KPMG Cyber Threat Intelligence Platform

Cuba Ransomware : Incited by Hanictor

Cuba ransomware (a.k.a UNC2596) has targeted more than 49 institutions spread across critical sectors such as the manufacturing, information technology, government, and banking. Active since 2019, it has primarily targeted organizations in North and South Americas. However, it has been observed to spare the entities that provide urgent care. The threat actor is using custom packer which allows it to evade the detection even though it has been in market for a while now. Having picked up the pace in 2021 the threat actor have earned at least $ 43.9 Million heretofore.

The Russian aligned ransomware group primarily uses the Windows-based virus, Hanictor, which has been in use since 2013. It has shown a preference for exploiting vulnerabilities in Microsoft Exchange, with ProxyShell and ProxyLogon being the first targets. One method of delivering malware to an endpoint is through social engineering, it also secures initial access to the victim's endpoint by exploiting Microsoft Exchange Vulnerabilities, compromised credentials, or legitimate Remote Desktop access. After gaining the access, the next step is to manipulate legitimate Windows executables such as PowerShell and PSExec. The ransomware will then encrypt all files with the suffix ".cuba". In addition, the organization takes files and threatens to dump the information on the Dark Web unless a ransom is paid in crypto.

The simplest way to protect oneself from this ransomware is to keep up with the latest Microsoft security patches, using multi factor authentication and using strong unique passwords. With increase in number of publicly available vulnerabilities the threat actor are seen using them in their operations.

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

Cuba Ransomware : Incited by Hanictor

Indicators of Compromise: IP Addresses	
31.44.184[.]82	37.120.193[.]123
45.32.229[.]66	157.245.70[.]127
108.62.12[.]122	185.153.199[.]176
40.115.162[.]72	

Indicators of Compromise: Domains	
accomead[.]ru	windetheta[.]com
kabimmo[.]com	sweyblidian[.]com
jollygul[.]com	mettlybothe[.]com
Pospvisis[.]com	aklatdelmundo[.]com
dialencelu[.]ru	makemoneywith[.]website
undereasus[.]ru	cuba4mp6ximo2zlo[.]onion
frougelylo[.]ru	quickcompanyreg[.]co[.]za
kurvalarva[.]com	medicinainterna-critica[.]com
gatiallyde[.]com	

Indicators of Compromise: Hashes
3fe1a3aaca999a5db936843c9bdfea14
ba83831700a73661f99d38d7505b5646
7b6f996cc1ad4b5e131e7bf9b1c33253
ee2f71faced3f5b5b202c7576f0f52b9
d907be57b5ef2af8a8b45d5f87aa4773
99c7cad7032ec5add3a21582a64bb149
72a60d799ae9e4f0a3443a2f96fb4896
26f6537ae7eab818013eb021f54c46d2
6541b3e2c5a8f86531721ec1d417be6c
7fb1cc93b51cf6db68ae20bdbd197023
882ea66f8685633ae0195060dc60076f
8ee94ecdec0de4f4e60e589dae57dbdb
4dd315284258a738e747250cba91cb3f
4bbb69bb35f95223e82a573ce0794a78
4c32ef0836a0af7025e97c6253054bca
f9239348c88b2593814541d33c2df11d

