KPMG Cyber Threat Intelligence Platform

Play Ransomware – A New Formidable Threat

Discovered in June 2022, Play ransomware (aka "PlayCrypt") has created quite a reputation for being notorious and has impacted victims worldwide in nations like Brazil, Argentina, Spain, Netherlands & India. Despite their recent inception, the attack TTPs are pretty mature to an extent that they resemble much seasoned ransomware groups such as Hive & Nokoyawa. Play has been observed targeting hotel chains, cloud hosting providers and government entities alike, by exploiting vulnerabilities in unpatched Microsoft Exchange Servers.

Play ransomware leverages unpatched ProxyNotShell vulnerabilities, Fortinet SSL VPN vulnerabilities and valid compromised accounts for initial access. Post gaining access, existing remote desktop software (Plink, AnyDesk, RDP) or SystemBC RAT is utilized for further access. Play also uses 'netsh' command to enable RDP, if disabled. With persistent access achieved, network discovery and AD enumeration is carried out with tools like AdFind, Nltest & Bloodhound. Post discovery, ransomware executable is distributed by creating GPO or by leveraging DC shares. Scheduled tasks or 'PsExec' would be used in later stages for execution of the same. Elevated privileges are met by credential dumping through Mimikatz or Task Manager along with WinPEAS scans. While Cobalt Strike beacons are used for staging and C2 operations, Play also packs in loads of evasive capabilities. Anti-malware services & Defender is disabled via Process Hacker, Powershell scripts, etc., and logs & artefacts are cleared via Wevutil. Prior to encryption, sensitive data is collected and compressed with WinRAR & exfiltrated through WinSCP for classic double extortion.

With adversaries like Play that exploit very recent vulnerabilities, organizations must adhere to frequent patch management cycles along with multi-layered approach to security by adopting MFA.

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

Play Ransomware – A New Formidable Threat

Indicators of Compromise: IP Addresses
84.32.190[.]6
104.21.43[.]80
172.67.176[.]244
139.177.192[.]90
67.205.182[.]129

Indicators of Compromise: Domains	
newspraize[.]com	realmacnow[.]com

Indicators of Compromise: Hashes
594ddacc1b726286b64b7c132c4ee09a0edf46af
d1ca86647bdd456e67a0a6a72a7256bf99671f43
00982a400c4d7a0d04d6d85f3043027412d85103
a5210232804b21d40b12b8203129fd3170dea1a1
9e9687ac163bdcd2766def5716a399b24bf659bc
28a8262563452c9903a74e5c1432e4e4109e29b7
e3e9fa8f9b5cd45ead5029ef41ab6c12d0ac71fa
98cb2ebef1e8549902b64629527dfe5ec334128e
907f94850a2ffd71b11d0a19006c7c3497263600
3a1955df1e40a92d317826cacc20c2d42599c2a7
dde2ae2ba4bf43a579b76cee9b5edc4ef792fa1a
5e6100689cab65fd352d79b93b5e83f42d480fc5
64966b2c8ec04ba57976020dc64f13a5014627e2
cf9cf8d3d91e966328f8983fbeac50698a4cdedf
9bafd447a32fa43ffb4f000c0e95cd95febf1030
5d5cefc237af647547b0cf5891a1e96da26826ce
40a05ac654a1501b923da9fbb0ce812f8e0f0e92
c3051ca5ee95e437d52dacb3742961581c0dab6e
429a0b1433d6c5aff49bcbf362f2a65878a6e104
5cfb84e4733841659ccd1248b89a99f876212438
4695b51c6b505013a8d04f7f78fa1e903b2aaf44
879bf5aab7a684a14aa9d3a973380144a38186d3
6eb3039824756dbafaa29708ece1c9adb0aee484

