KPMG Cyber Threat Intelligence Platform

ToddyCat APT : Both perilous and quiet !!

Exhibiting similarity to China-linked hackers, ToddyCat APT made its debut in December 2020. Primarily targeting government organizations, military entities, and contractors in Europe and Asia, this APT group initially compromised limited Exchange servers in Taiwan and Vietnam. ToddyCat APT has displayed a distinct behavior by using two never seen before tools, namely "Samurai Backdoor" and "Ninja Trojan".

In the first wave, between December 2020 and February 2021, the threat actor exclusively targeted a very limited number of entities, in which the Microsoft Exchange servers were compromised using an unknown exploit. This exploit was further used to establish a "China chopper" (a 4KB web shell) on the target systems, post which the threat actor gained full access to the remote server. This web shell then initiates a series of multi-stage attacks which involve "Samurai Backdoor"—an advanced passive backdoor that works on ports 80 & 443, and "Ninja Trojan"—a trojan cum loader developed in C++. Both these tools enable ToddyCat to bypass forensic analysis & basic scans and establish elaborate post-exploitation capabilities. In the next wave of attacks, the threat actor widened the scope of attacks and organizations in Indonesia, Kyrgyzstan, and Uzbekistan by leveraging the infamous ProxyLogon RCE vulnerability targeting unpatched Microsoft Exchange servers. The threat actor was found shifting its focus from exchange servers to desktop systems in the most recent round of attacks and is continually enlarging the area of attack evolving its tools & techniques.

This threat actor uses various techniques to avoid detection and keep a low profile, so the best way to cope with it is to practice multi-layer defense. However, the complete map of tactics and operations used by this threat actor is still unknown.

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 protected with multi-factor authentication.
- Conduct 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

ToddyCat APT : Both perilous and quiet !!

Indicators of Compromise: IP Addresses	
23.216.147[.]76	45.76.78[.]237
149.28.28[.]159	137.220.40[.]10

Indicators of Compromise: Domains	
example[.]xyz	eohsdnsaaojrhnqo.windowshost[.]us

Indicators of Compromise: Hashes
1ad6dccb520893b3831a9cfe94786b82
350313b5e1683429c9ffcbc0f7aebf3b
832bb747262fed7bd45d88f28775bca6
5c3bf5d7c3a113ee495e967f236ab614
5a912beec77d465fc2a27f0ce9b4052b
93c186c33e4bbe2abdcc6dfea86fbbff
ee881e0e8b496bb62ed0b699f63ce7a6
f595edf293af9b5b83c5ffc2e4c0f14b
5a531f237b8723396bcfd7c24885177f
8fb70ba9b7e5038710b258976ea97c98
bde2073dea3a0f447eeb072c7e568ee7
5cfdb7340316abc5586448842c52aabc
ae5d2cef136ac1994b63c7f8d95c9c84
33694faf25f95b4c7e81d52d82e27e7b
8a00d23192c4441c3ee3e56acebf64b0
5e721804f556e20bf9ddeec41ccf915d
73e904c29c98bfa714568c804c9570fd
c78ca5f3f16cd7711ff1aaed66a8ca2a
7bbdfe8cf153c3f1d804230cb5fc8159
61c81424e3cc66ec7b397ad0f303d39f
e49395728509e51e14d8e71feea9f620
7677a3d2a91e96f15bfcb425dbbb9be0
3d7f54543952157c941a554a8d874e1d
4ef8ae0fdd3afa3afd88fde1a42e993dd79bef61
632debeb48d4f119cf3e1d24aa00ab23afa04609
e98c7ec89df0f773b51a94eb64365e7db1a6ea8d

KPMG

KPMG Cyber Threat Intelligence Platform

ToddyCat APT : Both perilous and quiet !!

Indicators of Compromise: Hashes
3c159cd8614f2226e114c83c6e9224320f37d86c
e2bdb39105f9a508ef815855027d4cdb5481e9c7
285f84e8aeabcdc0a0ee1349aa9156794dde5e08
66687169db9406e13d0c1d51785890fefc1ac37b
3399681cfd6f7f2a270d9a543021ed9b93e85675
a71923ff816ecc4dbd87981b9b238f9b92838bdd
f89b1cb4514806e099bb38b0477ec0f37f6a01bf
21a52a33e10303a2a0c517452bbec81cdb99568f
9afa2afb838caf2748d09d013d8004809d48d3e4
caaf9e7afe82d2ee97135dd97b84300890a75819
92568d5606ec5cc531f8b13e9d3ce73947a06d0e
19e45c3658c04c7a728013b4673a75018565d080
4c04bc719069e03dfd45abaaad9d4e9fb824410b
a015975fabc65546195f0f2ef1f084ff658982ae
2f23c74bd9873519926542cf263e97d798e95393
f1922427f27e20f76ae55cdadfbabfa7be802239515a01eacb76061e2dbae23a
e9bd74e4609cdcaf77e191628ccde2124be03a8daf38f1615df6fe7d096b0fba
d5863435af5310d2f5fe5cb83e6a0769011696c3cc163673341cb3ea1a6f5ebe
be34b508eaf7d58f853fc912d43b0b51e6b963726742e383c2a8b2b0828a736f
8e2cd616286a13df82c9639d84e90a3927161000c8204905f338f3a79fe73d13
8c4eaa88a45e6558c1993f173845fa850c54b7e764074014702d0caa059bf685
7e85f7afeac89957c10309bc3cf9155f1a126de3670a3162e333329bc3a4caa9
5a1d4337431be103268ecc0ce2b1b44910da21fbbaec8ed6196f2042d887755a
3bea76f0819752abc5ff0c3d9f19b0d3ef1405eb8affaba5250b5ce2dc402c3c
2b0e66bb1a4877cfe650a027754e18085d0e34ab73025d9458e6136560120ec5
1fbe4fbdfe524eae20528ac37d68fa2de87d09b0a6147d86347e67cbae9eaa2b
1609f8ca52b30517ba17160acb9db9bf43d308907cbca9cea62ada76215e86c5
0a43b690b6c63c853ecc1dfd34af36f83099a07b0daf3c98c94cec402f91ad3c
033a5845b9058e88594a15746fe191532e7dc5c6ebb1d4c2e633b2af664eb6e8
b93c38c36296bfda57ece9a6e0c5a041972253b7a50cecdffd03cca0a4a09d5c
92ee96993605b4f0bb4b44092d5e200b7869f815d0b5895d5ba8edd0743f9d5f
dd2f3e28e92c3d3cb173725179d6939696c08e8c67696e679cb039d8d8c053c6
ff03c0a6d5a75179eef0cb70ac62c2ab492b41dfdcbf7d14dfe1b15f56ac99cc
007b952cde24ffd359fea25666186072c6011f3eeb4b2f95a4edb4b11e2c84bd