KPMG

KPMG Cyber Threat Intelligence Platform

Cuba Ransomware : Incited by Hanictor

Indicators of Compromise: Hashes
23d0033fe765242cbc07ceeab7ba3736
77be0dd6570301acac3634801676b5d7
2841848ef59dfe7137e15119e4c9ce5e873e3607
209ffbc8ba1e93167bca9b67e0ad3561c065595d
25ebe54beb3c422ccd2d90aa8ae89087f71b0bed
867d41458d94e985f6b3e2bae1dfb75e14cbc57f
d1ff26ea3d2d2ced4b7e76d971a60533817048d7
4de5d433af5701462517719ce097bb4c0e5676c9
a304497ff076348e098310f530779002a326c264
c524ca6a8a86c36a34fb4dc06a4a2696e80a1c07
704d981f358ba00f8297bdd249f388ed157a0dd1
86ed4544eeca78dc64881a916fe1e1f73dc17f7b
0763e80f967822c263d85525d29cb535004e3156
d318737c9116dd181c2ec074c1ffc9e2f42bc31b
d83fbc9534957dd464cbc7cd2797d3041bd0d1a72b213b1ab7bccaec34359dbb
c1c89e5eef403532b5330710c9fe1348ebd055d0fe4e3ebbe9821555e36d408e
915ea807cdf10ea4a4912377d7c688a527d0e91c7777d811b171d2960b75c65c
c4b1f4e1ac9a28cc9e50195b29dde8bd54527abc7f4d16899f9f8315c852afd4
944ee8789cc929d2efda5790669e5266fe80910cabf1050cbb3e57dc62de2040
78ce13d09d828fc8b06cf55f8247bac07379d0c8b8c8b1a6996c29163fa4b659
33352a38454cfc247bc7465bf177f5f97d7fd0bd220103d4422c8ec45b4d3d0e
672fb249e520f4496e72021f887f8bb86fec5604317d8af3f0800d49aa157be1
e942a8bcb3d4a6f6df6a6522e4d5c58d25cdbe369ecda1356a66dacbd3945d30
907f42a79192a016154f11927fbb1e6f661f679d68947bddc714f5acc4aa66eb
28140885cf794ffef27f5673ca64bd680fc0b8a469453d0310aea439f7e04e64
271ef3c1d022829f0b15f2471d05a28d4786abafd0a9e1e742bde3f6b36872ad
6396ea2ef48aa3d3a61fb2e1ca50ac3711c376ec2b67dbaf64eeba49f5dfa9df
bda4bddcbd140e4012bab453e28a4fba86f16ac8983d7db391043eab627e9fa1
7a17f344d916f7f0272b9480336fb05d33147b8be2e71c3261ea30a32d73fecb
c206593d626e1f8b9c5d15b9b5ec16a298890e8bae61a232c2104cbac8d51bdd
9882c2f5a95d7680626470f6c0d3609c7590eb552065f81ab41ffe074ea74e82
c385ef710cbdd8ba7759e084051f5742b6fa8a6b65340a9795f48d0a425fec61
54627975c0befee0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc
1f825ef9ff3e0bb80b7076ef19b837e927efea9db123d3b2b8ec15c8510da647

KPMG

KPMG Cyber Threat Intelligence Platform

Cuba Ransomware : Incited by Hanictor

Indicators of Compromise: Hashes
40101fb3629cdb7d53c3af19dea2b6245a8d8aa9f28febd052bb9d792cfbefa6
00ddbe28a31cc91bd7b1989a9bebd43c4b5565aa0a9ed4e0ca2a5cfb290475ed
729950ce621a4bc6579957eabb3d1668498c805738ee5e83b74d5edaf2f4cb9e
196CD59446AD6BD6258EDAF94D4845E1A73455F87BCAEFF4241606366B6F7D87
947c192f7dd6e8329d66faaa8abcb6b5f59fc7fd8adaf19811da4a4e8b463983
6d5ca42906c60caa7d3e0564b011d20b87b175cbd9d44a96673b46a82b07df68
1d142c36c6cdd393fe543a6b7782f25a9cbafca17a1cfa0f3fc0f5a9431dbf3f
79d6b1b6b1ecb446b0f49772bf4da63fcec6f6bfc7c2e1f4924cb7acbb3b4f53
5cd95b34782ca5acf8a34d9dc184cb880a19b6edcaf4a4553fa0619b597c2f50
B952e63fe46b25ee4ecb725373bddd1b1776fbc4ba73aee7b7b384a3b0f7f71e
b14341b1ffe9e2730394b9066c6829b4e2f59a4234765ae2e97cfc6d4593730a
e82cc49c03320a0fb6ec3512c0ca3332eb1b40070cc53a78bc80b77b4aba975c
4b5eefa1727b97b6f773be3937a8cc390f0434ddc2f01dc24b68b690fafbcc93
7f4bdf94a0e0457f41bdd1a8d8d9fc39fc383d3d0a331048828d391bbf727a1e
141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944