KPMG

KPMG Cyber Threat Intelligence Platform

Play Ransomware – A New Formidable Threat

Indicators of Compromise: Hashes
daf195df847fd862ed0370253f64685eae686ae0
6d3fdf2d61109ec6c40499104afb8a40105b4de9
f2afc65f0c61e471c6624563b8eb310ea41e4703
af029df8bfc2957448081b2bfbdb6e9aa2be2537
14b67512f4d7ecdbc27222c86a30270d615d84f7
babd45557131bfe3e929d35745b68c1898f2a6d1
d90228c331f1aa500c67bd54c9c6d72a8a1c7915
7b658b4f09f7b06f77631f5eaad39fb30861debe
10f1313d46208b0e42df6ff8386f555d7ef9eab2
42b554e986154669c296a600f0228a942925b125
4b1e5197602b4bb7b2f929b68acbbfab47991e32
f248c3b418f8927eae784131670f7e65687d8a7d
a70ed1a694b586d64083a36893f507a452c84ede
2dea1a3eb2eaae00370f734c525d1670cad77d2b
74408c03e64d48978db6afe36d24b5c4a3df6d59
8a09e25fb6f3e6d95369c55ad3f2d3e2e1e1d58b
5ca233d62392e0d65af0a91c46cc0f79544c8ecd
3b544ce4d55be690c1c74fdf8b8fa9ac21b823f3
a8910c1b738e3916e661245a5b37776b2334e197
7ec824d694d1435b99eba1cda04ce91c515f92f5
acc064b47d41886b784c2b8815649e5efb7eb685
ac8f99586230162c5c52820e3929f48d1e2c52ab
a2f97112653b4f710538dbbcf6e1548d667bf115
ceb211ebe31b7dbd40c86175f544a2ef17bfab11
f1387388bebe5a1f498bdf9ebc662a6d72586294
644ab7e1d796f735f8647a2bf5d6f78f5c603461
5aa56cb63a98090bb46eb6d5e45616832f9df8cb
c4e954df8e1917993a73f4445c9ce941bed4c5a3
f7515f992a9b0d7580d0da2f906714a12aad6c7a
3845b736c5651b2d544ad04cc611bf7101aa4c77
74bc1eb1a22d5b77d24368abfe75f1263ed14b66
a6d0782c0e204130fcfb1632d2f171e2ed65eb53
68e69f79ea35e56e257a458da327ea2e3f22aa3d
d73a54aad6f8ad32ec85524b5307b05625ebe1a8

KPMG

KPMG Cyber Threat Intelligence Platform

Play Ransomware – A New Formidable Threat

Indicators of Compromise: Hashes
a097f3f29a947cd1b5fe2aa060f7355e6c74b0de
dcaeb40cd4795aeecaf5942a692c3386d6e61e56
28ec3ec99f75625cd04c80fd959e85e14413971e853a30b0c4eccc04c89965c8
2a7b0c1a564590d2db18c661332b86ef1d63b57f93b0d8f5b67234dd62f95a82
2f41b2b8efd7cab306988c0eceed693357ed3b4faeffa4470d0305bb81b627b5
2fd3277e5ec0c96db527fe13f48b65053780f3cb42b9257f81723f8810b59c44
2ff93638fbe56a072d72599c845a636e0e3a5ce4d389ef6fce83cd1e8206bd69
339a261f3e9e69c06e2c014a30c2fd593ffda87bb8407834946ec5581173497a
3cdbf9ce96a59768a19dac80b22811ba81bfae4b1364dee9bd76436a7bfa2d7e
fc2b98c4f03a246f6564cc778c03f1f9057510efb578ed3e9d8e8b0e5516bd49
c316627897a78558356662a6c64621ae25c3c3893f4b363a4b3f27086246038d
c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3
e1c75f863749a522b244bfa09fb694b0cc2ae0048b4ab72cb74fcf73d971777b
094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde
e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173
d4a0fe56316a2c45b9ba9ac1005363309a3edc7acf9e4df64d326a0ff273e80f
c88b284bac8cd639861c6f364808fac2594f0069208e756d2f66f943a23e3022
f18bc899bcacd28aaa016d220ea8df4db540795e588f8887fe8ee9b697ef819f
e641b622b1f180fe189e3f39b3466b16ca5040b5a1869e5d30c92cca5727d3f0
608e2b023dc8f7e02ae2000fc7dbfc24e47807d1e4264cbd6bb5839c81f91934
006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55
e4f32fe39ce7f9f293ccbfde30adfdc36caf7cfb6ccc396870527f45534b840b
8962de34e5d63228d5ab037c87262e5b13bb9c17e73e5db7d6be4212d66f1c22
5573cbe13c0dbfd3d0e467b9907f3a89c1c133c774ada906ea256e228ae885d5
f6072ff57c1cfe74b88f521d70c524bcbbb60c561705e9febe033f51131be408
7d14b98cdc1b898bd0d9be80398fc59ab560e8c44e0a9dedac8ad4ece3d450b0
dcaf62ee4637397b2aaa73dbe41cfb514c71565f1d4770944c9b678cd2545087
f5c2391dbd7ebb28d36d7089ef04f1bd9d366a31e3902abed1755708207498c0
3e6317229d122073f57264d6f69ae3e145decad3666ddad8173c942e80588e69
3e80aa26785dc1b3c313175a56f3fe39489996e7a976df0877809b23a25cf243
dd101db5d9503f33a0c23d79da3642e999375748f7c1532e98c813b114bdfa1a
47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57
703075181922eb8db8d23279eaed8f7263dfa2b64383cff675da4cedc2394af5
f39d6741cbb99a81decbe5e75c07e846b5a36b40bc1bb0c0c61415300cc43b6c

