KPMG

Threat Intelligence+

Zeoticus 2.0 : an offline payload executer!

Zeoticus marked its first appearance in early 2020 followed by an upgraded version named as Zeoticus 2.0 in early 2021 which offers an enhanced offline capability of deploying a payload with no dependence on C2 server thus executing payloads without connectivity. The zeoticus revised version is specifically designed to function for all variants of windows, additionally, it is restricted in some countries namely Russia, Belarus, and Kyrgyzstan given the backlash imposed in these regions.

This attack fixates on speed and efficiency resulting in rapid encryption and hiding its track by destroying certain binaries by using ping programs. This variant is believed to encrypt and rename the victim's file and change the desktop wallpaper and thus creating README.html ransom file. The required files are recognized using extensions by executing the Zeoticus 2.0 payload. It's worth noting that the encryptable-extensions list is totally adjustable and under the threat actors' control. The malware encrypts files using both asymmetric and symmetric techniques. On the symmetric side, XChaCha20 is used, while on the asymmetric side, Poly1305, XSalsa20, and Curve25519 are combined.

Following the encryption procedure, the files are updated with extensions including the adversaries, email addresses as well as the string "2020END". Zeoticus mounts a new volume with the ransom message inside. Instead of using an onion-based payment site or something similar, victims are advised to contact the attacker via email.The group has been specifically targeting windows OS with advanced encryption algorithms. The continuous upgrades in the attack makes it inevitable for organizations to contain and mitigate the risk in the ever-growing cyber space.

What should you do?

- 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.
- Implement well-documented and tested DRP and BCP procedures.

What is KPMG Threat Intelligence+?

The KPMG Threat Intelligence+ approach is an industry defining, research-based capability for enhanced visibility into cyber threats. Our machine ingestible feeds are the result of automated, sensor-based intelligence metrics with dedicated, expert analysis of each threat to provide you the right context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP. These feeds are additionally co-related with out industry partners and independent researchers to ensure you have the most accurate and contextual data. The intelligence is then curated from Strategic, Tactical and Operational perspective to give you 360 degree 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.

Range of services

- Strategic Threat Intelligence Report
- Machine Ingestible Threat Intelligence feeds
- Threat Intelligence driven pre-emptive Threat Hunting Exercise
- Cyber Incident Response Services

Contact us

KPMG Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security, KPMG India
+91 98100 81050
atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG India
+91 98455 45202
raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG India
+91 98455 65222
santhony@kpmg.com

Chandra Prakash
Partner, KPMG India
+91 99000 20190
chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner, KPMG India
+91 98181 99432
mtembhurkar@kpmg.com

Rishabh Dangwal
Associate Director, Cyber Security
+91 78277 54752
rishabhd@kpmg.com

Threat Intelligence+

Zeoticus 2.0 : an offline payload executer!

Indicators of Compromise

Domains		
vitrez.xyz	o08a6d[.]top	sitcalls[.]us
so118[.]cn	c6tjvl[.]top	sheylter[.]top
yu1u[.]org	vcev5c[.]top	goodslet[.]win
00508[.]net	gwz8gh[.]top	goftegoo[.]info
e6in0v[.]top	lxvmhm[.]top	somegave[.]info
d4rksys[.]cc	glg1i0[.]top	zenoproxy[.]org
025021[.]net	bvbg1l[.]top	the-tech[.]info
vbfyit[.]top	gre2b6[.]top	fenstermane[.]org
bw9e2z[.]top	rys9pj[.]top	blessingsxx[.]top
5p76tw[.]top	03337[.]info	falloutgood[.]top
85kvie[.]top	wet4io[.]win	wonderworlddd[.]top
63rx85[.]top	bmores[.]info	margate-zone[.]info
wwa4tu[.]top	bigfind[.]net	supportalpha[.]info
va3ibn[.]top	mykings[.]top	koessammcorng[.]info

