KPMG

KPMG Cyber Threat Intelligence Platform

Casbaneiro Malware - An Emerging Banking Trojan

Casbaneiro malware (aka Metamorfo, Ponteiro) is a multi-stage banking trojan that was first seen in 2018. It is financially motivated and targets financial websites to steal credentials. The threat actors behind it have remained active over the past five years and have made changes to their attack chain, techniques, and C2 infrastructure. Recently, they have been observed using a UAC bypass technique to achieve high integrity level execution. The malware has infected numerous countries globally, including Panama, Spain, Virgin Islands, India, and United States.

Initial access is achieved via a spear-phishing email embedded with an HTML file that redirects the target to download a RAR file containing CMD scripts and binaries. Post execution, it sets off the events to deploy the malware along with scripts to fingerprint the host, gather system metadata, and leverage living-off-the-land (LoL) techniques for evasive actions. It also downloads 'Horabot' malware to spread the mail infection within the organization to evade email security solutions & it utilizes a UAC bypass technique to execute code discreetly, exploiting the legitimate executable 'fodhelper.exe' to avoid UAC prompts. Further, a fake folder is used to side-load DLLs with Microsoft signed binaries in 'C:\Windows\system32' with 'fodhelper.exe', which facilitates UAC bypass and evades antivirus detection. After bypassing UAC, the trojan binary is executed, which steals financial website credentials through keylogging and form grabbing. The malware then gains admin privileges and exfiltrates sensitive data for further attacks/profit. Finally, it connects to the C2 server, enabling communication and data exchange.

Organizations should educate their employees about phishing and malware attacks to prevent them from clicking on malicious links. They must use security solutions that can detect & block phishing emails.

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.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Casbaneiro Malware - An Emerging Banking Trojan

Indicators of Compromise: IP Addresses	
185.183.98[.]135	192.53.120[.]76
216.238.82[.]27	45.79.48[.]129
45.32.90[.]70	45.79.52[.]41
139.177.193[.]74	45.79.52[.]25
139.177.194[.]76	172.105.105[.]85
172.105.98[.]184	45.33.53[.]179
185.230.141[.]242	

Indicators of Compromise: Domains	
contactofiscal[.]cfd	wiqp[.]xyz
tributaria[.]website	live.xtream-ui[.]info
factudigital[.]cfd	k9b[.]site
factdigital[.]shop	a93ks.hopto[.]org
cgdf[.]shop	ckws[.]info
serviciofac[.]shop	m9b4s2[.]site
fiscalcgdf[.]shop	newyear1.gotdns[.]ch
a9m1x[.]icu	

Indicators of Compromise: Hashes
b69c72e0d031f64ce4a2da747070a487
1a7a6bf11337f0de5ba28ebd93afed06
d33ea2a1a6d706cee714cd200448273b
0b57acd184980fb9c2fad42f17d534ce
c178834be3a0126360d02c38401c952b
d82a702a6686ac93573f8e32776c642c
0d3d9a765e54499a3addfb3834e35658
c15912564bf2e6a21932c3644738499f
c02a82fcccb6915402a9d159e8a1eb6b
173a24ddf0309c4b34857e865fb3c4e3
6a8daa0a58814132fef76e0f8ab60d60
50f3c6d7145a42d8957b574f00b5d6f1
59754b36d3fa91d9a8cd736d9018c06f
bc23de1e7d7774f4714394419b7f56ed

Indicators of Compromise: Hashes
c56b5f0201a3b3de53e561fe76912bfd
99cfb00d716a4965f9bd6a24eac4ff1c
4c92e519021b2ebb1cdcec2278af0bd9
ed47a9c672de133a15f9f9e2b773fb7f
a02c84518cd357642745cdbe09f8f73eda723eb2
0a553c70955830a30804fa562fff1ffd335a201d
7b4a4f1035e076beb1525a604176e104a7c330a7
8df3e5c5d82ab73b220a233115541676c947e344
fbeb9f7a7a058f49ee9cc13bd6430d07b1843ff3
2a4062e10a5de813f5688221dbeb3f3ff33eb417
d41fbaa6516d553138b992ce9887ced5a55481be
1521d9513137eb4d9566dba7a9d0bba746baa941
88b50eeaa46ac046fa35bbb24f33150034752129
6e18736cd63c60ec853b55e7bcf5c4540ee7290f
c5e6ffae9a8edc7fe4620a61d23f387b06ea63ae
62c493b9f5ec46004f7a5e56ce25b91313487a25
cc5f29915e6d0a3224b33ba5f7a5fa20b32685c9
0c9297ed45cbddd1c1b66c6f20591aa6d7ec1f6a
7097e8a0d0aadadd55b9cfc3f287ab396348ac02
0f032b6c7a3799e4e3c29f5c05cad2c046d52227
1862bd5367fdc5eae0ddd7bc4ab9b55f20eef261
74126d3e5be80f54c6e24a4ce9acbe589f696d6a
217f234b5faa9f40a5e2522baa13d5125d9786ea14bee59c53053a2b8685b61e
c62acf95bf44552f63a3dc44616869c1c40475b971182f52606440b0eebfbb21
88173a9fdd1aa0da81ab0a778d52a3387c57020a4fa2d3b1a5adf08ecc1b7d4a
1c0b9744b4ae0bbd71d477796c013ad38cf128b0d84c54d23fc644867f8ae50f
c1902ea576bf0dd0e26d5c42902466d8bf643554c4218e94045394b00d642650
b9dc5b22a577bb990a062b8078b9a342ed2b4f5b2c2981b3f59f2fa118523418
bed60691140f5f41561048b4a83a6eeb87b26ae9a65c980ff8e6afe372a4f8a7
65c3d43f0f968dcf65ae44d2632d4bfc054afc64a020f2d2f6568af95c443d8f
3cdfdc001bca62ec3ee2e651da89c2321e1b5c2ac5bfdbafdb728c6c3e402f08
29ebe7ccabe41ae84d571be063a8892fbafb9815f5addf86b10fae4942d779cd
da095620a65e574f9854e31a5272338ba9888b0f82c1581b93be328d9f9e955c
407eb313ff6cd9c60714d54d7ee7492e4ed2e5b69e7c9361a0d4a9046f11d713

