



KPMG Cyber Threat Intelligence Platform

Haron ransomware is the unholy lovechild of Avaddon and Thanos ransomware



First spotted in February 2019, the group Avaddon Ransomware as a Service (RaaS) was known for triple extortion tactics - exfiltrate & demand ransom, name & shame their victims and conduct DDoS attacks on targets until the ransom is paid. They have recently closed their operations and appear to have renamed their operation as "Haron" and while borrowing code from "Thanos" ransomware.

Interestingly, Avaddon seems to be a play on "Abaddon", which as per Merriam Webster is "is a place of destruction, an underworld abode of lost souls." akin to hell. Whereas "Haron" seems to be a play on "Charon", the mythological ferryman who used to ferry souls from the land of living to Hades, the Greek version of Hell. "Thanos" is a play on "Thanatos" which is a personification of death. The groups seems to stick to their naming themes over their RaaS variations. The threat actors behind Avaddon (and Haron) were very active on underground dark web cybercrime forums, promoting the their RaaS variation to potential affiliates, but closed shop in June 2021 wherein they released 2,934 decryption keys, each key corresponding to a specific victim.

Haron RaaS sprang to life in July 2021 and claims to take techniques from Avaddon and Thanos RaaS. It also operated from the same domain, had almost identical ransom notes, used same timing notation, leverages the same open-source Russian chat program. While Avaddon created and used their own ransomware based on C++. Haron, on the other hand, is using the publicly available Thanos ransomware written in C# whose source was leaked. They also tend to carry their techniques and have measures to deter forensics/ reverse engineering, delete backups, use phishing as an initial access measure et al.

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: raghavendrabbv@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjosh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia





KPMG Cyber Threat Intelligence Platform

Haron ransomware is the unholy lovechild of Avaddon and Thanos ransomware



Indicators of Compromise: IP Addresses

104.31.66[.]68	217.8.117[.]63
----------------	----------------

Indicators of Compromise: Domains

hir[.]ee	loft-06[.]de
mp3v[.]ru	tldrbox[.]top
tglyr[.]co	tldrnet[.]top
tscho[.]ca	angele[.]date
myip[.]com	skreiply[.]gq
rzbl[.]net	1825678[.]com
zhug[.]top	edm789[.]info
8coins[.]ru	qsclan[.]info
czyfd[.]com	shop1000[.]nl
7782t[.]com	invonews[.]cf
myzko[.]com	myersinn[.]com
bwxptn[.]tw	filmtele[.]com
tx819[.]com	bancairro[.]tk
xddry[.]com	hofanef[.]info
yft6e[.]top	rectobiz[.]com
tldrbox[.]ws	gakadesu[.]com
poy778[.]com	jakilevy[.]com
rohkem[.]com	zippo520[.]com
shyhou[.]com	amyfelts[.]com
vn-tek[.]com	aroursali[.]tk
rotavi[.]com	bwin90ir[.]com
452065[.]com	wy6g3x5f[.]bid
evasrv[.]com	xiheiufisd[.]su
fajien[.]com	asciipr0n[.]net
wxbccg[.]com	opticmeans[.]pk
dgxtwj[.]com	topreplay[.]net
websahutpins[.]cf	5o0wx3gci[.]xyz
tejebetiliti[.]cf	aneoeauhiazegfiz[.]ru
cerkezkoycilingir[.]com	unokaoeojoejfgnr[.]ru
avaddonbotrxmuy1[.]onion	ouefuguefhuwuhs[.]ru



KPMG Cyber Threat Intelligence Platform

Haron ransomware is the unholy lovechild of Avaddon and Thanos ransomware



Indicators of Compromise: Hashes

06072312768ba47c162d2aead14bb170
c9ec0d9ff44f445ce5614cc87398b38d
db09bb973600aa0ebcb4f3e3fa84e3a
663ed357c545a72676219752d6236b0d
5074483417c273031124997af2316837
0475d9d3485583090f00b1c37450771ccd0df00e
e65df27b70ba3206d216a49b43f6beb2095cfe1b
9d38ce8e4c3ca5fbdfdfbed3ec452151041189c0
9cd9dee39f132cb398a3408cd16a53b98dafa7e
8ae409a74a209c304233ce6c6f778915fc59264f
5a1ffabbc8709c5c29911a4bd09b48a79731968
39e30adae70f605e09db5c5a359a53e4e6f3a14a
cc0feae505dad9c140dd21d1b40b518d8e61b3a4
319ec1a54148644197b40ed4d73b8fe5646c4f6ebf76d1487bce40a72d37baa7
f7895214503b4888e4da809ac6869929bd33df0776177f10e4416e0879fd0672
6b60be2abbe479f57f83c9af4682c2c8c65c98574307f920f5a0a7a47a85f72a
58a2de7b3b5c4a1719b35fc1fd37811fad749bb81d794fe675cfba1f83f6e064
433875f694fb7f96b4fe51e4c3d9a45515e849d1ffd9aa528fb9b23f6323e106
81493b11fc6acd0d4d8bb653dd9fcdaec16affbcbb509c01f6377db68efceee3
e224be036759ce0a8611d9863a0e6def4db9d5ea45948d63b82ab42627a8c919
e3493fea655027d88224954f32985caff0aebaa858df3314747f6f4e4a92ac8d
5886ac60da0c972c25c3a67c3cdb025ad5f87b471c5bf312b14e8671983d4201
b2d554660744869010b032ae7442f6b9f78ed4918d9e23c669cea4bc592236a3
ddee9852f4a2b0bfa861eadce78e0366b3554b03f5619a1dc7507cd285b8a393
57aec830833d4baed7936376d3985d14c8bd5020bec6182ee00c8885b0218282
a0424f14aa77301280d5ca5cbcb30ca9865c32ef0be4e33a65b0175907f163f4
e998f113f94fa5fd31b4c62ab245f5bbb163ad5e39ad2613f12efa9c8ceba6ad
accdf7be34e793269c8e340d73a34199a9a4b3503e9b2120e9f3ef250f18922c
5c3c7ca062428645ef199eea00b98ded1a1d97d8d534a3c9652a6b077349a395
240d0e4653fdcac298777ad397af4df50fe355aa87fd82146ae40e9e998eab90
f318f43399f0472b9ad8aa6667b47c2736f9beb4a4411c561af102016f7319c0
fc95f4af5d0e0244e4a9556d908f0a9279bcacf0ac243f088e1971af7436c6335
bd2bbb9cf42fade98a4c9df8b28b21eba5015e23883d09b46b73a92962748000
34de1542ad6cd0f8dd003c061efd1618696ca1c06343fc7532a880ccd2b497c2



