THREAT ADVISORY

April 1, 2024

Vultur Android Banking Malware

SUMMARY

The Android banking trojan Vultur has resurfaced with enhanced functionalities and advanced methods for evasion, including encrypting its communication channels, using dynamically decrypted payloads and masquerading as legitimate applications. The new version gives operators the ability to remotely manipulate mobile devices and collect user information. This infection still requires at least three (3) victim interactions, including the initial phone call to the threat actors from the initial SMS text, interaction with a subsequent SMS text that contains a link, and installation of the fake McAfee app that has the malware payload.

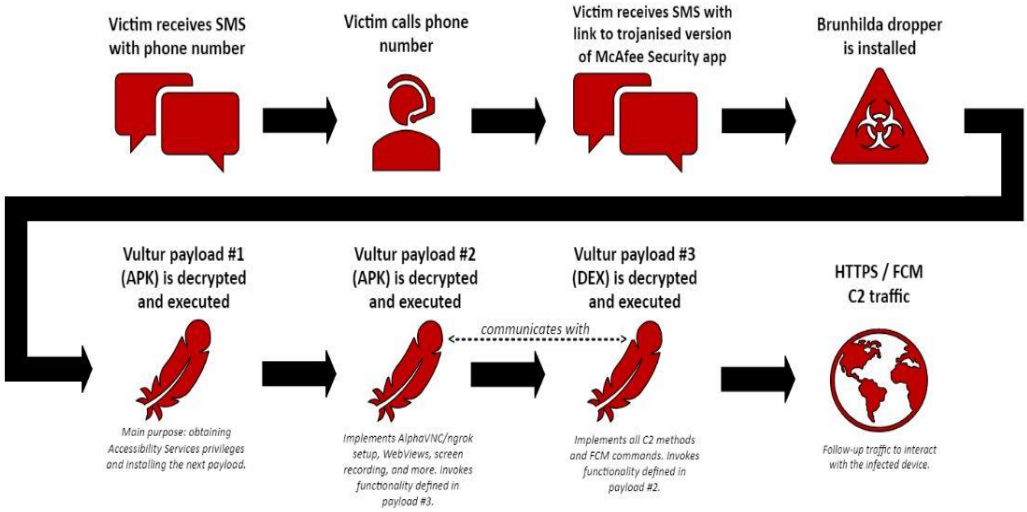
TECHNICAL DETAILS

Vultur's infection cycle begins with an SMS alert concerning an unauthorized financial transaction and urging the recipient to call a provided number for assistance. If the recipient calls the number, they are coerced into following a link provided in a subsequent SMS, leading to a webpage offering a malicious version of the McAfee Security app that contains the 'Brunhilda' malware dropper. Once installed, the app decrypts and executes three Vultur-associated payloads (two APKs and one DEX file), which then exploit Accessibility Services, trigger remote control systems, and establish contact with the command and control (C2) server.

The new Vultur malware retains several capabilities from previous versions, including screen recording, keylogging, and remote access via AlphaVNC and ngrok, enabling real-time surveillance and control for malevolent actors. New functionality adds expanded file management capabilities, including download, upload, deletion, installation, and file reconnaissance on the targeted device; and Accessibility Services to execute various user interactions like clicks, scrolling, and swiping gestures.

Evasion capabilities include stratagems, including blocking specific apps and displaying customized notifications to mislead users; overrides Keyguard to circumvent lock screen security, granting unrestricted access to the device; and encrypted C2 communications (AES + Base64 encryption) and dynamically decrypted payloads;

INFECTION CHAIN (NCCGROUP)



IOCs

File Hash (SHA-256):