KPMG

KPMG Cyber Threat Intelligence Platform

ToddyCat APT : Both perilous and quiet !!

Indicators of Compromise: Hashes
0775756338aef0508650e6f6623664b1cd7ebbffb40f4357ae1ba4588f986ef1
10819ef53a05f27d3bcacc9c5eb95071d6d0b859c6bab68bcabd0f30a9ec5217
21e33ce1681efce4e69834494c28a78b677910ea25cf2cf77c40117c949b379a
2cde833301ae67e6abc57c85ad3d5a254b932d84aaa02dad2137565e250a353e
3063650a21617abc27e14a8811bac44df4a601b71e6488fd4b614f9ba5396739
4988a1db6f3ce94ca65aa60d73989edc14c30b1f61a1e0a7141d04ef3e8169d2
4c5e7d48b29e86887cb970d8849e89bbd801da0de466681e0ce0bc22a84fb5e6
5000d475681fe8f45a8d14652057943c3c2c22242803fa68c28f9a3481e3299c
55bfadff2e4b010cf9ee4c618c51f79b7127e53248d5c0eb63ebf2fdc545098c
56a27c07bdb0d483bba2e20500f56acd200cc562a98f41823026f1d7fc1df60e
658c5e80f9cb24a2507c0cb4c2d5db48af4bb095c56a45c7c295b54a58f9c880
752822c5b6082a29463a7048e9163e225db54308d4d737e6c2f725b69296e236
79d08921b5f1e22ee831feba71a0236dec27faa8e7359947f8da6d1baaf3242c
7d3bd7494a772b678c4acc30f324e637123ae55fe7fbce2498f0147f2b73f60c
7d6b70c220c2ad8ffc92643bbdb03f6b3a1daf8b8fa9856dd1ae0a4500d966c5
809ca8add272189239e6d855240b77c026ddb3b37ad623f5b513c6b2257fd1a4
8a7376dc1841a1e64275dbaa8499cd385425552e352d4db9366b7251541b9d38
8ab336e42cf5cf8a0406ecbc9ca0a6d6a3db625525d731aecfe4d925c7e1383a
9b32a4068ac9287f403a8b4d6503a3d2c1b60af148bff4816617febba72810c5
0aa00761ec7690afd0597dac0709070c4b7915471c4362d7abede6aef5b2a36c
14bffcf21331cf9ea9f2d6f2ef0e248f594023c26834da8b0f04b609c164e5ba
1c6d393f2642a28b0246987b881dcae1e1ed9f33001760939e645f2562372f2f
3fdf77518ccf3d6792ecfc73c05ae3324beaeb921a5a72c8cae632b3e98be792
476cc565153abae80ef4e6f5c6fd1f53a4ec3fc86bdf0438a05bc69d2e47a481
58907382e96b1232ffadff24674904e92109cda1a87d87b3ef40bc1364bdff4a
661ed267bcde431fd55d09c66f67e2aca9d3fb264f32658fb26c775684186ca7
6d40e3af23569303f9781b31bf8105d37d33b4dbe12f5aea4f5509ca662928d8
6e0a77cd74941410c950502dc685626626d368921d5e5c9424a0524ed6e711b7
751552c5f8ead833d52ba6930c4e5e3c2df7121c7a26663023e87f3e1e081f72
85048617afc96a879f511b176a3464d6c07f3fd1e22b821afb2b5c14adfd4e58
8819ed727d81295f1f47daa1e343048198d54358f04bd695fdb95d813856f172
9038e0b2c036cb3ec8e4e0937252ddea9b8c4cb3c9c9061613bb241c7a27f644
90ca166eb9e6109fe2e8d003ba08eb2837f16801e6699747225167477bcedb89
a7079465522100a3c455c5512b359dd7bb9c6c9df6b55c9d68decbb9e70d1834