KPMG Cyber Threat Intelligence Platform

BundleBot Malware - Comes Prepared With Its Own .NET Bundle

BundleBot is a new malware strain that has merged in July 2023. It steals personal and financial information by using the single-file dotnet bundle, a self-contained executable format, eliminating the requirement for a dotnet runtime version to be preinstalled. It targets a broad range of data, including system details, browser histories, Telegram data, Discord tokens, Facebook account details, and even capture screenshots. Since the malware exploits the dotnet bundle format, it has little to no static detection, making it extremely covert.

Initial access is achieved by causing inadvertent malware downloads via Facebook Ads or posts leading to phishing sites posing as popular software, AI tools, games, etc.. Payload is delivered as a password-protected RAR file, of a self-contained dotnet bundle in a single-file executable binary format. Upon execution of the second stage, the downloader component is deployed which retrieves a password-protected ZIP from a hosting service. The second stage is extracted and executed using encoded password hardcoded in the first stage. The extracted archive contains the main BundleBot executable which deletes the Zip archive on execution. The dotnet bundle allows the malware to run without a specific .NET runtime version, making analysis challenging. It evades sandboxes using sleep patching and manages persistence via registry manipulation. Stolen data is processed, serialized, and compressed using a custom library (DLL), then exfiltrated via TCP socket communication or HTTPS to C2 server in ZIP archive format.

BundleBot's covert, multi-stage infection, leveraging dotnet bundle's low-static detection, poses challenges for defenders, potentially prolonging compromise and increasing risk of unauthorized access to sensitive data.

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

KPMG Cyber Threat Intelligence Platform

BundleBot Malware - Comes Prepared With Its Own .NET Bundle

Indicators of Compromise: IP Addresses	
51.79.180[.]158	139.99.80[.]193
85.239.242[.]27	139.99.38[.]193

Indicators of Compromise: Domains	
marketingaigg[.]com	googlebardai[.]wiki

Indicators of Compromise: Hashes
bcc40da7a7a99d431ff18b9678cb37d3
03503ba8c213b1d1fe6e601d2fd6948d
186a105da8509efb73967242e03780a5
19e73e28c10ae26b4d61d9c49eb7ee01
43a03c16ca4d0833dd0631f3256e6785
e71c9d63501af1913f1a957ee102b76d
68f055272cbdbf6535291831170a8635
d106a1d8ac4b243a90f3c8f102812934
7b842f1490bc86770f14beb435f08348
4d99c5c4017fb139210b654ecba12e55
49e9f8641f83c18723403f91f6146b90
eda2868fbbd4a4f8d17bcde9f80aa4d9
53156e5ba921c3dbac245cf7bb354761
168984823dd372d28d0b9fe33fc9a005
69c713244c4d3217f63f7bc414bcfe1b
e4721ad5c12711d6e5da0aebc747a5a7
146f7c388777c1b61b2cc1bd747c070b
ac63b08a3f4550e0ddfd9b74626c1824
bdb2770bb65819b6530b75bc5a2b55a5
99293bd8082e94f17e6e25adcde35d6f
61b06249a291aa732c984ab45f412d19
bbd61c1e3e3adbec0017eafbaa434612
03fb8b7e2c7b1baed7bb5cc04dc550d6d1496410
d5bed74eef3d22bf2e5c09021acf02010116d000
582e3a90ac19c9f2d4d4b3e617b42b4aecdb614e

KPMG

KPMG Cyber Threat Intelligence Platform

BundleBot Malware - Comes Prepared With Its Own .NET Bundle

Indicators of Compromise: Hashes
d194ec7ad4be7a5dd160847fb1d6fda3b09af2f4
8fe5e8e9764dcdd822334aad18726a20bbab4835
e5cf6a260cded9345f7fe8d9ae3ebf1604f3274a
0520f2cd5a05c659e7559fc32e0fd8e28d1c5293
8f929a58bc803493444f442fec6cac7946a96a0b
02e3b1ca2db55a112b649953fa9fc90f2796c13f
cd899f9e5731dda95478b71268943f72aec53d43
6a2a8db6e9c67d76edc635de9405d0b06f60c8ae
70d4344ca343959aa7cbbf6765a205a7241aba26
0b39c01227b1978ffd7432d54c5c9b568390899c
d1ac9e235482d457800d92612c36109f70604daa
1c26cac6604a6ffc27d24a8d8d28e57817e2ced3
9fa4ab23034950841ad33af76603efdcebf43541
35fd805ac6d2ba4cf0fce5fdef1a08df41ac5bdf
3a7183594d23fc0ca99fa3db0478ee84686a5d41
1511e39de4a3b3faf56d7d84bca230460e86a190
b5fadabcca0c94747328d2da21827bc44e35a445
9127800989acf9217b5dd1fdea05e56baca77236
e96a612d820ae04628511b413e2ee097aa7e853c
57c3fcd82ac5f7b0297e3f0b85ca0947309842c7
334b3fc9df7c70132cde575b54c78e5fac813d26
dfa9f39ab29405475e3d110d9ac0cc21885760d07716595104db5e9e055c92a6
303c6d0cea77ae6343dda76ceabaefdd03cc80bd6e041d2b931e7f6d59ca3ef6
90b37f26d7574a23437a2f0ad75d3cce5ecf3928efb58beacedde289fd3568bf
af92d0545ce01e5dcbe228a43babe6281a1631836e5631286908c7f0aa225f3d
25c0f65acb3ecfe435a39bed3f5013eadd85eca1e78a0dc754cb4b82389ee4bb
a99dbc0cb0a051ec68bd89c468fd589b201380f47330bdedbb69f9b076099711
b47ac379cc23a059e1aaaba351f528c5a955fd56da35928c0bc0043c4ab8b38a
3198a613574a8ab84637bf80ebe5f6a56c851aa292973515c5de856f1e958d6d
a1389d02c0b7892ffeae60b7869f3a761c2326629bd1c304839a1e8b7400744e
22bb60b0ea0d5bb57e105287843867880f336ddafa1545332e2de16d412cde12
4b4f69b01edd2c96db6374a9d0d980f5023383d440914831301f19d1d29ae4d9
bc1fceb2d6c5dc7bedfdf1790ac0f06ccf0a9777c79d831d037dff10ae4ace8f
d0146a3bbed91d5680c9b44c0f0e69deabe4d6c0f114e50d9fdee9cd202242fc

