KPMG Cyber Threat Intelligence Platform

ToddyCat - Redefining Modern Espionage

ToddyCat, a cyber espionage group, initiated the "Staying Alive" campaign across Asia in 2021, initially targeting Microsoft Exchange servers, since at least 2020. They relied on a passive backdoor named 'Samurai' and a trojan malware known as 'Ninja Trojan. Recently, they upgraded their arsenal by incorporating the 'CurKeep' backdoor and DLL sideloading as their initial attack vector, alongside other custom loaders with unique features. Their primary targets are European and Asian Russian countries, Slovakia, Taiwan, Vietnam, Pakistan, Uzbekistan, and Kazakhstan, with a focus on the telecom and government sectors.

Initial access occurs via spear-phishing emails with zip attachment, containing legitimate executables and malicious side-loaded DLL. When executed, these files exploit Audinate's software through DLL side loading techniques deploying the "CurKeep" malware. This payload uses 26 functions, sending recon data via reporting function, executing remote commands via shell functions, and downloading files for further execution via file functions. Persistence is established via scheduled tasks of executable by duplicating in AppData folder. Communicates via HTTP with encrypted data stored in the JSON 'msg' field and sent to specific API paths. Data is exfiltrated to C2, while command execution and file-based tasks are managed by the threat actor. The campaign uses various tools, including CurLu (contacts C2 server, DLL loading and export execution), CurCore (delivered via IMG files), CurLog (mainly targeting Kazakhstan, delivered as DLLs or EXEs) and StylerServ, a passive listener monitoring specific ports for XOR-encrypted configuration files, distinguishing it from other loaders.

ToddyCat's ever-changing tactics create challenges in attribution. To protect themselves, organizations should focus on robust security, regular system updates, and flexible SIEM rules.

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

ToddyCat - Redefining Modern Espionage

Indicators of Compromise: IP Addresses	
77.91.75[.]232	136.244.111[.]25
65.20.68[.]126	185.242.85[.]124
70.34.201[.]229	45.159.250[.]179
45.77.171[.]170	178.23.190[.]206
207.148.69[.]74	185.136.163[.]129
167.179.91[.]150	185.243.112[.]223
178.23.190[.]206	139.180.145[.]121

Indicators of Compromise: Domains	
ad.fopingu[.]com	www.githubdd.workers[.]dev
cert.qform3d[.]in	git.gitbusercontent[.]com
pic.rtmcsync[.]com	raw.gitbusercontent[.]com
cdn.pkigoscorp[.]com	imap.774b884034c450b[.]com
idp.pkigoscorp[.]com	cyberguard.certexvpn[.]com
proxy.rtmcsync[.]com	gist.gitbusercontent[.]com
admit.pkigoscorp[.]com	ns01.nayatel.orinafz[.]com
update.certexvpn[.]com	eaq.machineaccountquota[.]com
admit.pkigoscorp[.]com	qaq2.machineaccountquota[.]com
backend.rtmcsync[.]com	solitary-dawn-61af.mfeagents.workers[.]dev
sslvpn.pkigoscorp[.]com	

Indicators of Compromise: Hashes
64d7674a4e9e2a973c976fade4e64e82
b31c32af306d736572263371afbd1802
ad8f36645796b44ee4e6465c8ad5ead9
dbe6f9117e0cac23a31b0f871561348a
dffce9860497d0dccd414ce31e59c058
b34df10485790ded5e1bf772b832f90e
9e737418f7d0f09f22167229853c9eba
e282d63beeb78fc1ef6f954ab3296669
e25f061dec65a7d2721f49d24b1187f0

KPMG

KPMG Cyber Threat Intelligence Platform

ToddyCat - Redefining Modern Espionage

Indicators of Compromise: Hashes
5b3d4bd07f4ac158ed8965b717598458
753d9f3d05e9f8543e9ebe8c8bc11134
dcd66b9d9c461df948d18bafcf679d23
069d062e4e0d85c5ae51ead7d41d2b76
638234ad07eca214612d2829ad6de543
910ea9f6b7f6d06fc42d448b143a3634
e9fabe8fde49e1456b79de4d614aa6c3
22f4179dd0de6f1b5dd3e9fb2114ce02
9242a46ffa03d909dc93cd73e60abae0
0da769a721fe2cc786729d8e0fca5e63
af2d14423c034422cf4f15ecc3563400
044123543bbb15a027f76fa141c6a490
490bb295fa0cd31adef20d29a13f2ee4
e4b060fe1e74d3163ee74d43f5cc2575
b6708711f6b8ce93f2adf22484a5a7b0
a4ec8366a8a28f6b588c3f09254cf8ae
61f57598051268ae80b3926a4e3daeb9
b525b542db59b07f6486b0ef003374f7
12d7d7c7b0349a3ee3f5b6b9d5b419cd
507641012e9ce459c448da48549d8609
97d0a47b595a20a3944919863a8163d1
90b14807734045f1e0a47c40df949ac4
0f7002aaca8c1e71959c3ee635a85f14
d3050b3c7ee8a80d8d6700624626266d
d4d8131ed03b71d58b1ba348f9606df7
bebbeba37667453003d2372103c45bbf
828f8b599a1cc4a02a2c3928ec3f5f8b
65af75986577fcc14fbc5f98efb3b47e
14ff83a500d403a5ed990ed86296ccc7
4ad609dddf2c39cda7bdbe2f9dc279fd
d0cd88352638f1ae101c2a13356ab6b7
318c16195f62094dadcc602b547bbe66
c170f05333041c56bcc39056fecb808f
8351a715462e211dd1a833fdab6086fb423cd7c5

