The Godfather Android Malware: Threat under the lens

Archived: 2026-04-06 00:36:12 UTC

Earlier this year, The Federal Financial Supervisory Authority of Germany (BaFin) sounded the alarm bells about a dangerous threat lurking in the crypto sphere. The Godfather malware, discovered in 2020, has been wreaking havoc across multiple financial sectors, making it one of the biggest threats to the industry in recent years.

Shockingly, the malware has already infected over 400 international targets, including banking applications, cryptocurrency wallets, and crypto exchanges worldwide. The Godfather malware has emerged as a significant threat to the crypto industry, putting the security of crypto wallets and exchanges at risk.

Godfather's modus operandi is particularly insidious - it displays or redirects users to fake websites that look identical to legitimate crypto exchange portals. The malware's deception is so convincing that users may unwittingly give away their login credentials, not realizing that they are being targeted by cybercriminals. It's a classic case of bait-and-switch, with the Godfather malware luring in unsuspecting victims and stealing their sensitive data.

Once users enter their login credentials, the malware steals their sensitive data, leaving them vulnerable to cyber-attacks. The stakes are high, and the Godfather malware is a force to be reckoned with. With this information in their possession, cybercriminals can swiftly and efficiently drain user accounts, wreaking financial havoc in the process.

Given the rise of crypto-related cyber attacks in recent years, the Godfather malware underscores the need for enhanced cybersecurity measures, such as two-factor authentication and stronger password policies, to protect users' sensitive data and prevent attacks like these from succeeding.

What is malware and how does a malware attack take place?

To truly understand the godfather of malware and its impact on the crypto sphere, we must first understand the broader landscape of malicious software. Malware is an ever-evolving threat, constantly adapting

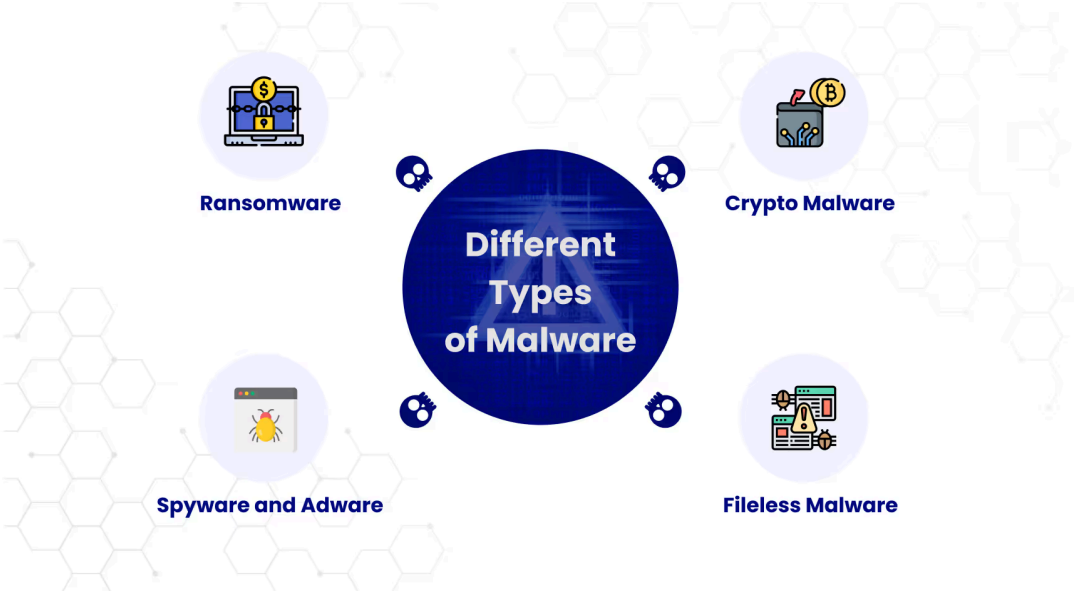
Malware is a portmanteau of two words: ‘malicious’ and ‘software. Designed to obstruct the normal functioning of a software interface, it is a catch-all term for various types of viruses, and trojans that are used by malicious actors to infect victim devices. In simple terms, malware is a software program built with the intent of making a profit by causing harm.

