KPMG Cyber Threat Intelligence Platform

CoralRaider - Pilfering Financial Data Across Asia

CoralRaider, a Vietnamese threat actor, surfaced in 2023 with a focus on financially motivated cybercrime. They excel in pilfering credentials, financial information, and social media accounts, particularly those related to business and advertising. Employing advanced tactics like tailored malware and exploiting legitimate services for command-and-control (C2) hosting, they utilize uncommon living-off-the-land binaries (LoLBins) such as Windows Forfiles.exe and FoDHelper.exe. Their main targets span Asian and Southeast Asian nations.

The attack starts with malicious Windows shortcut files (LNK), prompting the download and execution of an HTML application (HTA) file from an attacker-controlled server. The HTA file then executes an obfuscated Visual Basic script, which triggers an embedded PowerShell script. This PowerShell script performs various tasks such as anti-VM checks, User Access Controls bypass, notification disabling, and downloading and running the RotBot, a QuasarRAT variant. RotBot conducts detection evasion, system reconnaissance, and connects to a legitimate domain to fetch a configuration file for connecting to the Telegram bot Command and Control (C2) infrastructure. Once connected, RotBot loads the XClient stealer payload, which gathers data via plugins. XClient collects browser and application data from social media accounts like Telegram and Discord, takes screenshots saved as PNG files, and dumps stolen data into text files and ZIP archives. The exfiltration of stolen data, in the form of text files and ZIP archives, to the Telegram C2 concludes the attack chain.

The group's multifaceted approach underscores the evolving complexity of cyber threats, emphasizing the critical importance of robust security measures and vigilant monitoring to safeguard against such malicious activities.

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

CoralRaider - Pilfering Financial Data Across Asia

Indicators of Compromise: IP Addresses	
14.225.210[.]97	14.225.210[.]209
14.225.210[.]98	14.225.210[.]222
199.34.27[.]196	149.248.79[.]205
51.79.208[.]192	118.71.64[.]18

Indicators of Compromise: Domains	
lapz.ddns[.]net	exchangeserver.zapto[.]org
exchangeupgrade.ddns[.]net	

Indicators of Compromise: Hashes
51bad062733f1babc99254ca06db0e46
90a4af96abea4d8179c789fa3c72ddcf
4ae673c323966d2f9399a16e1799f9a1
b86ba0844db442df61a5889b004e615b
82456d523f39ecb87324542c918e7dd6
30a2a6ffdbf23be8dd7e6dd2942b55bc
ad90b65075eef88585d1e070de7c5bd7
c9d5357080b71eff9cd800e29b5b26d5
6dd355c754cc7d3bcdeeeef32fdc16c9
5ad0618df8bab68d45cec4dfa5f17c6d
ef478f6463290ed321e4c07e01280441
8ca351d65a09ff99a340bbcaba22bcbf
ad716385d26c1d33d0b8e3fdc84a3335
30705266725f9bad60ea12821acf740a
8bd7eece235cee14ab700f23b7ac29db
120c6d7e78fb92b2feada47c9d8bbab0
dffa48f29a363071d47fffd114545009
27e96e13a0a538aad23540d52977012f
72b0ca267df69ce8c86440a81cd2f321
23f6b621c70024749217614680a2d2b2
e0f4afe374d75608d604fbf108eac64f
07c47f9b80c3861f219078902b860077
82fce2c2a557e1580c82c9c7e15a8c79

