KPMG Cyber Threat Intelligence Platform

TimbreStealer - Mexico's Cyber Users Under Threat

TimbreStealer is a newly emerged obfuscated information stealer, active since at least November 2023. It employs sophisticated evasion techniques and stealthy execution methods. The malware targets Mexican organizations, notably those in manufacturing and transportation sectors. Previously, the Mispadu trojan has been seen utilizing similar Tactics, Techniques and Procedures (TTPs) as TimbreStealer, indicating that it is highly probable that they are operated by the same threat actor.

Initial access is achieved via spam emails with financial themes, containing a malicious link, often themed around Mexico's digital tax receipt standard (CDFI) or generic invoices. The link redirects the user to a compromised website tailored to detect user characteristics, like geolocation and browser type, ensuring they are in Mexico. Any attempts to access the payload sites from other locations results in receiving a blank PDF file instead of the malicious content. The compromised website uses JavaScript to profile users and downloads a Zip file containing a .url file, which triggers a download of the TimbreStealer dropper using WebDAV via HTTP. Utilizing advanced evasion techniques like direct system calls and Heaven's Gate, along with complex decryption processes which involves a main orchestration DLL and a global decryption key, it thwarts analysis. It also incorporates multiple layers of protection and anti-analysis checks, such as VM detection, debugger detection, and sandbox environment checks, to impede analysis attempts. The malware contains functionality to communicate with remote C2 servers, facilitating data exfiltration and receiving instructions from attackers.

TimbreStealer's sophisticated techniques in evading detection show its adaptibility and resilience, posing a significant challenge for cybersecurity efforts.

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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

TimbreStealer - Mexico's Cyber Users Under Threat

Indicators of Compromise: IP Addresses	
157.245.8[.]79	146.190.208[.]30
167.71.24[.]13	167.71.245[.]175
24.144.96[.]15	167.71.246[.]120
45.55.65[.]159	104.131.169[.]252
24.199.98[.]128	137.184.115[.]230
159.89.50[.]225	143.244.144[.]166
159.89.90[.]109	143.244.160[.]115
64.225.29[.]249	157.230.238[.]116
104.131.67[.]109	162.243.171[.]207
137.184.108[.]25	192.241.141[.]137
138.197.34[.]162	

Indicators of Compromise: **Domains**	
trilivok[.]com	manderlyx[.]com
chidoriland[.]com	bailandolambada[.]com

Indicators of Compromise: Hashes
df58b6143d1bba75d6e65a6e5cd79003
8337cfac4e8b63d96388f3318d8a51e4
8838d90e769cdc48e69c6f239a8c326f
d1fe45c2cf8719610260e2b7d9dcc4ed
0eee9f539ff70bb55830c1444b82d62b
337e6ce35c193912ee1703919cbb30f4
fa8005568c2658a02c352c81f8fbf473
4b27f900c2b4b50dcb06c7f1dd2412d
fe01a7923688dbbaff8173fead0d233a
73df841035605da559cb74b5d8e6e15e
5c0b4b99c02bdbed832e9af387d6bb28
a9df12daa3b559010baf3b3bd5e99c33
28cec4bc9b5c68f0848d6500c67f3872
ee79b70841231848eaa52968179cec91

