



# KPMG Cyber Threat Intelligence Platform

## GodFather – Massacring the Android Defenses



Imitating the standard android security tool Google Protect, GodFather trojan was first observed in March 2021. Sharing code with the old Anubis credential stealer, GodFather is tricking users into entering their credentials on legitimate looking HTML phishing login pages over apps. Specifically targeting financial sector, GodFather has compromised almost 400 online banking sites, multiple cryptocurrency exchange platforms and wallet apps in regions including United States, Turkey, Spain, Canada, France, Germany and UK.

Distributed via trojanized apps on Google Play Store, GodFather checks system language to inhibit execution if it matches RU, AZ, KZ, UZ, TJ and other languages part of the CIS region. It then checks if it is launched in an emulator before requesting almost 23 permissions which would then be abused. Masquerading as legitimate apps, it doesn't launch unless 'AccessibilityService' permission is granted & hides icon post execution. Post admin level permissions, GodFather performs keylogging, screen-recording, reading SMS & notifications, exfiltrating OTPs/pins/passwords of targeted apps and overlays fake HTML login pages of known apps to steal credentials. As for C2 comms, the address is updated from a telegram channel's description via HTTP request. C2 features include ability to transfer money bypassing the dialer UI & to generate fake notifications from apps installed on the device to redirect the victim to phishing page. Stolen credentials & sensitive data are then exfiltrated in encrypted form. GodFather also comes with the ability to set-up reverse VNC via native libraries along with a persistent WebSocket for remote access.

While GodFather doesn't directly impact corporate organizations, it demonstrates how threat actors are catching up to mobile defences & bypassing android security checks.

### 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: raghavendrabbv@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2023 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjoshi

home.kpmg/in

Follow us on home.kpmg/in/socialmedia





# KPMG Cyber Threat Intelligence Platform

## GodFather – Massacring the Android Defenses



### Indicators of Compromise: IP Addresses

45.61.138[.]60

168.100.9[.]86

### Indicators of Compromise: Domains

henkormerise[.]com

heikenmorgan[.]com

banerrokutepera[.]com

pluscurrencyconverter[.]com

### Indicators of Compromise: Hashes

d7118d3d6bf476d046305be1e1f9b388

7e061e87f9a4c27bfb69980980270720

735ede5f45394a36d3a44c9eba738925

0ece45f5deb77db816d8950fce07cabb

ec9f857999b4fc3dd007fdb786b7a8d1

47a58afb9341909de2627d2d82799172

f6bd2e43ba89e65094019a671526258b

ab3e2c175c4b19d189f380ecfd011c6a

8039d9e03537db55f030dc79f636b531

766b19f10bf89c054fb2338bf6db3604

fb63a65e673bc63c9f8a610f533d4257

f9d0ff38d885f01d650eb73b171ab6e3

f5c7bf733d8693379f59c3e393d3398c

da7687c35ec3a70a792d8691e68965f3

d9bfb3d68e989828d2766dc872e83414

d81e079a031c21e1a651cd727875c84f

ce8c34181d0aae0d5f86dee43d10c8ab

c685ca051d3ca0cdee08f5a33a548031

c5d12034694e80115e8e0fb599ae4718

a109b8411df59b0597f2941f97d0a269

92ec81034584caac63fdb1e2899fb3bf

8ee3a7a5655c069f5d444444887f230e

8c3f5de84c7c233f7acdcc1985013fb9



# KPMG Cyber Threat Intelligence Platform

GodFather – Massacring the Android Defenses



## Indicators of Compromise: Hashes

8430f01843a529514343e233816f4110

1e431e07d9c115038165e288a422c7da

00dc2e7722a366c0a29ecfa09c34530a

e3abf2f1e5cf5de264b7a9488edf9187fab30695

3d74ce909e34f4e995363e0f079666de17f51d30

34d37927b35f422e7c28055ea989ef6524a668ef

2b3b78d3a62952dd88fc4da4688928ec6013af71

3fa48a36d22d848ad111b246ca94fa58088dbb7a

157e40bd93941a6169a60dca1a1f25f3d8c6a69c

5e54a91b01d2e780e6370215eb98e2a2d510f7e9

2ad5efe4eea66ebfc0866171984328907507520f

53d17f182c81178efa1206a4506ccc8d10abbf91

e9557410246dde67da90fb877f932a207fcc6ee5

e8cd8f685c0f9b4a186ac7feb81b3663ceae0c9e

e2757e1edd96238202862ba5e7f926f5a3911e17

e170f445625088eb270ea8e8ef89f1ddd55266c4

d3da40f12cd8bd1228a3ee8cf60f09933b3d6ffc

c76ed19b319c692e8d06b72879b33d20cb9b5f22

ac75884b3a8bd38bd3ffd759fa18a2583e7fe9d2

70f69b9abcd17238479eb39f47fbca664568b787

7040031c1a3a9c77065de758ee5bf14111038f36

5f8e6d21efee05a901db605163a5ece1cd00d8d6

5c6a5ab83f0252faafb4f204e543e2eae24d68a3

52f9c74e27e9a01803a6096e2f85cc3147f855f1

4f8780db90c0a32bd300f096cbc1444875067867

38c63ff6d425e499b13969a013502c59d756ba42

37b006b2a2f2a9cdfde4639dbe7372d25d0db9e3

1e49f4034eb0604c38f32097bb3ed32efe4e0426

193cdb9eb0dc885a5bb7c211c13f1a1bc18c56

142d3e6fdef8a776ba4b2c386ff45bd750d5cc68

e6fb245a7dd02af549e2d62f42413dcacda0fb847ee84d52b0f69c8219f3e81d

e67b8b78550396f542ded77d2118487ac1afb0d4ac6b70774889bbb4e6d88265

da021a501372f8de9a1d2c11802ec452f218a1c3fd39356151acae076c3304ff

d981bccfde804bb662e4acb1e7a97298b4a081c02b498a01abfeec74a60b8fdc



# KPMG Cyber Threat Intelligence Platform

GodFather – Massacring the Android Defenses



## Indicators of Compromise: Hashes

b58b9a2ba58813ad4fbf2f6349a522f9a49bf8b3190237eb9c43c1d085f4497e
93a8d9d57a816b1c0401660256db8e37d29a92a43cd7d9668f9d05db820aa572
8d07967b9253951b52c631383a3dde8513572b3c996c338819f4e12a7a60bf23
896301f184ff67a0fa9570e4275eafe66ab907636e381b86b87d28532aea0c82
7d9d89371f0409660136ad7a238e345b140b9359fae186814ec9572996f373a6
76cd894001f01f56299079b7eace162947b51b8b3a587c26709613e42279b850
61e67d1ce1577d5a08d0ae970ac20fa5f0b8db3660b6c6c83189130be3039675
55183db5a190f08ce9e1589b2b7186ce64523c85c2c8b2ea03c52315b529b451
536e9a5b341eb6e0708e58f65679232513b2896674b8b2615ff93c58fe1dbc9
50df8248535002052622f00b691bd60ad735e16e685a9d7b95a0850dc4229ad3
40a099d574cd588903d9cf8701da8d006e58be406049d26a61cc291720270b60
3f7eae6cc61fdc2553a2acdede69be84945a7a724b632dea3ff8466f74b56249
363eb5d89b43946a4af03e2399e47125bec822729d764b08004eb492212d51db
32c7ef93f3329709bf38b7d6ea5f076fb8bd86d36785ed811d99efcb98f8ae58
138551cd967622832f8a816ea1697a5d08ee66c379d32d8a6bd7fca9fdeaecc4
0932a99030a80786f8215e5cb5c879708848bd62141ff4672e23823ddc562ac7
06b0bebc1422a969ef10a0f13fb253b0697d079d7126551370b9757da6564c9d
f8d2382f72890b1975e1f149d07fdd3c36fff1d523e4ea83b2b1f593f956e7a0
d652ac528102de3ebb42a973db639ae27f13738e005172e5ff8aac6e91f3f760
c79857015dbf220111e7c5f47cf20a656741a9380cc0faecd486b517648eb199
c4bace10849f23e9972e555ac2e30ac128b7a90017a0f76c197685a0c60def6d
c3dad9a593523d1bf3fe76dabf375578119aff3110d92a1a4ee6db06742263a
b6249fa996cb4046bdab37bab5e3b4d43c79ea537f119040c3b3e138149897fd
a14aad1265eb307f7be71a3a5f6e688408ce153ff19838b3c5229f26ee3ece5dd
9dfb5b4ad9aac36c2d7fbb93f8668faa819cb0df16f4a55d00f1cdda89c9a6d2
9815ba07d0a2528c11d377b583243df24218a48c6a4f839f40769ea290555070
7664293fc1dde797940d857d1f16eb1e12a15b9126d704854f97df1bedc18758
38386f4fabd0bc7f7065eae818717e89772fb3b1a3744df754c45778e353f70
0b72c22517fdefd4cf0466d8d4c634ca73b7667d378be688efe131af4ac3aed8