KPMG Cyber Threat Intelligence Platform

TA866 - Multi-Malware Menace

TLP : Clear

KPMG. Make the Difference.

TA866 aka Asylum Ambuscade is a financially motivated threat actor active since 2020, primarily targeting organizations in North America and Europe. This group uses diverse malware, mainly targeting the manufacturing sector, followed by government and financial services. By combining crimeware and cyber-espionage techniques, TA866 employs sophisticated reconnaissance and data collection tools to identify high-value targets before deploying additional malware specifically designed for data theft.

Initial access to the target systems is done via malspam or malvertising. The actor employs malicious Google ads and SEO poisoning to redirect victims to a 404 TDS which redirects them to the intermediary servers where JavaScript based downloaders get delivered. The JS downloader retrieves MSI package which contains more malware payloads like WasabiSeed which creates persistence on the systems using LNK shortcut. WasabiSeed contains a VBScript which retrieves a second MSI package, deploying additional malware like Screenshotter and AHK bot. Screenshotter takes periodic screenshots of affected systems and sends them to the Threat Actor via HTTP and AHK bot performs system enumeration which collects software and hardware information of the victim systems via WMI, and domain identification along with keystroke logging and credential theft. All this data is sent to the C2 server via HTTP. Additionally, the AHK scripts facilitate the installation of Remote Utilities software on affected systems, enabling remote access. After compromising, the threat actor performs activities to delay additional payload deployment. They conduct reconnaissance and gather information within the network, using native Windows utilities and legitimate tools for stealthy data collection.

TA866's crimeware and espionage tactics expose finance and manufacturing sectors to significant risks, underscoring the critical need for robust threat detection and data protection.

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.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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

KPMG Cyber Threat Intelligence Platform

TA866 - Multi-Malware Menace

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

89.107.10[.]7	18.225.200[.]157
8.210.10[.]62	194.135.24[.]246
22.113.16[.]27	212.113.106[.]27
22.11.106[.]27	212.118.43[.]231
37.1.212[.]198	176.124.214[.]229
46.151.24[.]226	185.225.200[.]157
62.204.41[.]155	193.233.133[.]179

Indicators of Compromise: Domains

petnibs[.]com	teamtakeem[.]com
onticweb[.]com	lesaffre-meca[.]com
criminaly[.]com	spychipsthreat[.]com
duinvest[.]info	clarkuniversitycci[.]net
otameyshan[.]com	repossessionheadquarters[.]org

Indicators of Compromise: Hashes

76ee9db5e71a63746a2b2e992cf63544
a8233c9fc267a39cee5363348315b03d
eccad3f43e7107dcc36746617b6608d3
3dfcdc806c5f8d68e3612cb33d49b6a1
5a2888b564f38b46361a22b916889ac8
885e07d2442b5804e73641d626afe3a2
3d37a3c81d3cd4872bd3226a70193051
784ed9c98f7af972b233844e423a39fe
e4bdb253a966dc72a991cff9f3bcacb7
6abc16891a92f3d17a87ddd854247c81

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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 Cyber Threat Intelligence Platform

TA866 - Multi-Malware Menace

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
73e61b03e1bd6944cb7979c470f30606
ad6f99a870d3b94614c37045132f882d
4e7f48435e4da4bdecd44e3265ac229c
e595ce9a9aabe1d9f4ab707e59d7ec34
4d3d117f91531631024614ff8e8b7833
d1e40585f121179ce54898e44fb647ff
cab55d9338840e580558768c3ca95a96
8a6bc8a611db60c474e261987f2f3961ae2e3a01
86037f962d70caf0990d9030b8a33a2017bc60ac
b88c2819763a3df0cd57cead225dbf76006e2acc
3f52ea1eaa25332a5632bbf4ac615eb2e7f8aa1d
74beef3b75c5997e9b99b36f8170f4cca942a4f8
b7ae8ae6ed8fbe0cc4f077953b05cdc1d4219325
3622bf8eeb352eb1d5acaa463e21296b584f5d93
25c21489837fcaf198446e0417a5f5f82dfe4fa9
5ea19a524935d6a2420340c8553d2faf59ea07f9
0e3300b5cf775ee70b227a2e04eb4d4f9fad07a0
24b678cfda21db95e1b7ff04ea7bbc15dc8e3d73
c63a1b9ca1853311ae529b2f000a9ad5accaf909
c7a7f004aa57680af5a6615134eecdea5c4bf189
8643af681f396a71dc0333f787272ad4c3f5202b
418542b364fe762d7d8482ba867823d81a9d3288
3d6c3f4413c267b790784d7441c10bf69be8920b
88973440fa0a96091aabc3858418d21d37fe1052
2ad17a9ffba3cdeb36233acc88de8f1bd93888c3
29490a5776d58e0ef7cf44e4070fe391841c3344

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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 Cyber Threat Intelligence Platform