KPMG

KPMG Cyber Threat Intelligence Platform

CoralRaider - Pilfering Financial Data Across Asia

Indicators of Compromise: Hashes
3a326ef320df0d7f111f3a0b27caf238
91a533644f0a1440c82572b563d9eed9
dd5694d0797e22f521faeb6026eddaa8
f8b318648494128da3b35f659526365b
eb8d418c036b00e4381671bf67c2e1b0
56f667c940811facae3ff7fd9ca8a3cdc4c6d1f5
8a3e9aa26eb981a21d6992ea4e5cb5aeac028b9b
d9b1cf6a1e0d8558af4e0a0de0ea7f510e68370e
3c6a65bade42081593d651abbda8c5f108be9adb
0b4e4bece54b2f1c5fe48d88e44310ffdf9a4185
47de2265afdf23794e81d8c5b26881377f83f653
461c041bfdec88d97d0e82277b4168d947daa9be
2902fb1142058e3b9a132fd27f69f082235a51b4
d409ed86161aeca0cf920f2ec014f19d5b22ab79
bb9b51f287b3efb9ced0230d95c835f07e03e7f6
b099aa5f46af0b54904e3b9d8be2d876c43c04a8
5e048aefb3527de836941fd78d6d919957a9108f
03933aa5b7421a06ccbe140f548f1aa8dad7589e
5a063409c69d909f031925ee066ac008088e3ef9
1dd5ebc671ec1c633c11188e17efb95e8db5ca6a
c93f2bb4b906eb4ec60cc472be8dc877e866c794
3f1e048a7feb76e209ac2a03106c45cdb6b67fef
2e068c72137073cb250bf021eb502516e5e7b86b
0259e9016461edd6bf1c8e99e9b4646df3b02c05
97f4a1d182b812f94b432ce4a22c6f8d12d8a823
3e79a2e6747adcd898f146b29dd5d30b6bb08222
22441cff10885cfb1a2b9eeeb0de088ec77f70d3
686c4c99d4766ae242b22d5275900750275d856d
0938360274a6511e2c92cdd96a5f065febb9af8e
91eddbe83c121b41ce2675fefb51d68afe202455
179a161d33a2b9d37a0cffe6d51c673c554a0f68
0fa6242395b7a80f5879b298b6d4937b54192fa0
547735c3febf46852b69b67bf653cf153c869cc4
de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4

KPMG

KPMG Cyber Threat Intelligence Platform

CoralRaider - Pilfering Financial Data Across Asia

Indicators of Compromise: Hashes
de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4
020d3d03ede3a80f1287ab58053f30ae7bfaf916ab0b1fc927f07b4b9d1f5c34
075091793768885977c29a41a0ac591340ebafab26d2a65ce1dccb53997485a1
0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a0
1db18d89a636f9d9307e51798c0545664fae38711a2a72139d62c7dbd6f17fe3
2c4ed97859060ea6ac5a8c2f605debf98257a96f0f3d2ddfaeb066f59a86d4af
4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643
77acb85a28e79dc6479798c024282ddd54977dbff6ce40eb439b2a06ce9cb542
93c747fff1ec919d981aa4ad2e42cda3d76c9d0634707a62066dbadda1653d1c
9bf684b010e4ec314d697acfac78c71ec24ba5f6e2c09b3be623ec62056aed02
b2fd046022231171941 81c97ca8692a09f6f5cfdbc07c87560aaab821cd29536
c29732d898dcf116f40eea3845d4e25a240e5840378985c7f192e0443a51a228
c84ff4fb6549c36ca0028e84ea8292ee3ae438254cddd63ef3d9ea769e0a1dfd
d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e
e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f
28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f
f71f7c68209ea8218463df397e5c39ef5f916f138dc001feb3a60ef585bd2ac2
c6419df4bbda5b75ea4a0b8e8acd2100b149443584390c91a218e7735561ef74
73c7459e0c3ba00c0566f7baa710dd8b88ef3cf75ee0e76d36c5d8cd73083095
29741f7987ab61b85adb310a7ab2f44405822f1719fa431c8f49007b64f6f5cd
7905bd9bb4d277a81935a22f975a0030faa9e5c9dbb9f6152c2f56ba1cd0cdea
a99a9f2853ff0ca5b91767096c7f7e977b43e62dd93bde6d79e3407bc01f661d
0058d495254bf3760b30b5950d646f9a38506cef8f297c49c3b73c208ab723bf
d267e2a6311fe4e2dfd0237652223add300b9a5233b555e131325a2612e1d7ef
3adcc81446f0e8ed1a2bc1e815613eb5622afba57941d651faa2b5bc4b2f13c1
5655a2981fa4821fe09c997c84839c16d582d65243c782f45e14c96a977c594e
7abf74260ae5b771182e95bc360fefa1b635b56b3aa05922506d55c5d15517c3
0a5aa03e35d6d9218342b2bec753a9800570c000964801cf6bfe45a9bb393c0d