In the world of crypto, malware is a growing threat that can steal sensitive data, drain users’ accounts and lead to significant financial losses. As programmable devices become more prevalent and connected to the internet, malware is rapidly growing to become an integral part of the cybercrime industry. Cybercriminals incorporate several ways to distribute malware, some of which are:

1. Via emails and phishing attacks
2. By inserting malicious code into legitimate websites that redirect users to untrusted sites.

3. By infecting the victim’s device through malicious clickbait and malvertisements.

Different types of malware



To identify which category of malware Godfather belongs to, it’s important to familiarize ourselves with different types of malware :

Ransomware - Ransomware is one of the most notorious and lucrative type of malware that encrypts a victim’s data and demands a ransom in exchange for decryption key, often spreading through downloading or installing malicious files that give attackers unrestricted access to the system,

Spyware and adware - Spyware is a malicious program installed usually without the victim’s knowledge. It infiltrates devices to spy and collect data that can further be used for malicious and fraudulent purposes.

Spyware attacks are usually followed by adware, a malware involving fraudulent advertising. In this, attackers use the data collected through spyware and display fraudulent advertisements relevant to the victim's interests to attract them and eventually infect their devices through clickbait or redirect them to malicious sites.

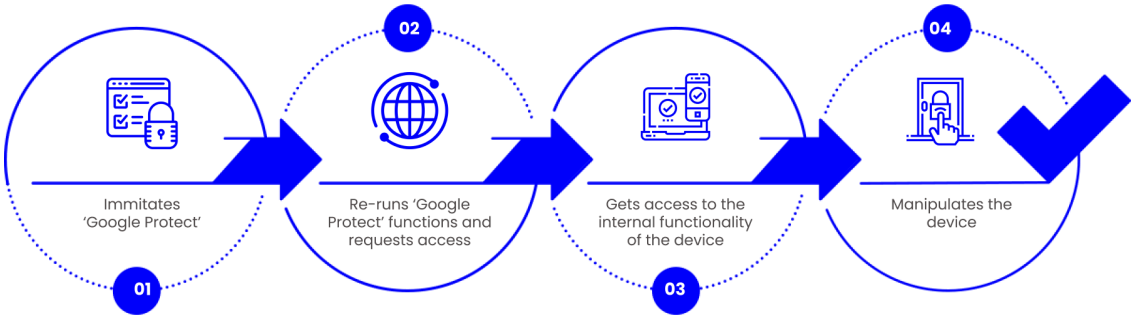
Crypto malware - Crypto malware or crypto mining malware leverages the computing power of a victim’s system to mine cryptocurrencies. Mining programs use large amounts of processing power and energy that are usually too high for a miner to afford.

Fileless malware - Fileless malware is a type of malware that uses built-in software or applications that are native to a device’s operating system to install and execute malicious activities. These attacks leave no traces like malware files to scan or trails of malicious processes behind that help them evade detection through antivirus software or other security scans.

Understanding the "Godfather" Malware: An Overview

Threat Analysis	
Name	GodFather trojan
Threat type	Android malware, malicious applications, unwanted application.
Symptoms	• The device is running slow • System settings are modified without the user's permission • Data and battery usage is increased significantly • Browsers redirect to illegitimate websites • Intrusive advertisements are delivered
Distribution Methods	Deceptive (trojanized) applications on Google Play Store mimic legitimate applications.
Damage	Stolen personal information (private messages, logins/passwords, etc.), decreased device performance, battery is drained quickly, decreased Internet speed, huge data losses, monetary losses, stolen identity.
Malware Removal (Android)	To eliminate malware infections security researchers recommend scanning your Android device with legitimate anti-malware software. Recommended anti-virus software - Avast, Bitdefender, ESET or Malwarebytes.

How Godfather exploits vulnerable devices?



1. Once installed, Godfather imitates 'Google Protect,' a security tool pre-installed on all Android devices.
2. The malware then re-runs ‘Google Protect’ functions including running a scan action that requests access to the device's internal functionality and accessibility.
3. Once the victim approves the request, the attackers get access to the device’s storage, SMS texts, and contacts, and also get access to send push notifications to steal the codes for two-factor authentication.
4. Moreover, the device’s accessibility service is abused to prevent the user from removing the trojan, exfiltrating Google Authenticator OTPs (one-time passwords), and stealing the contents of PIN and password fields.
5. Godfather exfiltrates a list of installed apps to receive matching injections (fake HTML login forms to steal credentials).
6. The malware can also generate fake notifications from apps installed on the victim's device to take the victim to a phishing page.

