KPMG Cyber Threat Intelligence Platform

NOKOYAWA: Another Stealthy Ransomware!

Nokoyawa suspected to be related to hive by some and Nemty Karma variant by others, marked its first appearance in March 2022 with enhanced destructive attack chain capabilities. The alleged RaaS is believed to leverage phishing mails and advanced tools to gain an initial system access through RDP for lateral intent of file encryption and ransom extortion. The threat vector has been primarily found in Argentina with large number of its target instances also reported in South America majorly attacking financial, health and education sectors.

The attack accelerates its efficiency with the use of latest tools like Cobalt Strike, Mimi Katz, Z0Miner, Boxter and anti-rootkit scanners like GMER, PC Hunter for information gathering and defense evasion, depending upon the victim's environment. Unlike Hive's encryption approach, it generates a random key through BCryptGenRandom API for each file and abuses Ivcelcve and Salsa to encrypt the files. Contrary to this some analyses show that Nokoyawa manages multi-threaded encryption just like the Nemty variant. It's also worth noting that Nokoyawa didn't use any packer for binaries resulting in open code strings which are easy to analyze. The threat vector is believed to encrypt the required files with ".NOKOYAWA" extension and leave a ransom note in "NOKOYAWA_readme.txt" repeated twice in both English and Chinese..

Provided the potency of the ransomware, mitigation becomes crucial for organizations. Additionally, enabling Mutli-Factor Authentication, being wary of the phishing mails, making employees aware of unopened and unverified mails and patching the required software can help organizations protect their privacy and data from such malicious cyber manipulations.

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

NOKOYAWA: Another Stealthy Ransomware!

Indicators of Compromise: IP Addresses	
20.50.102[.]62	185.150.117[.]186

Indicators of Compromise: Hashes
d14afc1019e09ab7efdcd4fc133e9301
78d7516f2b75aceb180f7afee7a810ff
16cde93b441e4363700dfbf34c687b08
88d9b3f64787d1a0a6ca3058316eeb6a
da59d51f2b54cfe2731e1343a2388a31
073a9a00cfe536b3851825ece3fc9d44
149220cd224916b3aaa31eb0e147a170
122e535ee64716dd245a64c7ca8af734
af34779d0eb6ce52086e14d75d0fc401
1876d7443a6c0359d24f26465f9487d9
f944cbb7aff2f2c79595365267ca35d4
07b2b4016e7d0a1b4314615e7f8e8a49
119bcf7605a2178b28ae959acd1da986
6199d71f916135e6649f6978f13f748d
318a6f65e3f7a40b6a85079a912e3f21
3d51ad41f0fa71cfe67395f42a45fcb9
bd624abb90c019e197034179453b6d70
df7515c814e9b7b8bc1c8f0dfeeb7103
2e936942613b9ef1a90b5216ef830fbf
c44f50581d3379307e16849f20f722dd
19963c62cb0d94686fd247e64427370c
e5e78d7352ccba0d501a594f96a59a3e
b5402e3c43ee0b5f4a6c1b4be8f17aff
d41d8cd98f00b204e9800998ecf8427e
790e1636821bb83eff48fd8314557817
807e207d1c7ca20356fbe11cf7fe7e59
f64219ef30d34067e9a5a085151f43f5469c5675
db00db3f885f8382e9aa708d20110c9159fcddb9
092ac6f8d072c4cf045e35a839d5bb8f1360f1ae
32c2ecf9703aec725034ab4a8a4c7b2944c1f0b7
9b68ebd37d17b5f54d465d128bcabb9fa8dd698c

KPMG

KPMG Cyber Threat Intelligence Platform

NOKOYAWA: Another Stealthy Ransomware!

