# Vultur banking malware for Android poses as McAfee Security app

Date: 09th May 2024 | Severity: High

## Summary

The Vultur Android banking Trojan, first reported by cybersecurity researchers in July 2021, has been active since at least March 2021. The malware primarily targets cryptocurrency, banking and social media applications in Europe and Oceania.

## Attack Vectors

Vultur deceives users into installing it by masquerading as legitimate applications, such as a counterfeit version of the McAfee Security app. Once installed, Vultur exploits Android's Accessibility Services to execute its attacks covertly, enabling actions such as screen recording and keystroke logging without the user's consent.

Vultur is likely associated with the Brunhilda malware as they use the same command and control, and both communicate using JSON-RPC.

In the beginning, Vultur was limited to screen recording and keylogging, but in 2024 researchers reported on a newly released version that includes more robust capabilities. The new malware version, delivered through smishing campaigns, is capable of blocking applications from executing, using accessibility features (swiping gestures, clicking, and scrolling), managing files, generating misleading notifications, and disabling keyguards.

Among the companies whose applications were targeted by Vultur: WhatsApp, Facebook, TikTok, HSBC Australia, BBVA, Bankia, Coinbase, and Bitfinex.

- File management actions including download, upload, deletion, installation, and finding files on the device.
- Use of Accessibility Services to perform clicks, scrolling, and swiping gestures.
- Blocking specific apps from executing on the device, displaying custom HTML or a "Temporarily Unavailable" message to the user.
- Displaying custom notifications in the status bar to mislead the victim.
- Disable Keyguard to bypass lock screen security and gain unrestricted access to the device.

# Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| Domains | • mcafee.930204[.]com<br>• mcafee.582342[.]com<br>• mcafee.092877[.]com<br>• mcafee.581574[.]com<br>• mcafee.053105[.]com<br>• mcafee.593942[.]com<br>• mcafee.908713[.]com<br>• mcafee.582630[.]com<br>• mcafee.784503[.]com<br>• mcafee.960232[.]com<br>• mcafee.353934[.]com<br>• cloudmiracle[.]store<br>• resources.prodaft[.]com<br>• safetyfactor[.]online |
| URL | https[:]//resources.prodaft.com/brunhilda-daas-malware-report |
| File Hashes | • dafa2f40b09ebb8ba0695001a29546a4<br>• 5724589c46f3e469dc9f048e1e2601b8d7d1bafcc54e3d9460bc0adeeada022d<br>• 52abc7f45a449ffd2760ef58672d2b71<br>• 4fed4a42aadea8b3e937856318f9fbd056e2f46c19a6316df0660921dd5ba6c5<br>• 5d86c9afd1d33e4affa9ba61225aded26ecaeb01755eeb861bb4db9bbb39191c<br>• 92af567452ecd02e48a2ebc762a318ce526ab28e192e89407cac9df3c317e78d<br>• 2a97ed20f1ae2ea5ef2b162d61279b2f9b68eba7cf27920e2a82a115fd68e31f<br>• 8e83d178c1a3b9da0c71c613e2c77647<br>• 764af13e353f09617c33ec8a100acad5b2240505<br>• d9cb590817405738cf57f8545ff583848b1c3b19<br>• fa6111216966a98561a2af9e4ac97db036bcd551635be5b230995faad40b7607<br>• fd3b36455e58ba3531e8cce0326cce782723cc5d1cc0998b775e07e6c2622160<br>• e907e2a4dc7455d068b1f5a28fbda8ea8abdb30e0c19a6200083ad2fb607961d<br>• 819044d01e8726a47fc5970efc80ceddea0ac9bf7c1c5d08b293f0ae571369a9<br>• aeaf26e5d5e130382719f879fc987cd7ded76465<br>• f5ce27a49eaf59292f11af07851383e7d721a4d60019f3aceb8ca914259056af<br>• 436736451c497872d3ca1007b0d4950692d1baab<br>• b58a7cc0c8cf529ae05589f8b76cd8a7<br>• 1fc81b03703d64339d1417a079720bf0480fece3d017c303d88d18c70c7aabc3<br>• 6bb99bd81bc27916f14883541b41ad6a<br>• 0f2f8adce0f1e1971cba5851e383846b68e5504679d916d7dad10133cc965851<br>• 627529bb010b98511cfa1ad1aaa08760b158f4733e2bbccfd54050838c7b7fa3<br>• 4c950bb7556d287bb740e7dcadabbb46d467df25a3309e664a8255c18b1715b0<br>• b1b5eacc4d1cd7500e930286833f1626<br>• dc4f24f07d99e4e34d1f50de0535f88ea52cc62bfb520452bdd730b94d6d8c0e<br>• fb1e68ee3509993d0fe767b0372752d2fec8f5b0bf03d5c10a30b042a830ae1a<br>• c0f3cb3d837d39aa3abccada0b4ecdb840621a8539519c104b27e2a646d7d50d<br>• fc8c69bddd40a24d6d28fbf0c0d43a1a57067b19e6c3cc07e2664ef4879c221b<br>• 001fd4af41df8883957c515703e9b6b08e36fde3fd1d127b283ee75a32d575fc<br>• 2da004a28be64e61f21a5b562795b2b9<br>• f4d7e9ec4eda034c29b8d73d479084658858f56e67909c2ffedf9223d7ca9bd2<br>• 26f9e19c2a82d2ed4d940c2ec535ff2aba8583ae3867502899a7790fe3628400<br>• f9e2f2933310a34d1b756482e0847d31bd2f50aa<br>• 7337a79d832a57531b20b09c2fc17b4257a6d4e93fcaeb961eb7c6a95b071a06<br>• c646c8e6a632e23a9c2e60590f012c7b5cb40340194cb0a597161676961b4de0<br>• 5daddee01e70eae61842eae36b8d69ca1f980601<br>• bca6f9f22b2045e8218f07dd76ce2759fa21e542c2e76e3733fed99153207d39 |

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hashes | • cbcc6d7e10f9138a896e0cf77ed4727e11d272ac<br>• bfae871e0c89814e133a6810276ff324d0bd376e<br>• 7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c<br>• 89625cf2caed9028b41121c4589d9e35fa7981a2381aa293d4979b36cf5c8ff2<br>• f931794df50c0876bab25b112d85d702<br>• 7ca6989ccfb0ad0571aef7b263125410a5037976f41e17ee7c022097f827bd74<br>• edef007f1ca60fdf75a7d5c5ffe09f1fc3fb560153633ec18c5ddb46cc75ea21<br>• d3dc4e22611ed20d700b6dd292ffddbc595c42453f18879f2ae4693a4d4d925a |

# Recommendation

- Employees should be educated on the risks of ransomware, and on how to identify and avoid phishing emails, malicious attachments, and other threats.
- They should be encouraged to report suspicious emails or attachments, and to avoid opening them, or clicking on links or buttons in them.
- Avoid sideloading apps and shortened URLs
- Exercise caution when granting app permissions.
- Keep your Android device updated.
- Have good antivirus software on all your devices

# Reference Links

- https://cyberguy.com/security/protect-your-android-from-the-vultur-banking-trojans-remote-attacks/
- https://www.bleepingcomputer.com/news/security/vultur-banking-malware-for-android-poses-as-mcafee-security-app/
- https://thehackernews.com/2024/04/vultur-android-banking-trojan-returns.html