KPMG

KPMG Cyber Threat Intelligence Platform

ToddyCat - Redefining Modern Espionage

Indicators of Compromise: Hashes
f8900a1d6a6868547333cfa5511104201d28ee37
8be6d9f79a37c698d94c88820e2f369b50ddc811
6939b842bae577f600bdd2d26e443edad66bd8b8
71dbd626aed9bc98e4347087be7efe0f7042f5fa
bd3651da6717b7af4a84b762d963fb8be6839c59
b201e4d5efe65813b08da9eeb9de0f80e6ae292a
4c7005b33dcad81ffcf82841ad7cdf96a022cd8e
3202616b92b96ea0e6eff76671eb65f7ac8925bf
de80ffb1eed36eaaaa2584ee52b6edb6d8a48160
561bfe296e786d3d5105871083a10276c5db5e75
9cbc3dc37f0c3a4e0723d26a6083c77c30154b62
ca17a6c3c2efd3c3a9008f789246897ebe1a8d38
c4e4f1e71756e5e7172a8b47bcd0bbad3994ecc2
2d2dc7316ba5b9de546d175c620d2ccda72fab5a
a09a55c1223096669524d933052f712f48c7e781
0315c6be23a806a93fd23d29756d76794ec0eeca
ecbcf0c709bf7dae40bec88172dc4aee99dae1f1
88d7d37ba888679415458a99f1641758cc6df030
56c39daccc2853a6cd96c2471cfd005d5b305830
02a69010c27c7c75a0d36d803bbb466974360d32
f9db3599ff00b2822d1f0e1828cd21f0c1d80679
071882f521b4807ddf8c3ab0a10963157adaa19f
d062d2c1e3f2ad9f50d3221bc12c273854b86345
06d721b6f01aef11a66bfcb2a009b97072a1741f
60169ba7ef8781df9de226f2723bc424254282fd
a3aaf25327dc949f1f6e9fd1bf5996a471d0dc44
81a6126ad454a5e9eeffd410321b17c1c7e27c8a
cc631fd2f0b55ab42d50864a550e4319c99354ae
a252b05f8fa8b0384ba8363ce5dc6b47a51872d6
86e8e1d727384573cdc4f790c8f4233c2af21471
dfbc40292ca83efe53c12e0f1fc00ba4d67e7dd0
7e4a2bb5198a64c68e3ee4fdf97fc14b60a02f84
3d088f65839c7b55a540d736a1178a855337b2d1
34894d5ffa541ab159b69a2fe0937a5430dac545

KPMG

KPMG Cyber Threat Intelligence Platform

ToddyCat - Redefining Modern Espionage

Indicators of Compromise: Hashes
6eaa3381236586551204402 0bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746
78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd
409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c
4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6
437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a
c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac
da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9
451f87134438fa7e5735a865989072e7bab4858ca0b1e921224ed27dea0226b0
93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347
482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651
877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697
c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0
d94ed414dbfb9bbcba42e3bf2db3b76eb8172b03133d1745d6abcde6f9edbaa7
732621aa53683c16edf3959dfe9d93de5359c431c130784b31d4a598fbbd80a9
12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc
a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172
60030b970491bced72a56c9dde09a1d2260becfbf80a2b0d217a0b913e781c3a
36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652
b3fc497f94ac04abc4c9a6f23ab142fdc2387c520ce5c6fdae1b511793bc6ba2
4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d
d4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30
47de9bf5f60504c229fe9f727aa59ba5c34d173a23af70822541a9e485abe391
1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6
2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed
6f3de35c531993aa307729e2046ff7aa672f5058b7e0fc6557bbd4c500fb46e7
2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782
a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9
778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e
7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e
357d198131905900bc8fd308add72d9ef1f29e937622cac677d337bce3a81bc4
0c1a59e3dccc4c0fecb938fb20ccc57a646a854d89a9ba6d2a6844eb7ce468b5
f913515b1bebffae8e090b726ae7fb6e08a7213e1ac9636ee250d5b861fc5038
9d8cd5911f7f5af68766a47494b6ae47a1a6f461174f6ed06f2e0d487a8d5043
bfdb3f1a50f061faa7dfc49ba507364d3def60c0eb7f588c94a268742860f87e

KPMG

KPMG Cyber Threat Intelligence Platform

ToddyCat - Redefining Modern Espionage

Indicators of Compromise: Hashes
1ab42121bb45028a17a3438b65a3634adb7d673a4e1291efeabf227a4e016cfb
295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719
462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a
caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1
d33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4
1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a