CoralRaider Malware Campaign Exploits CDN Cache to Spread Info-Stealers

Date: 25th April 2024 | Severity: High

Summary

A new ongoing malware campaign has been observed distributing three different stealers, such as CryptBot, LummaC2, and Rhadamanthys hosted on Content Delivery Network (CDN) cache domains since at least February 2024.

Cisco Talos has attributed the activity with moderate confidence to a threat actor tracked as CoralRaider, a suspected Vietnamese-origin group that came to light earlier this month.

This assessment is based on "several overlaps in tactics, techniques, and procedures (TTPs) of CoralRaider's Rotbot campaign, including the initial attack vector of the Windows Shortcut file, intermediate PowerShell decryptor and payload download scripts, the FoDHelper technique used to bypass User Access Controls (UAC) of the victim machine," the company said.

Attack Vectors

- Attack chains involve users downloading files masquerading as movie files via a web browser, raising the possibility of a large-scale attack.
- "This threat actor is using a Content Delivery Network (CDN) cache to store the malicious files on their network edge host in this campaign, avoiding request delay," Talos researchers Joey Chen,Chetan Raghu prasad, and Alex Harkins said. "The actor is using the CDN cache as a download server to deceive network defenders."

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 3ae459746637e6f5536f3ba4158c822031578335505a512df3c31728cac8f627 • 7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8 • c84ff4fb6549c36ca0028e84ea8292ee3ae438254cddd63ef3d9ea769e0a1dfd • 42654394f29f2e8db878fc4fd1c59e41afcd0add3b93f7d2f47ea3295b2bc643 • a04c6804b63220a9cb1ea6c5f2990e6a810d7b4b7225e0fc5aa7ed7e2bac3c99 • a99a9f2853ff0ca5b91767096c7f7e977b43e62dd93bde6d79e3407bc01f661d

