KPMG Cyber Threat Intelligence Platform

Titan Stealer – Another Day, Another Stealer

Titan Stealer, discovered in November 2022, is a versatile Golang-based information stealer malware developed for stealing sensitive information like credentials, crypto wallet information, FTP client details, screenshots, etc. It comes as a new addition to the family of numerous Go-based info-stealers that has been on a constant rise recently. The cross-platform malware has been actively targeting major browsers with support for popular crypto wallets as well.

Titan Stealer is distributed as a builder, offering extended customization options to attackers. The attack path starts with delivery of the malware through telegram channels & phishing websites. Once the malicious binary downloaded & executed in the system, it decodes the XOR encoded Titan Stealer payload in memory to evade security mechanism. It loads itself in the memory of already running process of windows legitimate "AppLaunch.exe" via process of hollowing. Post infection, it steals system information such as computer name, IP, country, CPU configuration, list of installed software and sends to the C2. In addition, it also captures browser information, cookies, saved browser credentials, including cryptocurrency wallet information & FTP client data from Windows AppData folder. It then compiles the stolen data, compresses into a zip file, Base64 encodes it & communicates it to C2 via a POST request.

Titan Stealer has been observed to use padding to inflate file sizes to evade security scanning and hence organizations must be vigilant with the configuration of such security monitoring tools. Restricting access to instant messenger apps such as Telegram & with sufficient training of personnel must be carried out to ensure safety from such threats.

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

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.

© 2023 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.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

Indicators of Compromise: IP Addresses
77.73.133[.]88

Indicators of Compromise: Hashes
0f3ac2b54489cfb63beffdec269c9f0e
b07263f74d432404b68c0bb1ad2f7844
00f0b502e17c9525e9e52ac8f524b525
b7729d9da4b68849baad56b115fcad79
d79252fc03409494c21963842bb880c7
2bb3b6a9e445047087fe27ecb1cac2dc
6e090ecf5cc303cf305932c7998e8553
cbe8e15c575d753324413f917ecbe245
e7f46144892fe5bdef99bdf819d1b9a6
b10337ef60818440d1f4068625adfaa2
b0604627aa5e471352c0c32865177f7a
a98e68c19c2bafe9e77d1c00f9aa7e2c
78601b24a38dd39749db81a3dcba52bd
5e79869f7f8ba836896082645e7ea797
1dbe3fd4743f62425378b840315da3b7
1af2037acbabfe804a522a5c4dd5a4ce
01e2a830989de3a870e4a2dac876487a
82040e02a2c16b12957659e1356a5e19
7f46e8449ca0e20bfd2b288ee6f4e0d1
2815dee54a6b81eb32c95d42afae25d2
2155e10488f0e1bec472c6c80ab23271c94f18e8
5936d4e9771ff57ac41852eae6865418fe041e1f
a51f8ce5cc8bf6c82bcec3caf1836059d729ebe0
f380628ad32e7a2b805e73802d9c33b3b19ccd23
94efe24e005bfb0158559978a7555800bc2a0415
4221774bb845ec56aa02b63dcb515f177fe31683
87c9bd18058ded5cc0d3e0d409a27c485a9dcc7a
b5f00f28d9c7dd66df6d2151a6fb52d908504b10
763ac1ea8c3de617457f64a8ce4eabe7ab8a3abb
48fedb8fbbb3c7adb5eff891c713c0decd6a6c07
9c3f46f24a2fc4dbab05abc0012197b1026a5bdf

KPMG

KPMG Cyber Threat Intelligence Platform

Titan Stealer – Another Day, Another Stealer

Indicators of Compromise: Hashes
90097f106675b3ee460a9d32f94d15cb6f8daefe
70f91a528227f6746fb932deb2b3f1e4011953ee
119f5b7da9e57bad8b618c660d21a91d06d1795c
c9870daede50e20cb277f77c6c7971b901dcabbc
a7c64edea5f345f6da9160e113f1af34c5b91acf
a4bc61e671875a5a63f3221b9e04d9295bc8e5be
9620f97ab57a8c274f661a70c96f546e6fd30f82
1285315ced4d787fea9f8f05d6a3620c08bae42d
0e4800e38fb6389f00d9e35f1a65669fecb3abf141a2680b9b8a5b5d255ae2cb
6e96dcad29a10b63f89f50040f107cdd29e850aa21c5831344976953f6704ff5
28ed2fded652523af511803dbea91b8cefc040ecec703b5308a6c849fb009888
32e1fafe04aa05424aaf18bca254760e87bba0114a16788a06768233ea9b70ab
129c9bdfe44b7b79abf04f56b35a65edd43d63b6294c7f05a3d140413533f385
dd3730841bb62b131a08cb37fbd8e1e541fb9cab6baf6c378e84d1c77e858e3a
e4584bb5db986d9f64297863cd5a7c4062aeeb7e4775dbda4d93d760406165a8
e01264912f6b5d3f3cd84261b4b19408c317e06f83292d6f2ca87ebfb0b71fdc
67e3b73fd085d36488e82c8421869343be3a662949aef2a9fe0e89aca343cf4a
9a50a49f8516855ecef0ee02c073a69357ee0836507df64f7c5ec88e71646f0b
b12da9cdf5de68ce96b9ef156eecfc11cd64f0f1ceb6a5b0f2309dc50029688e
eb8faad12b1bc7657060878a8b672344c95a0a6cdedeedf7b2702c7add6a815d
e252a54e441ea88aafa694259386afd002153481af25a5b7b2df46d17ac53fcc
c78767cb268589c7e3519f8643c7d7bc891ee3e8f8660f9340419af278ade263
aea823d6446fbf9059391125a9b7fceb9f433b846275d28dc5f433645984a683
a7dfb6bb7ca1c8271570ddcf81bb921cf4f222e6e190e5f420d4e1eda0a0c1f2
e54a6551dd6e290cbe53d9ceda9e6d2bf36c1010ee939f3192c97de6b5a2650c
af58e830feef2f4086fb52dafda6084b3b85c6200f4cbc35a5460fb703dd39df
4264a0c8d7acc6f10539285aa557a2d9d0298285b0a75a51a283241ccf11c94f
421dbec55ce3481c5cecb630b4d216bacd07ce35a912abe57af81a3641414e83
30c1f93a3d798bb18ef3439db0ada4e0059e1f6ddd5d860ec993393b31a62842
152ef5fcd0278e127c3df415018857f3aed0a7481600323567868l5ccbe870d5