- edef007f1ca60fdf75a7d5c5ffe09f1fc3fb560153633ec18c5ddb46cc75ea21
- 89625cf2caed9028b41121c4589d9e35fa7981a2381aa293d4979b36cf5c8ff2
- 1fc81b03703d64339d1417a079720bf0480fece3d017c303d88d18c70c7aabc3
- 4fed4a42aadea8b3e937856318f9fbd056e2f46c19a6316df0660921dd5ba6c5
- 001fd4af41df8883957c515703e9b6b08e36fde3fd1d127b283ee75a32d575fc
- fc8c69bddd40a24d6d28fbf0c0d43a1a57067b19e6c3cc07e2664ef4879c221b
- 7337a79d832a57531b20b09c2fc17b4257a6d4e93fcaeb961eb7c6a95b071a06
- 7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c
- 26f9e19c2a82d2ed4d940c2ec535ff2aba8583ae3867502899a7790fe3628400
- 2a97ed20f1ae2ea5ef2b162d61279b2f9b68eba7cf27920e2a82a115fd68e31f
- c0f3cb3d837d39aa3abccada0b4ecdb840621a8539519c104b27e2a646d7d50d
- 92af567452ecd02e48a2ebc762a318ce526ab28e192e89407cac9df3c317e78d
- fa6111216966a98561a2af9e4ac97db036bcd551635be5b230995faad40b7607
- dc4f24f07d99e4e34d1f50de0535f88ea52cc62bfb520452bdd730b94d6d8c0e
- 627529bb010b98511cfa1ad1aaa08760b158f4733e2bbccfd54050838c7b7fa3
- f5ce27a49eaf59292f11af07851383e7d721a4d60019f3aceb8ca914259056af
- 5d86c9afd1d33e4affa9ba61225aded26ecaeb01755eeb861bb4db9bbb39191c
- 5724589c46f3e469dc9f048e1e2601b8d7d1bafcc54e3d9460bc0adeeada022d

- 7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c
- fd3b36455e58ba3531e8cce0326cce782723cc5d1cc0998b775e07e6c2622160
- 819044d01e8726a47fc5970efc80ceddea0ac9bf7c1c5d08b293f0ae571369a9
- 0f2f8adce0f1e1971cba5851e383846b68e5504679d916d7dad10133cc965851
- fb1e68ee3509993d0fe767b0372752d2fec8f5b0bf03d5c10a30b042a830ae1a
- d3dc4e22611ed20d700b6dd292ffddbc595c42453f18879f2ae4693a4d4d925a
- f4d7e9ec4eda034c29b8d73d479084658858f56e67909c2ffedf9223d7ca9bd2
- 7ca6989ccfb0ad0571aef7b263125410a5037976f41e17ee7c022097f827bd74
- c646c8e6a632e23a9c2e60590f012c7b5cb40340194cb0a597161676961b4de0

C2 Servers:

- safetyfactor[.]online
- cloudmiracle[.]store
- flandria171[.]appspot[.]com
- newyan-1e09d[.]appspot[.]com

Dropper Distribution URLs:

- mcafee[.]960232[.]com
- mcafee[.]353934[.]com
- mcafee[.]908713[.]com
- mcafee[.]784503[.]com
- mcafee[.]053105[.]com
- mcafee[.]092877[.]com
- mcafee[.]582630[.]com
- mcafee[.]581574[.]com
- mcafee[.]582342[.]com
- mcafee[.]593942[.]com
- mcafee[.]930204[.]com

RECOMMENDATIONS

- Limit mobile application downloads to trusted sources such as the official Google Play Store to minimize the risk of encountering malicious applications.

• Educate users regarding unsolicited SMS alerts or messages, especially those of a financial nature and those containing links.

• Verify the legitimacy of callers and requests for contact, especially in response to alarming or urgent messages.

• Review the permissions requested by applications before and during installation; grant access based on intended purpose.

• Install reputable mobile security software to provide an additional layer of protection against malware and other cyber threats.

REFERENCES

• https://research.nccgroup.com/2024/03/28/android-malware-vultur-expands-its-wingspan/

• https://thehackernews.com/2024/04/vultur-android-banking-trojan-returns.html

• https://www.bleepingcomputer.com/news/security/vultur-banking-malware-for-android-poses-as-mcafee[1]security-app