KPMG

KPMG Cyber Threat Intelligence Platform

Play Ransomware – A New Formidable Threat

Indicators of Compromise: Hashes
8d94028bfaac5bef84c56b01f40e429ae4cdf799b2b755dfba9eee3b72448b5b
f0a3047e9d557e2150501e302d5e96a1c2669858fb0072f97024fe0dd07d5271
8556dfe5582a5647a5e96cd77e6239874504a01a9c7b9e512e70329ec6f61aea
5e94626c6bcb825acede3826811ed693644d6dbb7caeeefb8575c2ec711a65a6
a29e20d89e8c933e05b690b2779f82716fb31f688594b99d868e4382058caa8f
757524b09e5d4f2399172c4ac0f6996ec34dec90110542973d438d5370aff280
3a36e917a4a6587290a393d5b10d0bd42f99cf0c72a2e7de751a4bfaeb9d30c5
92f3abed62d710064a19f2a50c4482cd02adfd821ace4c2f3030f96290166189
157c43a3a4e014827e42cf4dd20cc8efa71cdf098f5d1d04b6cd1a972d6a8c7a
5eca08ddca898427de5ab13fedf25426102c3a0621d086b63f2e37d2d04ba3e9
2b4111121fb35b46665c42e3ea2cf1b8eda5afce580e310465cb259bb1abd053
12d1a0dc37d877dbf81bd18e8bd57b2843cc254c9a3cfcbecb70305612e60cae
bb51255ec929ae1fb34981b8b988769027ee49e68c0958a4a2a76b59a0dc1cff
51f44e31b0f3718a5d145a1f77fd79cbd7ff21fecf8bba3181fea019b508cfeb
73e19be4da76bb4e52cb82493c75690977fc3a5f589a9b47e834362545ef512a
bbd84d10f6a56bfeca23fd5d11d9e370fdfa91be73aa60c9d460b2671145c109
0ed328af77f2576071bfd543938fc01101daac01f216dc43bc091a8da4aff18d
f054f373cead893f868fd9b4acc24f751afefbb80cf961e305f97741f952a641
176476f9d924d83343a51a90ade097d12b7594dc5dbca1771c440047dfbe81eb
957a6aee2437a5c4d31372af2f6bceb29e1c7a49d650fe207cefc624bf6bca82
2e9126dfad03bdaf54f9b29ade42038c83f65ac7288376f45768901660f62d7b
2ab190542c3ec7b2b6e6d4bccce4c5d6a572f98c6bc89b014fea0c8fd6db6723
025f2979fead7a0a01a865fa13faa6ddeb52cd0b5adeefde772c850ebfe855ab
0985f1db50775fffa6f8bb61f0f999511b00417116ad90727ef685612ee49fe1
0d96417148e8edc070786d8dedb26321f00165d01037829308a070d59c38f48e
14105dbd5898e3377144681ad6f1ce7612f85db44124d8eb8c2706470c3f5b1e
16240fbc4bbf7554c6908de5ae26268d2358403930cd4c86bfa345cdd7cea8f6
1858dae19836ab5f3487f99430bb63ff0c26905a652c35238bad044ab267db0f
189285ef59c910fb07e7a1f7b69588de3fdf0eaefe5703d01a3db138c3b647bc
19112dca43575586f4b26433172a864196202d2b8df4e696bd1e9cd2a7cfc15d
19dd0dc7d7a278d3fdd4cab2d150012563e391b8ebbefaed6fafffe1f9a57537
1a91441acc4e9141a8067c9dc9d532133d7a28061ae99272d5cd62b6c5cb75f8
1c3d58e1785554d315ae768806c2ce5dc6079bf8c39e17d4cc36fee80e2e0074
1ef45833ba3835b19f03c60d07c2642d5435ed89030756410d4e3a9c20770ebc