KPMG

KPMG Cyber Threat Intelligence Platform

BundleBot Malware - Comes Prepared With Its Own .NET Bundle

Indicators of Compromise: Hashes
1c27a31830946ca806be10d07dc67b185d3f1e2bbc76cd5365719055966600fb
20b833c028322139b81e220cc165513ec2d4a490cfbd84e88e985a84d3173025
0e2bb46c9cb2baa0263824f4a6725a2e4db2541eafd392f25bd9a4921a2e04f3
4c39df6e78b110e4912f3cb543130297b9b3cc3d33daa2d613999a1b991ba763
9b4c6dcee2848e2c23cffe1b8925ebc37d4d98a441fe6b0ff82dc788595a68be
601f888abbb545b003ed37e3835237de7915874893f22ee5bb6ebc9f5db618b5
2038aa28b4e23806030f945aadcf5dbbfa2e3f7ae2b924bd987fda62f87773fc
cd1c00427973b7ff7bac1803d35c071ff0fdeb975c4eb5a54829bedf12c4d136
5ac212ca8a5516e376e0af83788e2197690ba73c6b6bda3b646a22f0af94bf59
67f24b507fe2f6dc06a294b85486cfa1dba6af188e59c51a74adc3b3f9ed29d8
97f777abfeada170c1caa625ffbf12b8d097ae5331f3f4c5b57dad4fc0c4f8c1
8d1aa8ca616afc7fdf3cd6552e94fb486196d67e062adf5c97ada05b7b176985
9e6175a02a129fe559f108f6dced7fb6bf66c468cfb3ca276f3621ab8c312e91
953e1b59b2163ddafaafe7872033ae6351a46500b575a717c853b6393d2c7ef6
230e5844ac0c767baf4d5d660f9ebcd0a9dd7f5a5ec5869387f53fa3eb902aa3
26d0853adcec8b273346924e97170226abd7b800b5ee51f6768c58ac45f59d20
37a06e2e28d16096c45bfd3ef2679fe8dc722810b6f6119b7dc5f1483e66ec01
50b7447d83715b8b7b36a15d0e7c7b8ae881a56dc0f39eb1aa22604e00f97d17
6552a05a4ea87494e80d0654f872f980cf19e46b4a99d5084f9ec3938a20db91
6834be1cbde6718d153a729f2e68e3f3b21bcbcb51a9f381e98f78b7a414969f
bfa7b12cc68b9cd26022a4c611ceaa473c84ffe36bb8008c67c1692b968b88d8
2e0492507ed4127b25e523444b205c58312902fa0bf2f5697c184049af5e4e18
0ba224ecc2546d0a5ccc13bc8f929ec0035ca884fce44c8aebcfec185550169c
0c5ef531c2d5be15ef2a031c381a9531db22e030b14a1c2de311c68da23fef48
41c884718ce264195d75695252b22021680c6d5470a303f999f3f333a5eef9c9
5beb1ce875166ec47ee7fbcd9e48c891fe0b27ccec04edf3da82bf8b3b2ea04b
84319f401994ca83d2659aef8fa5810224f4a0fef2d3ed6883a5a265d3a8c291
9b0a6fdc188de6d80117f9f0894c456e9f541f19ba5b4ed8cfd03e86d8fb8af9
386189e521d431428157cf37b4653444f8c2116ee0a5229313012c43e5839edd
4856cdb407d67ee82d44e1cd606e382cde7b6bcaf9127dd7924e2d604c1cad38
6632c655875279ed1c19937805416a716d9994db71c8e30d2c8b4a3a3c3f9620
7a0cd3cc214b312cda20a54f7e0e93509fbcf5f6e6d9f41fd95d6dfa3bb5bcdc
a47d68411f64887300800cbe471f3cb24047e2e352bff74b810ad1940cfff85c
fca477e3e0fe31dfc14a4bade9828da267b6f234c343f9fb654e6921ba71bd08