KPMG Cyber Threat Intelligence Platform

Bumblebee – The new buzz among malware loaders

Bumblebee is a deleterious malware loader used for initial compromise of the system and networks. Discovered in March 2022, it has become a key component in the wild and has been actively used by popular threat groups like TA578, Conti, Quantum, and MountLocker. The malware loader comes packed with features like anti-virtualization, anti-debug, second-stage payload deployment, data exfiltration and can run on memory to stay undetected in the compromised system.

The initial attack vector starts with a phishing e-mail attachment that contains an ISO archive of an LNK file and a hidden Bumblebee DLL. Bumblebee has its own command for downloading executables, injection of malicious code, and making persistence. On execution of the LNK file by the victim, windows native "rundll32.exe" is invoked to further execute the hidden DLL. The DLL then contacts the C2 & runs an "ins" command to establish persistence by creating a scheduled task to run a VBS file. Further, it uses the "dex" command which allows it to download & execute attack-related tools such as Cobalt Strike Beacon, gathers system info & drop AdFind to enumerate Active Directory information. In its recent iterations, Bumblebee attempts a stealthier way to deliver the initial payload by replacing the ISO file with a Virtual Hard Disk (VHD) file that contains an obfuscated Powershell script to load a second-stage malware into the memory via DLL injection. Once the system is compromised, the final payload – usually an info-stealer or ransomware is deployed.

Bumblebee as a loader is in demand among many threat actors and ransomware groups which could lead to high-security risk for organizations. In order to avoid such attacks, particularly ransomware, refrain from clicking any suspicious links, and beware of the ISO / VHD attachments and LNK files.

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.

© 2022 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

KPMG

KPMG Cyber Threat Intelligence Platform

Bumblebee – The new buzz among malware loaders

Indicators of Compromise: IP Addresses	
45.153.243[.]93	51.75.62[.]99
54.38.139[.]20	54.38.138[.]94
54.37.131[.]14	51.83.253[.]244
51.68.145[.]54	51.83.253[.]131
51.68.144[.]94	51.83.251[.]245
54.38.136[.]111	51.83.250[.]240
51.68.146[.]186	51.68.147[.]233
54.37.130[.]166	54.38.136[.]187
185.62.58[.]175	145.239.30[.]26
185.17.40[.]189	51.210.158[.]156
145.239.28[.]110	146.70.125[.]122
142.11.234[.]230	146.19.173[.]202
104.168.201[.]219	145.239.135[.]155
209.141.46[.]50	

Indicators of Compromise: Domains	
phxmfg[.]co	elemblo[.]com
avrobio[.]co	belcolnd[.]com
faustel[.]us	lsoplexis[.]com
lagauge[.]us	craneveyor[.]us
amevida[.]us	missionbio[.]us
revergy[.]us	kvnational[.]us
conlfex[.]com	al-ghurair[.]us
modernmeadow[.]co	prmflltration[.]com
brightlnsight[.]co	richllndmetals[.]com
awsblopharma[.]com	

Indicators of Compromise: Hashes
254d757d0f176afa59ecea28822b3a71
59fc33d849f9ad2ab4e4b7fe4b443a33
f856d7e7d485a2fc5b38faddd8c6ee5c
f035940b5e20a2ecda4f7ea5c682aa84
e2e58c6b4fc6aa36eb5f6b5e6b8743ff

KPMG

KPMG Cyber Threat Intelligence Platform

Bumblebee – The new buzz among malware loaders

Indicators of Compromise: Hashes
21df56d1d4b0a6a54bae3aba7fe15d307bac0e3391625cef9b05dd749cf78c0c
14f04302df7fa49d138c876705303d6991083fd84c59e8a618d6933d50905c61
13c573cad2740d61e676440657b09033a5bec1e96aa1f404eed62ba819858d78
083a4678c635f5d14ac5b6d15675d2b39f947bb9253be34d0ab0db18d3140f96
07f277c527d707c6138aae2742939e8edc9f700e68c4f50fd3d17fe799641ea8
91d29cfe549d8c7ade35f681ea60ce73a48e00c2f6d55a608f86b6f17f494d0d
5d000af554dcd96efa066301b234265892b8bf37bf134f21184096bdc3d7230b
0b0a5f3592df7b538b8d8db4ba621b03896f27c9f112b88d56761972b03e6e58
90576eb6754dd1c38fb4cea4bf3f029535900436a02caee891c057c01ca84941
78c5d780b2ca553cbd3fb0140813e0e1fb7c48491090df605f03c309d0086baf
7db1126c80901edbc3be6948f208d4c450a23ea453ecf2e684bb4c8363c60db0
6804cff68d9824efeb087e1d6ff3f98ed947f002626f04cf8ae7ef26b51e394b
daf055e5c7f843a3dbe34c3c7b848e5bbe9c53b65df2556b4b450390154af3bb
7259b7a91df7c9bc78b0830808fe58c6ff66aa79bb856cf1bf50a107875b3651
ac20f3f9ed0c1e6b2160976a1dc4167e53fbb8c71b4824a640131acf24c71bfd
71f91acc6a9162b600ff5191cc22f84a2b726050a5f6d9de292a4deeea0d9803
f06566e1e309123e03a6a65cdfa06ce5a95fdd276fb7fcbcb33f5560c0a3cd8c
2e349b3224cc0d958e6945623098c2d28cc8977e0d45480c0188febbf7b8aa78
302a25e21eea9ab5bc12d1c5f9e5c119619e617677b307fe0e3044c19581faea
65e205b500160cbec44911080621d25f02ad7fcfcf2c3e75ce33f6f821a808b8
905e87d8433fa58f3006ee685bb347024b46550a3ceda0777016f39e88519142
6727d493d4ecc8cca83ed8bf7af63941175decff7218e599355065ae6c9563c4
c8db63bfab805179a1297f8b70a90a043581c9260e8c97725f4920ab93c03344
261b06e30a4a9960e0b0ae173486a4e456c9bd7d188d0f1c9c109bb9e2281b59
24bf01c1a39c6fcab26173e285d226e0c2dcd8ebf86f820f2ba5339ac29086e5
86d7f7b265aae9eedb36bc6a8a3f0e8ec5fa08071e2e0d21774a9a8e3d4ed9e7
4c3d85e7c49928af0f43623dcbed474a157ef50af3cba40b7fd7ac3fe3df2f15
b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682
9d0fa4b88e5b36b8801b55508ab7bc7cda9909d639d70436e972cb3761d34eda
ee5fbc193f875a2b8859229508ca79a2ffe19d8a120ae8c5ca77b1d17233d268
5ad4fa74e71fb4ce0a885b1efb912a00c2ce3c7b4ad251ae67e6c3a8676ede02
02ea7b9948dfc54980fd86dc40b38575c1f401a5a466e5f9fbf9ded33eb1f6a7
b722655b93bcb804802f6a20d17492f9c0f08b197b09e8cd57cf3b087ca5a347
a60136d7377bc1ba8c161021459e9fe9f49c692bf7b397fea676211a2da4444d