The malware requests users a number of permissions like:

Read_SMS	Access SMSs from the victim's device
RECEIVE_SMS	Intercept SMS received on the victim's device
READ_CONTACTS	Access contacts saved on a device
READ_PHONE_STATE	Allow access to phone state, including current cellular network information, the phone number and the serial number of the phone, the status of any ongoing call, and get a list of any Phone Account registered on the device.
RECORD_AUDIO	Allows apps to record audio with the microphone, that attackers can potentially misuse.
SEND_SMS	Allows an application to send messages
CALL_PHONE	Allows an application to initiate a phone call
WRITE_EXTERNAL_STORAGE	Allows applications to write or delete files in the device's external storage
WRITE_SMS	Allows applications to modify or delete messages
DISABLE_KEYGUARD	Allows applications to disable keylocks and associated password security
BIND_ACCESSIBILTY_SERVICE	Used for taking over accessibility services

Cybercriminals are constantly advancing their techniques and becoming increasingly sophisticated, making it imperative for organizations to take proactive steps to protect themselves from these threats. As the use of such illicit activities continues to grow, it seriously threatens user safety and the delivery of essential services. Such incidents indicate a dire need for improved security measures to safeguard critical infrastructures.

Warning signs of a malware attack

When a system is infected by malware, it can lead to a significant decline in its overall performance. The malware can consume system resources, such as CPU and memory, causing the system to slow down or even crash. Additionally, malware may create backdoors that can allow unauthorized access to the system, further compromising its security. These negative effects on system performance can have serious consequences, ranging from reduced productivity to complete system failure.

A common symptom of a malware attack is the abrupt redirection of web browsers to illegitimate sites that the user does not intend to visit. This happens when the attacker modifies the browser settings and injects additional plugins or extensions. Once redirected, these illegitimate websites begin to steal sensitive user data and spread the malware further to other vulnerable devices.

During a malware attack, users may receive various pop-up notifications warning that the device has been infected. These warnings are often accompanied by messages encouraging users to purchase or download a specific solution or product to solve this issue. This is nothing but a common tactic used by cybercriminals to trick users into paying for useless and fake products that do not actually fix any problem.

Some types of malware are designed to prevent users from shutting down or restarting their systems. This is often done as a way to maintain control of the infected device or to prevent the user from removing the malware. The malware may have damaged or altered critical system files or settings, which can cause the operating system to malfunction or become unstable. This can make it difficult or impossible to shut down the system in a normal way.

A malware attack can often result in little to no available storage space on your device. The malware may have installed additional files or programs onto your device without your knowledge. These files can take up significant amounts of storage space, especially if they are large or numerous. Some types of malware are designed to create duplicates of files or data on your device. This can result in multiple copies of the same files taking up valuable storage space.

How to prevent malware attacks?

1. Download and install software only from official app stores like Google Play Store or the iOS App Store.
2. Use a reputed anti-virus and internet security software package for your devices.
3. Use strong passwords and enforce multi-factor authentication wherever possible.
4. Be careful while opening any links received via SMS or emails.
5. Ensure that Google Play Protect is enabled on all Android devices.
6. Be careful while enabling any permission.
7. Keep your devices, operating systems, and applications updated.
8. Be careful on the internet. Avoid clicking on unknown links.

How can we help?

Merkle Science provides predictive blockchain risk intelligence and monitoring services that empower compliance teams to detect illicit cryptocurrency activities. We are at the forefront of the fight against Godfather malware, by leveraging our behavior-based transaction monitoring tool, Compass, using which cryptocurrency businesses can identify and block illicit transactions associated with Godfather malware.

Compass provides real-time alerts and actionable insights, enabling compliance teams to investigate suspicious transactions and potentially recover losses. We conduct post-mortem analyses, which involve monitoring and tracking of funds. This allows us to identify funds that are transferred to Virtual Asset Service Providers (VASPs). We promptly notify appropriate law enforcement authorities to aid in the apprehension of perpetrators upon detection of any suspicious activity and, if possible, the recovery of lost funds. To find out more, contact us

---