	• 2c4ed97859060ea6ac5a8c2f605debf98257a96f0f3d2ddfaeb066f59a86d4af • 0058d495254bf3760b30b5950d646f9a38506cef8f297c49c3b73c208ab723bf • 1db18d89a636f9d9307e51798c0545664fae38711a2a72139d62c7dbd6f17fe3 • 3c075a2bcd06e103e6ec3a1b74ceaaf600d3a9e179e2719795377f71c4f8f9c8 • 5655a2981fa4821fe09c997c84839c16d582d65243c782f45e14c96a977c594e • 88528be553f2a6f72e2ae0243ea907d5dcdcd7c8777831b4c3ab2a67128bc9b9 • 73c7459e0c3ba00c0566f7baa710dd8b88ef3cf75ee0e76d36c5d8cd73083095 • 075091793768885977c29a41a0ac591340ebafab26d2a65ce1dccb53997485a1 • 1942c417f2b71068fb4c1abb31bc77426bbe3513334cdaceaff3603955830e21 • 56f667c940811facae3ff7fd9ca8a3cdc4c6d1f5 • a28152ed5039484e858d3c7d4bac03c6ad66fbaff0e8ea3dfa8def95e115181 • e9e9d5ab6307a9ce98b1b3450def66df7a00d9dc5af613434af8d9b9cb3f2a0f • 958508a626b94d5e2e00ab0b94cb75dca58091cce708d312ee1a1c0688ef067c • a1f16ab97b9516e85c202ff00bd77b0b5e0e4ed29bfad28797fbbd0f25a8e0ae • d267e2a6311fe4e2dfd0237652223add300b9a5233b555e131325a2612e1d7ef • 934dc78ab89dd466b1a140954c6528b6a8591ca09a023616405cf71faf69f010 • b86ba0844db442df61a5889b004e615b • f71f7c68209ea8218463df397e5c39ef5f916f138dc001feb3a60ef585bd2ac2 • 5cb65b469023dcc77ede21c66a753fa9cbe67597aae142958fce4936ce3974aa • 28f827afd3bafa1e39526f84f8e1271c15d073c9d049a9bc8d03048c455dd33f • fd53383d85b39e68d817e39030aa2184764ab4de2d478b7e33afc39dd9661e96 • b3e694ce12e6f67db5db56177abfddebbc29f558618987e014f47a46996a8ced • 7db78346dde71258ae1307b542d162a030c71031eebd0ed80816112d82c008f0 • b6dbee1b6e444216668c44e41a84ca91cbd966e9035621423ecc12db52a36e01 • 3b54d05ec98321980c1d71b89c42ff77a42f121e37f6ea54a6368a58ce1b1ad3 • 2ad94e492bc18e11f513a29968054e1a37df504ac577fd645e781e654f2730c9 • 3c6a65bade42081593d651abbda8c5f108be9adb • 150dd450f343c7b1e3b2715eae3ed470c1c1fadf91f2048516315f1500a58ffa • 8d200892e4f1e68373e58e7cd7119fe26769fcf609636adc727df09f2377d1c2 • 19055fb87b9a98a75544a533ec4f14f36a09a130219b8a33a13cb6073751ff39 • 51c1eccc1b95ecbeaebc4853606c02808fce208ff1f76f0c7aa11ad7fbb4b763 • 6089c53ef2b0100fd91554c2a56aafaeea86b08c5ad0459fd66bd05a6602a3ee • 8c732ec41550851cc933e635708820ec9202fddc69232ca4ed625d420aec3d86 • b796cc4a54ee27601c1ed3a0016caa6f58206f4f280391f67820b8b019602add • e68c9aedfd080fe8e54b005482fcedb16f97caa6f7dcfb932c83b29597c6d957 • 74ea6e91c00baad0b77575740eb7f0fb5ad1d05ddea8227dc1aa477e179e62 df • de8a5d881cfc913a24c846bec8c13f3ad98e60fde881352845d928015bc6a5a4 • 93c747fff1ec919d981aa4ad2e42cda3d76c9d0634707a62066dbadda1653d1 c • 1dd5ebc671ec1c633c11188e17efb95e8db5ca6a • 1480b2038395f9edd2c21dff68eb29a4d6177708b70b687f758af60c8b02f071 • 963ffc17565079705c924b8ab86d1c7018f5edc50ce8e810df3eebead4e14e7f • 3adcc81446f0e8ed1a2bc1e815613eb5622afba57941d651faa2b5bc4b2f13c1 • 0790bb235f27fa3843f086dbdaac314c2c1b857e3b2b94c2777578765a7894a 0 • 7abf74260ae5b771182e95bc360fefa1b635b56b3aa05922506d55c5d15517c 3 • 31b4fd83c16bf7266c82a623998b0d7b54bb084b24a5cb71a2b5e9b17bb633 dc • d5d16d9bb75d461922eade2597c233255871dc74659f0169f3d3f40f5273ab71 • 5dc77655bddf8881b533e4db732dcf7ac5ebf3adad4be77ff226909a49bfc89b • d60bb69da27799d822608902c59373611c18920c77887de7489d289ebf2bd53e • 1aea1e7098221f2cc76ccd45078d9a216236b4e7e295dfa68e8a25aab3abe77 8 • c6419df4bbda5b75ea4a0b8e8acd2100b149443584390c91a218e7735561ef7 4 • 305bf697e89e6eef59b0beef2b273a1daad174ebec238a67a6e80c5df5fffaf8 • c93f2bb4b906eb4ec60cc472be8dc877e866c794 • 4b16ea1b1273f8746cf399c71bfc1f5bff7378b5414b4ea044c55e0ee08c89d3 • aea7c613ac659a083c35afd8e20f19a2c3583f81597dec48cbc886292cfcc975 • 02e03904d09ccece4f71e34a4a6d0f1181471c4d17208ee6cfe940e11e18501 8 • 1397268735c5c6e88d8bc717ac27f8810225b554ed2f0d76a3e0048b0933af1 8 • 020d3d03ede3a80f1287ab58053f30ae7bfaf916ab0b1fc927f07b4b9d1f5c34