KPMG Cyber Threat Intelligence Platform

Haron ransomware is the unholy lovechild of Avaddon and Thanos ransomware



Indicators of Compromise: Hashes

693b7b4d0546eafa22837413e7c98f18d276f1c6a2459a51371fc29b9d91b625
1a2eb88e8c189acb63177f0f27050e067340ccdec996de672f20f02f46f7d292
48d7cd572f14aed7a90d6b66097a885a889e6e7416a6aaa2eb442706fff661275
91e2140e38cab5d72b810dc8a3b0807cb6e7fb09e908379bafb4858ad15bc941
32643547aefae01363ff01beb15fa818827896088670a78e814a227ca120975a
238a008d432b20076b075ba8ad25412a39f7c44540a59913e5d36a4c23d6c21c
c9a588001a2cf732b6636aaef03c9d147a37d122681de7d16e3f0f4c3717351e
3d89284d1531d1f3d9c307f712d5fd8cc9f30bfa486e883265a9e0809fde4beb
adc75b7ab8b9296814d8f9c23d6033b1eb4b45550c1ddab30cdc7654f98dc46b
7e581424371b20d2b5a88547817c7350ac70a83940383ccf4293f38d866a0a84
c14dd4a0831ea2548e1ddfd54b9704fe8ad0057924ede041c8c064b66690a028
8b921d2333babce2c668096229f4fb6942bad3c7a1436b9d209ee05432ede990
74be995266568ae18ab3ceae79b210bc14f7fa433eebca23f92d7f82961e2a3f
d0fb16b8c62a08ebebee2962cfd054b72dd70e2493dfe4fb658d7c3786cc6be1
bc5c264c4dc0207f6d500c47f870cc2aef641c4bf0efa3b1a408b83922cc61ac
cc4d665c468bcb850baf9baab764bb58e8b0ddcb8a8274b6335db5af86af72fb
1733f72d558f1424c27d76992f38fabee06cf718b8c952ed5cc1e610fff8b695
05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
12bc439445f10a04b574d49ed8ccc405e2dfaa493747585439643e8a2129e5e5
94faa76502bb4342ed7cc3207b3158027807a01575436e2b683d4816842ed65d
fcf076de61f050573def84a471da943d940a8c9fd8120021eca893fea9bcaed3
e24f69aa8738d14b85ad76a1783d51120b8b6ba467190fe7d8f96ad2969c8fdf
6e6b78a1df17d6718daa857827a2a364b7627d9bfd6672406ad72b276014209c
d29abe6ed086a5508c54df31010c36cc19fea3bdc5d521ee7c0d7063a51bb131
cbdb04d23e395b270e16d7ca81cc6b734039fa069932989d4e4f4d4d266df28b
caf815381680cfa6afedcd7c7af5a5c838788b1c7ec593ce817114a25ab63441
81411c9010f2adcb4758bac5ed6128d5a76b24689d477f6ed2c3003fd57e4f3b
66ed5384220ff3091903e14a54849f824fdd13ac70dc4e0127eb59c1de801fc2
4852f22df095db43f2a92e99384ff7667020413e74f67fcbd42fca16f8f96f4c
c460fc0d4fdaf5c68623e18de106f1c3601d7bd6ba80ddad86c10fd6ea123850
0f081ea4e30ca05fc2977235bf239992b17fa9968b58b001990e4539f0899269
2c1af1c839a00a2cc88a60faab2d417d86c80a2ab4e7277ccea9d8f9d696b846
402a0160c6a721ba0bbf9acaace1b82d8c7285b964e5b4aaaac133d1c8ec79a6
01aa2cf8db4badde36f1896d341e31c0fe91a51772f1aa50b9f59ba368973993