KPMG

KPMG Cyber Threat Intelligence Platform

Bumblebee – The new buzz among malware loaders

Indicators of Compromise: Hashes
86c564e9fb7e45a7b0e03dd5a6e1c72b7d7a4eb42ebe6aa2e8f8a7894bed4cb5
1825e14e1ea19756b55b5ccec5afbb9c2dba0591403c553a83c842bb0dd14432
3dea930cfb0ea48c2ce9f7a8bd98ee37e2feca5fb4da8844890fa2d4f62dd105
52f145a4ccc0f540a130bedbf04370a842daff1ee8d8361c75a8e0d21a88cf5a
4c6a865771fdb400456b1e8bc9198134ac9d2f66f1654af42b4b8fc67ae018f2
fef7d54d6c09a317d95300d10ffcc6c366dbb8f5ebf563dec13b509fff361dc1
165b491e5b9e273a61c16de0f592e5047740658c7a2e3047f6bf518a17e59eca
a8faf08997e11a53f9d38797d997c51c1a3fcf89412c3da8dcca6631c6f314a8
01e22210e07708c0b9a0061d0f912041808e48bb8d59f960b545d0b9e11d42d2
f5218aaa046776a12b3683c8da4945a0c4c0934e54802640a15152d9dae15d43
bc41569c4c9b61f526c78f55993203806d09bb8c3b09dbbeaded61cd1dc2fcc2
29767c912919cb38903f12c7f41cdd1c5f39fccb9641302c97b981e4b5e31ee5
911c152d4e37f55bd1544794cc324364b6f03aff118cdf328127355ccc25282a
f5cd44f1d72ef8fc734c76ca62879e1f1cb4c0603cfdc0b85b5ad6ad8326f503
0650722822e984da41d77b90fbd445f28e96a90af87043581896465c06ed1e44
f01a3f2186e77251acfac9d53122a1579182bde65e694487b292a8e09cf8d465
290b698d41525c4c74836ca934c0169a989a5eafde7208d90300a17a3f5bd408
3d41a002c09448d74070a7eb7c44d49da68b2790b17337686d6dd018012db89d
f98898df74fb2b2fad3a2ea2907086397b36ae496ef3f4454bf6b7125fc103b8
0ff8988d76fc6bd764a70a7a4f07a15b2b2c604138d9aadc784c9aeb6b77e275
2102214c6a288819112b69005737bcfdf256730ac859e8c53c9697e3f87839f2
ee27cceac88199bf3546e8b187d77509519d6782a0e114fc9cfc11faa2d33cd1
ca9da17b4b24bb5b24cc4274cc7040525092dffdaa5922f4a381e5e21ebf33aa
c70413851599bbcd9df3ce34cc356b66d10a5cbb2da97b488c1b68894c60ea69
b2c28cdc4468f65e6fe2f5ef3691fa682057ed51c4347ad6b9672a9e19b5565e
a5bcb48c0d29fbe956236107b074e66ffc61900bc5abfb127087bb1f4928615c
82aab01a3776e83695437f63dacda88a7e382af65af4af1306b5dbddbf34f9eb
76e4742d9e7f4fd3a74a98c006dfdce23c2f9434e48809d62772acff169c3549
7024ec02c9670d02462764dcf99b9a66b29907eae5462edb7ae974fe2efeebad
6bc2ab410376c1587717b2293f2f3ce47cb341f4c527a729da28ce00adaaa8db
68ac44d1a9d77c25a97d2c443435459d757136f0d447bfe79027f7ef23a89fce
3c0f67f71e427b24dc77b3dee60b08bfb19012634465115e1a2e7ee5bef16015
31005979dc726ed1ebfe05558f00c841912ca950dccdcdf73fd2ffbae1f2b97f
2d67a6e6e7f95d3649d4740419f596981a149b500503cbc3fcbeb11684e55218