Indicators of Compromise: Hashes
a70729b3241154d81f2fff506e5434be0a0c381354a84317958327970a125507
c170717a69847bb7b050832c55fcd2a214e9180c8cde5f86088bd4e5266e2fd9
a290ce75c6c6b37af077b72dc9c2c347a2eede4fafa6551387fa8469539409c7
e097cde0f76df948f039584045acfa6bd7ef863141560815d12c3c6e6452dce4
5a08cd9ba3d16f45368fe914668e515e356be506f31cab7d841a5db21577526a
accf036232d2570796bf0abf71ffe342dc35e2f07b12041fe739d44a06f36af8
ec5526b24e9bd32e2d03ac182d0ff27372ef2dcda72844de1e4ad7d13c9e6167
388f75e900f0c15fd66249d7b2e7edf6e14eeefb859e6f766b75058e44f27af6
8bb321ef2daa5dcf5d20618d9c33668b12363e5fb04aa515b2c6840e02e4b2bb
f06d600ea4a3e401423ea4c7c7c947639e83fb2f2a0720138447c0d350242b85
56640099d7acacbae13355b944011eeeed4f5e63401e55defcccceb3391a0ddc
6b9bcc91b6e083b383ae4e98f5a6b6f786da77c51af88ef62c713604f9ccd751
5a317ab2e15354528a08bf82877d85c03d39ca7a613df7d8aa685d46a1a18f07
22c4e72498551bb053c3d159a78f837cbc4add47c95b9547bcb3b9f549eef7e7
45871f481e151135563619fe3e2e64ac63bd7b94a268c83e90bb1b0e94799538
d9eca1a38e9050c4ba053e78b4360ce24b8e04e882ce7ce721d354a98070606f
30781b14770fc74057ba0a2ef4aa82a930d78333d0402d5f9e753ccfe0569e43
218562b70ff5a82e124682cd577b633cdd715b77c5e8ae9343a4d43a7fcfacb3
55ebbd1bf108c8d83fd49affc56e8e630b063a455266331b2b2285025c0375e4
cd438410358c92322fd2210b22d58c3962c4efcf1207ed5adcae21d1bae7083d
4f6d2774d142fa420d29e19b664c1c7732f4a68fc684e0cfc794c2a0737baec1
c95ae2ac7c7c69b55cf94c2bacbfdadb73383dd464b4d9541b7c14d4d662469b
9f5589fad7a7148fa25e054fa51b868d20d20e8bf2ae3d386c706964f5339da3
9bf36d38deda9cbf07ce729bd4315742151e2523f07b801271398102adba5527
a876071454d701255e22d1a4e3214d749573fcbd7c256b356493f21c07ed5ef1
40f09e45d9df9bd7026920c861f74f49472b4753605fae9de23bc0a2f1409234
edda4b7476cdb6c84bc7cb2b06a49c559da45fd45aa4d8bede15369e53236e44
1eadb466656d9d0bc033cdd053a4187d30e657f26abf3249c6a6b17eb325731b
fbdbbc93b38df651fb8e8f863750fd988152d1383a9d5c736cf3f773d6581437
201bab87557f03102c46a5bd89c86b2fb63fd3e4daead979408601f9c0d48ac4
cf42aedf0fd0c2c5dbe790e0c65707b29bf609ddbe67c295859618ec92d8aec6
b043434cbc5d8acf88f2e1f2dd9e57efcc142b67e5895796a5687399e4d81c7d
2ef9a4f7d054b570ea6d6ae704602b57e27dee15f47c53decb16f1ed0d949187
f44fc40bda372f698344e7ae0465f906e175dc18ca36e4b9eca8448bcc875e8f

KPMG

KPMG Cyber Threat Intelligence Platform

NOKOYAWA: Another Stealthy Ransomware!

Indicators of Compromise: Hashes
1c47adb7846f1458a94d9cb873a16e76425804aae36a56f271c8bc9dc93f3dbf
9166ef7f0b9b3d50eff3c0d20c5e1dc31160d6728205c290888beb51459fc75f
65e1fca098b9af86bb168f65a104bc90601992020e20eb5d2bc5d195b1a1131c
5b7a8b144072664eca04d6a1d2734f00fb8fd6a01d99a85e983e945b6664986e
70522da9fac5b0fdb1c181d3d16dd5b6274468318a804bb6ef141f4d1397fe60
a5ba81861b80fa93d9cbdcba1768453fcf6d2aced0db518cf1eef25c71d414b0
1726d3125317f05233cd7e24d771c6591d3311ca444515a078edab92e623e8d5
f2e6f9070fb27d7fb70b77a99ebf9ef8b17954fbe93c7db0ecf4c7fa26eebf29
1f74b73bba5b807e7f22b66b6854621967a713cf0b6e834b0b87023a78a154c5
9d44674f0f1a4020266bc9385040ded9a0846e2816ec814d71134f962f6ff3b4
6eb2b5082366f96f14958f7fb517c68f82c53e348d75a2807471f6146c689f7c
5fe74196fe3553a54336814ebf4083647d88592839229d15cd1e8144da99436c
f4574582df00d9980860e301f2d4d47f568cb0ddf105ccf9629ffcf31f84d2aa
0eb19780c4d061204deb2d9798720f954707510405111b6c436d74c2a8b5f975
04c00f8e394dbc62c47de38782f364498b7fa12ab9b87a6c5ba7c43acc8d4f9f
291ee24e408ee31f3e27ba3bc99ed5f345db6cfb21c39143b262b10e6030b4d6
384a2e3c4eb4aa3d5f61b93399a552177ee1d718369f51df9f585874a249ad12
66741665496e3f534d23c1ff278855eaea04a278b67a5ec0ba685c9891a90e11
f8d71bc19a73d68f2810d454b130155fd9f044b962c748d86ad855f8cb86898d
37f754de8388f10bc97bb3c529de51b04d17333b581739b771236ad10b260a8e
07998eb67952637129701675b47ee81ac29ebf50883bca0cabb05ee92d1aa330
c9c3de582f5e9ddbd61c5eb14a1e0bf6677d1fbfe1b255987bb7b917d73d76c5
d6c85100001f7036439acd081704673d73459b08df0091a2de85e37a5ed3b631
ec229568523b713e7ab8482e93fd50b3f16f4514ebee0487931e0eed092c07a1
4a6a341a48cad563cc39457e01f66c7522498ae217d7fd0e3164c5c52089b671
82a08ac87492c82930a67c3ebde16d39cf15d55854a0e07f39bc468c1a5bd970
c42da72c2ff9fe70b6946dd59d34650d0b22404067f0a3b537d64d4c6c191a5d
f4230cea223f2562e068c5effb43432989036073ac89b02f41bcd2e10e968024
01d3472f7e8fda2a7eefb36686bd491508f6d0d69ade5d6562bfe4985af1d472
fc3df67b1e249c6fb70eab97c81cb727ae3f1711b3912c0013503a2e414f6508