	• eef156d681c4921cbed720e6de257a69ad6a187e814037257977958eb0c7604e • 5ad73cf7e08b8c7bab0d96ba92607b8c9b22b61354052cf59df93b782b6e039 b • 7f19557ee3024c59668e5bd1c96a8124b0a201a9fd656bd072332b400c41340 5 • 3ac52be2039a73df64e36672f3f0c748de10f6a8bed4b23642dd8da25613768 1 • 29741f7987ab61b85adb310a7ab2f44405822f1719fa431c8f49007b64f6f5cd • ec2f2944f29b19ffd7a1bb80ec3a98889ddf1c097130db6f30ad28c8bf9501b3 • f7d9c4c7da6082f1498d41958b54d7aeffd0c674aab26db93309e88ca17c826c • a3299ecee7b3f06ca106f4c5b62bf1e0f28f227df71488583d2077c7e3ee01c2 • 4dc9fe269cd668894c7ea4dd797cba1d2a8df565e9bdd814e969247c94b39643 • b2fd04602223117194181c97ca8692a09f6f5cfdbc07c87560aaab821cd29536 • 77acb85a28e79dc6479798c024282ddd54977dbff6ce40eb439b2a06ce9cb54 2 • 9bf684b010e4ec314d697acfac78c71ec24ba5f6e2c09b3be623ec62056aed02 • c29732d898dcf116f40eea3845d4e25a240e5840378985c7f192e0443a51a22 8 • 725888549d44eb5a3a676c018df55943 • 3a884d7285b2caa1cb2b60f887571d6c • f2a6c498fb90ee345d997f888fce3b18 • 0ba4439ee9a46d9d9f14c60f88f45f87 • 801ab24683a4a8c433c6eb40c48bcd9d • 3e679cff5b3a6f6f8f32aead541a0a12 • fb84708d32d00fca5d352e460776584c • e8606d021da140a92c7eba8d9b8af84f • 51bad062733f1babc99254ca06db0e46 • b5b3627606a5c5e720fa32fb9cb90aa813c630673d23c97a81012b832799a89 7 • 8bd7eece235cee14ab700f23b7ac29db • 120c6d7e78fb92b2feada47c9d8bbab0 • 0a5aa03e35d6d9218342b2bec753a9800570c000964801cf6bfe45a9bb393c0 d • d7dfa7009a9d808b744df8ed4f5852bd03ff82f7a07a258ea8b5e0290fb7d87 • 5226b67b5d49720981841fab64794533fe0530409ba2975e6125a4bc008f248 0 • 5eeab7b795a3303c368c72ef09a345f3a4f02301ec443e98319d600e8287e85 2 • 7905bd9bb4d277a81935a22f975a0030faa9e5c9dbb9f6152c2f56ba1cd0cdea
Domain/URL	• http://denv-2[.]b-cdn[.]net/FebL5 • http://gemcreedarticulateod[.]shop/api • http://metrodown-3.b-cdn.net/MebL1 • http://kbeight8pn.top/upload[.]php • http://triangleseasonbenchwj[.]shop/api • http://zexodown-2.b-cdn[.]net/Peta12 • http://culturesketchfinanciall[.]shop/api • http://metrodown-2.b-cdn[.]net/MebL1 • http://denv-2[.]b-cdn.net/FebL4 • http://secretionsuitcasenioise[.]shop/api • http://download-main5[.]b-cdn.net/BSR_v7IDcc • http://sofahuntingslidedine.shop/api • http://metrodown-2.b-cdn[.]net/SAq2 • http://peasanthovecapspll[.]shop/api • http://dashdisk-2.b-cdn[.]net/XFeb18 • http://modestessayevenmilwek[.]shop/api • http://claimconcessionrebe[.]shop/api • http://kveight8sb.top/zip[.]php • http://kzeight8ht.top/upload[.]php • http://kbeight8sb.top/upload[.]php • http://kbeight8ht.top/upload[.]php • http://dbeight8pt.top/zip[.]php • http://kbeight8vs.top/upload[.]php • http://techsheck.b-cdn[.]net/Zen90 • http://www.ondroid[.]store/ties5shizooQu1ei/ • http://www.ondroid[.]store/aL2mohh1

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Employ a Web Application Firewall (WAF) to help protect against common web exploits.
- Monitor traffic to identify and block suspicious activities.
- Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

Reference Links

- https://thehackernews.com/2024/04/coralraider-malware-campaign-exploits.html
- https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/66127d91c2c8d3ed181bd6b8