KPMG Cyber Threat Intelligence Platform

Casbaneiro Malware - An Emerging Banking Trojan

Indicators of Compromise: Hashes
981453e02969a6b90b2316f9a222470d9b47c5c555de9a068da0c1c3e0526448
d96cbd1f18a5d7e2cdf35ebd99e127aa4a4c707b19e948c4875c9ba79f7bd2b5
efef58d7abad4029fded1e9efcdb472ed1a5568eae1087e5fb4d036a45e8bd40
3e788dc51b6272d09bcb9694cbb8ce4dbbbf3cee236f178bc9b78ca700c18c16
b17d981ce6b7934dc1d723f54731aca675c176ef387e2bb0f65ba773dc011379
b7ba6830b7ff812fd2d356d344a390e5ecca7e2a8f6fce319dd6a3f4fbb73a1d
7cc7cef30d3a3f6d233f08e631988f5d8fae8efc16a61645ef959317f1331d94
bda897fa42a43423fee262f4e93d8a65d5d4f622064f96baff3a1650aa9cabc6
ce490c5a133fd2f0bd5c351c4ed582fbbd5c8bda650d267ca0f8f63813104740
2e6633d85c2404a61452645e07a309daf71f6103e1b5b5b8a6cd9466368ca126
8ff493ae2a753d31b9f338553f807a9be7f0be9c3c680e645b7029882fc1eed2
ed1e96e9d06befb13f063b5a3b438610ef9f09a7cb4af0c6186cc79fdd362c6f
680238aa61600ece738908cf7b4b0bd55d8ec049bea2986167b7fa3cd00d9070
362725b3cb081516ad4ac9d1528b530dd69f9244baa396e3dfd3c156d9a25f48
b5cfab7dd42dd20953b2ac13e57ba90039f02f722a15fa0222e3151229fe6857
04bc814b86b881c0e00134c7f20f17306d9149e9fc623ed8afac4b633130f361
f230c757f010bea596a13a00699349a05426d7c9767276a425014226a0b1c9f4
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
e449d87c3fadd6d2a5af88df00af0f609fe67fef79bacf758b729aa1c1a58b1f
6eff0e5eccf96166c4b3319beba635af3b18ec0b8e65f22c5721ce34e2c3456d
507188d71bcf423728a34c4813a0bf39f8a984f1296c9c85b4740985c682f907
be6541dfa193bb7ce04c323da76d7bf52e3ecb3c8e099d3adb9bbeeee119534d
9245d75a27ca65985cdeb27a122ee4989e4e0c9a020bb41f865dfec512b9d81d
bdc0c2040212acde13429e2d329949abe4f2edea24ef9e765616f8b2821e2d76
090e3a1be2b3124e46b65d2593c08d0b45a6660c7f809b238f41aded734d335d
c77016e4f94ae81f5a3cc702b46e32f029d5ffe36a7a10eab7356868ec516085
d997db37507103e19aa2efc0d28c5bbb46ab825828ae756b15b5d39a9adae2f2
c663f0715d083a76d5a13a71e90d3e42a60981055bef4b97da84b1d041f334f5
91b78766844f0771dfad52819e991065c1a248245df0b20c75cdf69ca9cf31be
e42f81262acfdb9a84505deb422a6a7aa799ac017a6619b64bb17a59cf031f85
b8c9a7353f463e93b30d3f5c55628c182580cd982a1901734d8e4ce3c5bcdfd3
89123cd09aa8f99b189da32e3a11268934b95686708a4f74447cb3aaec56892f
43693c3d9a5e83df26d4b4a2baffba5c3ca6c472d5dbc6545b7e299b0e103ff7
9e4290a850ab68b1036851556a7bd53f8e5855d2aea3dd47d6d28c6dc05d4adb