Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 26-JUN-2024, 21:30 IST

Title	**New Medusa malware variants target Android users in seven countries**
Summary	• The Medusa banking trojan for Android has re-emerged after almost a year of keeping a lower profile in campaigns targeting France, Italy, the United States, Canada, Spain, the United Kingdom, and Turkey. • Medusa is a sophisticated malware family with RAT capabilities discovered in 2020. • The new variant includes a lightweight permission set and new features like full-screen overlay and remote uninstallation of applications. • The TAs have started using “droppers” to distribute malware via fake update procedures. • Initial investigations connected the "4K Sports" app to the Medusa family, revealing significant changes in its command structure and overall capabilities. • Medusa's capabilities allow TAs to perform On-Device Fraud (ODF), making it a highly dangerous threat. • The malware’s infrastructure supports multiple botnets simultaneously, each differentiated by specific tags and operational goals.
Severity	Medium
Attack Vectors	• Threat Actors (TAs) use deceptive emails to trick recipients into clicking malicious links or downloading attachments that install the Medusa malware. These emails often appear to be from legitimate sources, making them effective in fooling users. • Malicious websites, TAs create or compromise websites to host and distribute Medusa malware. When users visit these sites, they may inadvertently download and install the malware onto their devices. • TAs exploit known vulnerabilities in software applications and operating systems to gain unauthorized access and install Medusa malware. This method targets unpatched systems, emphasizing the importance of regular software updates. • Fake update procedures, TAs use "droppers," which are malicious programs that mimic legitimate software updates. Users are tricked into believing they are installing an update, but instead, they are downloading and installing the Medusa malware. • Social engineering, TAs send text messages (SMS) that appear to be from legitimate sources, urging recipients to click on links or download attachments. This method exploits human psychology to bypass technical defenses and deliver the Medusa malware directly to users' devices. • TAs distribute malicious applications disguised as legitimate apps through unofficial app stores or compromised official stores. These dropper apps, once installed, download and install the Medusa malware onto the victim's device.

Indicators of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	• b9ee66c96b110622f4608581e77b0e4d • 7031c88ea3a306c4e4d786d3b0625a20 • 432cd820424c1a9ae0abac63a4f130c7 • ae53e2d732523c460d31e2805989e480 • c6153acefb8d3724f7defc177cff9ca9 • db097d837681d059a63725bc4ad93515 • 1db5ce9cbb3932ce2e11e5b3cd900ee2 • 811bcc33027f3784d800e75dea81f277 • 97abc0aa3819e161ca1f7f3e78025e15 • 8468c1cda925021ed911fd9c17915eec • fb3d3bdc13f445df3f4dd55f547aa92a • b6bbf8ed1cf8ec67b25bbcf26de483b4 • 1ed0d97491afd5c2d27f74f18e254cc3 • 469dfea6446a8bb5fada116bd28483d7 • 62faff68d6e3957973e91810a0abf166 • e501752247d32e908e4db70f457ced42 • bbecdd2513981eb9573b163151747e3b • 08344a2575efed552f2688b371ebac67 • 185f8c23fd680cae560aad220e137886 • 3b7df8e68eca9a4bcc559d79a2c5a4c7

		• 6b05a1e9faf5b77bad1826bacf322b24 • 4c12987ac5d56a35258b3b7cdc87f038 • 3fbe1323bdef176a6011a534e15a80f0 • 0e7c37e28871f439539b3d87242def55 • 646077aaf1ced1b32ae6519beced080f • 8d232fd0bfc9e1e4e77b8d719f24b48f • d98386401edf18ddbf45a40febf80c40 • 5a807cb36fdb3eaa50004351cb83a348 • 3ccb77a10497a32efcaa42ac646ca6cf • da92fc812b84137cef1571fb6c0285f0 • 2fb098a1868c7162aff9aa84fcc45071 • ac7741bca86793d28659b358f734a65e • e8ab402124e19af08d5ddc924d463991 • e65f01591ae40802748b09f9964bc61e • 8a4928ac9089adc4a153741d2f1c784a • cffad0170fc13756cab142d3989c26a9 • 29dd2f61f1d402ab46d963ed25c591d5 • a6157e3e5e1aef93ae71b3cff3ec9d80 • 2ecce74a26fe3f76252d0fc29cdc3ed3 • b9f3782c3d6034cdd12b6854e49b5fcf • 2a94a9157e7cb3259531cfb1bf9f1f83 • 25139a3dde2d6b9ded29de97452a8774 • 9437ea7aa931bfed9e6cdd76fe27d811 • b2ae7eb30163c8b004dc354ebb973e49 • df29a4a16af5da6e24aa3361b204a664 • 5d3958940abab05acee4b9dbab6bc4c3 • 0f83a144483ba17f4e3154d717361381 • 59735a4123c664f1795fb7154c95af67 • 920bdb47c0c060ecc5a06461c9715e26 • 3dac7bb95b01676d24cb194c3c47029f • d8e8eb2714c91b9968ffd409f771e7e1 • 53970ff7dd8edaec7fc0cdd030c0b038 • e69248a7308436d8c6dde803c22821cb • cb1280f6e63e4908d52b5bee6f65ec63 • a5aeb6ccc48fea88cf6c6bcc69940f8a • bd7b9dd5ca8c414ff2c4744df41e7031 • 9ceef4129ea27388018c0d1bb8554bcc • 3e0ee083fa9fce493383d75db1c69eee • 776b5b3c18a10b7e04f238478408f057 • 4bace6e0b61f5169bb0ca7f48c38aea2 • c9f30775469ef4ba09b1c09fdb13fd2d • 2580f696f903b11f4ca06754fa82b5a7 • dbf7b5f6faeacbed7adb0880d50380b4 • f7deb4066b016df32e8cd47b7ad44225 • 02c7e63ffa0c5488dd080b64bc297852
	Domains	• cincincintopcin[.]info • pemmbebebebebebe[.]info • tony1303sock[.]top • baahhhs21[.]info • unkunknunkkkkk[.]info • tonyyyyyyyyyy[.]info • a4a4a4a[.]life • pembe1303sock[.]top

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Never trust or open links and attachments received from unknown sources/senders. • Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**
References	• https://www.cleafy.com/cleafy-labs/medusa-reborn-a-new-compact-variant-discovered#5 • https://www.bleepingcomputer.com/news/security/new-medusa-malware-variants-target-android-users-in-seven-countries/