TA866 - Multi-Malware Menace

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
2a25dff26d7d9a400d2943c9f656c71b303d6664
6163d4c795630a448c6f71da92699d859f54aedb
b897525a5f2b057dad2b96cfc4682ab0e5a39bcd
0b7cd4e81dac6aeefe6102c2ad9b163c9bcf87ca
0856792f4d42c55a0f0be82bd4212a6ed769addb3c8e6d9f2d15e3c263f9f91c
098b9ca77ed79ea2294dd173d01c539a3165ac39d57f518d222b742d8a51350a
0a348f5c197fc2d3e37e047ea54527a57d5894e9d01f4851fb041a41e1870ea6
159b44a573cf090b0491db78caae27d3d16434f491ee3c7b44b6616f8abe9ea9
175b7c0284429a3b1698229b3d2e6ad821c9fdb2a2a2aa3b37e72bb5221f13ad
1806e777841f8cbf9061904941407bfd1a5e4d69ac6944d1922f78192fd2a7b4
25e0b673c015d29419b3b12fb5faafaf497c8e7d91a862faa66a027775901755
261aee196f4795ef905d80da78df3468fadff54086b96f43afb368cbac6cd336
26db2f501215309dad1887ffdd9f89709e841e6ff6b2f68d449cd7c38ef5d237
322dccd18b5564ea000117e90dafc1b4bc30d256fe93b7cfd0d1bdf9870e0da6
37df3ebce0b85765ded0bb7fe9d75a4852b55af4aa204d8aa605666215a07264
39d51698fd9ed5572fe60a03ea0452f9a6416f4c3043227ae49cbb7a40f20f3d
48f7475b0524bba5e3bff34b5f065542b1b916a574c12b2c2357a10762f948f4
498b15b93277d6d3508afca89ccc73b36507c1be372930b3b255fa9bf61be3d2
4baccbd3da535f4167b9009552b6abd8ed03e67c794509698a5a535d687f50d7
51f6c087ed0cbcbf4dde1c3de2fb977289833fc1ce5326a20fd74647ae517a89
5203764aa734a6dcbeaf9aef5d8e1fa053348f80616fa2a9c40586d7af0d1b67
53e4bfd27474f6e4829ac4d625d3d914452456baf5da2c1c51e2e6df35ab634a
608aee1e89c647f01dc2312b1e72d81921b4767b6048df2fef109bb08c5259b6
61487c4ba0df0cc945e0bb9311c82ac6fd223b1524b03035cb2f7c1fd033a9c9
616595555b6804f810d75d014a86ec48f05f4284c7034c5ae89f6acf384744d5
74ee03fc1f447e99de4544611458b9ed16933e3ae23895186c5de1e4c60d51d5

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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 Cyber Threat Intelligence Platform

TA866 - Multi-Malware Menace

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
796df57b8564b51845941ec61a34cc369b24e241ed310ed343d6196fa285449a
7b34f0a3c1978965de94833b383b33e908761de935a77d032f5129b0406bc61a
8573c6503fe4cc00bc5a47fb617b6795a2d07a4f424ed15566258223c07ce616
86709138f2a74fabb142b0d4c0462825c11c5742d0cfb8b6b7bc9726216ac4a6
87235836f641050dff5c278651028653479ec78c44b08a9f8ff8f96c7d613a1f
94c8e3a2e4343d045ee0a2545804dcfdeb2429a9b4d5880101a7ea519475cad7
956c285ab001a301d3fbee0701c8a21bb6c65abc619057bf6c4fce8355461abe
9628fd5a46d334f6f0b5035207d2dcf1812f3aa6b3aff193c4aa4e240c5c9df0
a0be6d44d3ac23049c92e3460372e8fd8a67477787989ec10106b5b521308990
a10cb0d5712a42915b8fc837343c836d13ecca72a6ca48c94cd5e0c2d8a8947c
a223c1b996071f53d780cd3a83d3cb8c0f19e0e87e09470cfb8a5a89437d7c91
b64684e709f291dc1b34873e0103711dd1fbee6751e99f94d891037d94ba8d2d
b762a4d3df7efaae77c5e840f1295d9b848d0d6c302d895e83201c75e1d097da
b9208217e01107a74b51879704cd4b77fef712ad34ee0f7a17b09cb72cbe6116
ca846b3ab356f817316043a910a6a4b361e0ad6070b481895d925e52c07488bb
cbef6b96558db14fa3cd66dfd236466fd62b843e11ca2eef0a1f76b94f7138e3
cc99c2036a6dfdcb1db04f8c794c915d2791481ab7801aa7fec10f6092648a26
d8e35ccb0cf17c6889dbcdf3f7bda92631dca4387efc83392c37175fa38a769d
d9c5f6449862263eca18b7bbc7cd96e1a37c66921c3b22d7e5f6b0a6886203a0
daa0d36ab73999f9c893a073c1419a3dc5d5d531982cdc907992f856a44cf92e
e648ff7ec3386c83bcb9b5689a5f9f45ed9674f7f67a879e6282313e0e6b6ba8
e7177d67d6d07944efb5fc9fa362b0ae3a33318e40bd6d29674af1ac1d39fb91
e8405ce615cad0380af518b0952cb8cfb4045f78a582cf3371aea647a7c53feb
fd0c5f82c90ddf4ad6973e338dcf5fabb70283030571ae95b0a703902ab134bd
fdced8acf85eb205f0ae837fc7a3c408ef4a8f6b9447bda06543912b23efaf1e
fe3237d9fe6302f585fa2cc1206b5a6d0fd71016d404c25360a8420aba7e22a2

Follow us on:

kpmg.com/in/socialmedia

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 endeavour 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.