736e51ad4ce651f0628abf98d5e10aee27
9aed0c5a047959ef38ec0555ccb647688c67557a6f8f60f691ab0ec096833cce
a2e55cbd385971904abf619404be7ee8078ce9e3e46226d4d86d96ff31f6bb9a
e88835e21c431d00a9b465d2e8bed746b6369892e33be10bc7ebbda6e8185819
85faf414ed0ba9c58b9e7d4dc7388ba5597598c93b701d367d8382717fb485ec
865e041b41b9c370a4eed91a9a407bd44a94e16e236e07be05e87de319a4486c
3adbbca5b4bc2a53e5ece41c885dbbe18bb4b0fd6a6c4f07204de99b4656c258
631d09ceb29aa9764ccc503088fa7df7111a1e6ec12e44a1182046efb33a6a15
a6d9022eff8fc6e0915d90a1fa8ceec29240f1dbd61f8f94182ef4c1371858cf
a3056045c26bd2b11e0b5aa5f2d3bbe89fe15edc0bcdfafe695e80eee48de932
73a0d6701ab7e71b7aa5a53383700d99626292fcd3c987bc85000e8ffdb7c392
eb5192d6e98e3d18c9491ae4d163d7b432489eb9d779b93ff3d4d8a52bac491c
6adde4444f2a249e027d3a234ce7c4071d4e4da1abcc89ea8059878ede7a4d38
4c53a7eb57407c93006e3c34d4243aa182cbb5836b38b994f1db9a8c5d0a6b33
947720245574759a836b12d9bf0c92fde7d0dc3119a0a4d13319d1d7645ac2e8
aa448d8ed36ca7782844344fcee0ab1e80fdf4950beda565cc00d9728f70e923
06daafd4c09594d660c2191b4a421564b492a7043e4db4e91827fbc732d068a8
93e96a9a139635989746f23566570975b448258c9261aeefe63c309fde0ef784
61f580b05b816ae880022c9c666c1e9531bb511075bfc2cb06742f9e3f2799fd
8453323dc06c2eeb9426bde653a3a4efcdc7c728319a92a73ed91d0e8165d1c2