Hashes	
d0e87fd356979aff2a420957ec070d54	941572dd276820d51760636ea7b4059c
acfd37368e16de42a7c224328bff31a7	90e6d826310d0ae894cfea1ac5d859cf
9fc80c55ecd0f69ba7d399ffa2014dc0	988dfacf31a8245a2beb6ea3ee13f4f2
0d8081418a6a09732bb5de4eed738b09	0cbe2007f4f89d7b78b83e92bcc7355d
5bc69b6c01ad36ae4a8c5dd470c56904	d3449118b7ca870e6b9706f7e2e4e3b2d2764f7b
25082dee3a4bc00caf29e806d55ded5e080c05fa	a5537c7cae031521b8dec2343d3d3c5914649dbc
33703e94572bca90070f00105c7008ed85d26610a7083de8f5760525bdc110a6	
279d73e673463e42a1f37199a30b3deff6b201b8a7edf94f9d6fb5ce2f9f7f34	
b541a9f64fe12c31fff460ab0deef392a8441eeb102805ed578effc6e6eaed96	
b3923d52a2bce6fc3afc0088d7113dbfe6d10038888a987983dd2abcce059262	
5bcef99228e28f024a4ee3a0a76d6436368cb411c4ea21b861afd89a200346b5	
ce87ccb8f821f18082c36b4c128d5f2cc66db3619fb3aa4e858b8fc179cfc5ca	
279d73e673463e42a1f37199a30b3deff6b201b8a7edf94f9d6fb5ce2f9f7f34	
0b67ef08680265244b33100c8fff13d0aecbc120bbf1bbc2b8ee0c6f276ac97b	
17c605ac63ad35a1ea57cb8a617388b4ed32b8e08879ac1eb61ff65600241f56	
1f4a221185501553d9eb7d1a93650b5edf6a4ad9c5a2aaa07364e1f397225c6a	
28524ec1d3013a8e8581aa3baf86646bc6825c5b9706a52e6cbded53989d3e0e	

Threat Intelligence+

Zeoticus 2.0 : an offline payload executer!

Indicators of Compromise

Hashes
310dc1b4d13c6c05a90bf736fc8c142ac3a5dd96043be2e104a1a61e7a086b9f
32766ab73e5a7bb872ae29a7909a45925c964a288f81f46c3dbe9a20be070165
3834d9b65bb302d21397174e73063865fddce84381d7ad208f5895899c67ebd4
44ca2c8e5f82150c6f7913bb7cf94b1de03365bc43d2f03dac180348f7adf2a7
4acb805fc49936ef47013e4cc9adc94c44dbb9dc5c207f7db52a80513877450e
4d44e032bb4626c22deb965fe57d449bec824eb4cf5b59b6b8031746326f8db8
4e3257864663355e0ef0e37eaa979bf21dd877f5c9fb111caf2024e31d7360f0
50408bdbbf4c80e4f8086f4888644aec74167373004badfaa731d9d1ba1014c2
505ff0ba0f8b94bdd7ff271a4819192430bd3dcb519534881bb87b080e523e7b
5876e678569988df2f5545ca1dc69d882014ca112923cb9367f98e1f47c1c297
5997d81b7f368b1c1d95a350556c10c15048ff914e6265192fd8c3d8800eb990
5a90ba7ab388a61427343daea09b969267b017849a5739047bf9b33a7c2e1149
5b961a4568384d7de29778219e545169d250ae3b40a628af2f10ecc3e000f2d7
61993134F49545F747A513A027CC6C907531098D069AF2CFB3B8CE06F4789289
33703e94572bca90070f00105c7008ed85d26610a7083de8f5760525bdc110a6
66a1143cc63214c3a61889e9c8963902c3e32a1b2ba119d335b1892d11d4f741
085b8d0ff06597100f7419e094e04e1a7567b2b9ad3f64b6972ac8419374ed3d
0af96358a3aaa7e20f18f44add2920b86846b90f7b292bc4c59686dd2ee83c72
113cdb7afebc9c0ae38fdc7e58236eb5a6acec256e108a7a0799cef4b65ac794
1205e1c2466300c1e78e2d0d91b064f25f54016926c1fbb8dbbee7cdd9b13595
1267ea52b6980e8964ce6b6d72dde5f406b2ce58fccbec9bb1f90d0381f416e6
1AA6996E82E57D61B1EB147BC80C69B7354A14CFC915A9FB423526C779A64378
1bc915f035b3383725f22b86f78083a8c1affe308a4bb1ff52d85816f1e54132
1d9d2409d7806116d8e9348fcc28017f8bb283c46eeb303523a3fbede76e18aa
1e448619d16e7eb7128434dc40607d826fb31bebfda27724a09ebd45b044b8a5
1f74b3080d31ff9d3cf867b3b2738ee74fb7257984d57788e463250155c68c96
21b78ad72325f2c9c0ccf9e4159e292e3db3035ee7c66700bb3b608f7fdecf34
2216b761678ce1d540b023280a86525b2498942aeef82fe997bb4a64e6c108e0
2bfbc39f86c598f01444aae326a452f2f5f1d04cdd7a2d93249cb5dca687c266

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.