KPMG

KPMG Cyber Threat Intelligence Platform

TimbreStealer - Mexico's Cyber Users Under Threat

Indicators of Compromise: Hashes
2c48f33ac9ab35ec7c2ee1a141bbe77e
88470a85faefdbafb1b698dc559ada5d
5098ffb7635e3b87c1476aea7d24a5bf
16aaa21f531698a2df00e906ee53835d
726175e6bd21f0134e02b6e39c71f198
0de0ff7772ba3f07d8cb48b88cd93fa9
1c70ec284abdd55518826d5c5c5e4fa9
757c47d750427d53d6a52c07aa7b7238
6b87b448de7d8a83247df231f3087e82
eaf31912da874d6b9ddce32a8f8adc5b
9a45e2fd79a40613676cec146302c779
6ef09ae3a05ab1656790f1d7275170a1
dd4e46c178ba7285d802f2ccc4697d31
07e70d303c2af11c47f04043fd67875b
d8570c12f3bc947595793dd91edacc6cdbe52f9d
e51aa687911999f40e2c7da36f065f4fa17b7252
8ecd4a57b3ff22290180d7be4a2a1d9a8f2f1f7f
e90c95847ea7f07fc46b26ba9b769c530decbc7e
10b290f71881fa82511e8cd9dd79db79d038dcfa
f9bd86bed122e3a0a45d76217446c64bae6f4803
73112dccfac77a318ded5c5baf611f863e74a281
36a90cb2fc55f3ef9697cc8258f46c0f4ea01b73
b3abc70af4f704c695251c2493caee5dc56d910a
6aed95f2b7cce6f1101daf23423ea780d8e24812
39896be1e2af82ce77574e478ef79dff27c6f749
d516331c470a3d753514c08dd0ccc870ed58ada1
1e04acb41fc94cdf254f2f6e1d6896ddbb704a44
cf45d0ce71a76516e61a83baea89d866a0e3c728
eb2b583e6af7af2ba4e3813b29c11b4f58de2f2a
353eb2e1b9f98683042708e445f0b5e0718981a3
0d2caa35bfe1bbdd04adf966da0da05a2fbaec1a
da9ae8f1f92a32fa17047923ddafdc3ac17d88ca
efc532207c4cfa5b6ff11dec8be25f589d1aa785
0f333bfcaf8ba04cc359b46881742f32985b3d2f

KPMG

KPMG Cyber Threat Intelligence Platform

TimbreStealer - Mexico's Cyber Users Under Threat

Indicators of Compromise: Hashes
1ebde5f94a0ef90393c51a04890c8cd09e24124a
f12c8e57665af24fa7adbfa24113f9570109ac58
4a3a4bd11e5a6f0fa44dd1e4a4154c8dd2c110a8
cfc55dd6ed0791037970f15594919b6b0dbf8380
1190f4410e641e62a4c01bc611be66d4a6d48c7f
9852d43546fd4ffaa1ca6d6de391b89b86df52bf
360937f8abf3b00ca8e684d96547e0b4e8fdb178
5189b4a5d6d8f9c0959ebf02c13681dbd94c1621
a83e163cc235025eb245dca406d64b51fc7c9937
8ea1dc5f8ed2eb0ca8814789b83b9a90f39e872a
f44d7447ed965c6a6085f66165b03809d9c2bf95
6f2788559e1d4a315f215e841162b2144dd1e310
07fffabfcbeb05bd7f134b6b6eb2a6e5ef38eca3
28eb4c9ba859a5cdabb489facd31f7dbf209e4e3
5b8d6252ad6d942a04d764552cf9abde700111bb
af3cd3ed49ef9b7021f9e6310884b7e4780762c4
50fa4755fd48e1b22a718b6a90b46dbead28fcbd
b1951a9a39103902f54d7a96cf75c382f36d17f2
6e07cf69dceba73b70a2f285b98eb7cd23494bd5
490ad59df91f955f39866d3e3f1ddbed2b423f72
0692c9bae14edd2371df8eabe9aecb0e81e0318d
41a635bad1929a494c56831cca8013660e61d27a
12bff33da7d9807252bb461d65828154b9b5b1dca505e8173893e3d410d40dd0
1aaa4fb29a88c83495de80893cd2476484af561bb29e8cdfc73ce38f6cd61a84
23b9e4103141d6a898773b1342269334e569bcf576cdcb4a905f24e26320cdab
27c1e41fde9bc0d5027a48ccada1af8c9c8f59937bf5f77edd21e49bd28f29a2
2a225784289f31adbaa8be0b8770495fa8950fce2b7352a0c7a566fc79067547
2a38b75e88f91f9cd28ef478e82c3b44f50e57cb958ba63e58f134d8bd368812
2a3f869e9e78b4d7945a60ceec27586c07bc8b0770be64463358fffe3b6b7395
2e04c36b7ddd6939b7bef258bfeba6f91a5c37a43389dd6d9a88eff5863df5ed
43e99539e4b966dde2f9de8dc1ffb4a22bc560e54c01de9aef6b15fac1412714
46226d4fb7ffe15ba8167e3724f991c543731672e19ef40bb43fddc6df648d0a
46cc07a9287da26e238a74734d87e0aae984f4648a80a26547afa0de8c850afb
51be3a3b4ebd15c305c0f9b57388c449f88f0d6d2d46a0a838f046f0fd21b78f

KPMG

KPMG Cyber Threat Intelligence Platform

TimbreStealer - Mexico's Cyber Users Under Threat

Indicators of Compromise: Hashes
55b0247b9b574978a4c9abd19c3bcc04ea78598398b9f8aeb35bd51cbd877576
56612bb0ab00cbb7af24326b027a55ff25852ddab1f1c8e24471b7ce97003505
5831f4f8ce715d4a021284e68af1b6d8040a2543484ac84b326eea20c543552e
58562e49c1612f08e56e7d7b3ca6cd78285948018b2998e45bd425b4c79ce1f4
62495620b0d65d94bc3d68dec00ffbe607eacd20ab43dc4471170aa292cc9b1a
682546addb38a938982f0f715b27b4ba5cda4621e63f872f19110d174851c4e9
69019b7b64deb5cc91a58b6a3c5e6b1b6d6665bd40be1381a70690ba2b305790
6bf082f001f914824a6b33f9bdd56d562c081097692221fb887035e80926d583
7923d409959acffab49dda63c7c9c15e1bdd2b5c16f7fcfe8ef3e3108e08df87
7ac22989021082b9a377dcc582812693ce0733e973686b607e8fc2b52dcf181d
8420d77ba61925b03a1ad6c900a528ecacbb2c816b3e6bc62def40fc14e03b78
850dd47a0fb5e8b2b4358bf3aa1abd7ebaae577b6fc4b6b4e3d7533313c845b8
96363b2b9e4ed8044cb90b6619842ba8897b4392f9025cbfdccfda1ea7a14a58
97157c8bbeb8769770c4cb2201638d9ad0103ba2fdfed9bdbd03c53bd7a5fcb9
a103b0c604ef32e7aabb16c2a7917fd123c41486d8e0a4f43dcf6c48d76de425
a82fb82f3aa2f6123d2c0fb954ae558ac6e8862ef756b12136fbe8d533b30573
a92934c014a7859bd122717f4c87f6bd31896cb87d28c9fac1a6af57ff8110f6
ab2a2465fccd7294580c11492c29a943c54415e0c606f41e08ce86d69e254ee4
ababe815e11b762089180e5fb0b1eaffa6a035d630d7aaf1d8060bd5d9a87ea5
b04a0a4a1520c905007a5d370ed2b6c7cb42253f4722cc55a9e475ae9ece1de7
c29b9f79b0a34948bde1dfca3acecca6965795917c7d3444fcacba12f583fb98
c99237a5777a2e8fa7da33460a5b477d155cc26bc2e297a8563516a708323ead
ca652fc3a664a772dbf615abfe5df99d9c35f6a869043cf75736e6492fbd4bea
b5a272acd842154b2069b60aab52568bbfde60e59717190c71e787e336598912
ce135a7e0410314126cacb2a2dba3d6d4c17d6ee672c57c097816d64eb427735
d3ff98b196717e66213ccf009cbeed32250da0e2c2748d44f4ee8fb4f704407c
e65e25aee5947747f471407a6cce9137695e4fee820f990883b117726195988c
e8ed09b016ea62058404c482edf988f14a87c790d5c9bd3d2e03885b818ef822
febf9c5ede3964fdb3b53307a3d5ef7b0e222705a3bb39bef58e28aaba5eed28
ff3769c95b8a5cdcba750fda5bbbb92ef79177e3de6dc1143186e893e68d45a4
010b48762a033f91b32e315ebcefb8423d2b20019516fa8f2f3d54d57d221bdb
024f3c591d44499afb8f477865c557fc15164ab0f35594e0cfdfa76245459762
03cd17df83a7bdf459f16677560e69143d1788ce1fc7927200a09f82859d90ea
075910c802f755d3178a8f1f14ee4cd7924fd4463c7491277bdf2681b16e593c