---

layout: page

title: "எனது சாதனம் சந்தேகத்திற்குரிய வகையில் செயல்படுகிறது"

author: Donncha Ó Cearbhaill, Claudio Guarnieri, RaReNet

language: en

summary: " உங்கள் கணினி அல்லது கையடக்கத் தொலைபேசியானது சந்தேகத்திற்குரிய வகையில் செயல்பட்டால், உங்கள் சாதனத்தில் தேவையற்ற அல்லது தீங்கிழைக்கும் மென்பொருள் காணப்படலாம்."

date: 2023-04

permalink: /en/topics/device-acting-suspiciously

parent: Home

---

# எனது சாதனம் சந்தேகத்திற்குரிய வகையில் செயல்படுகிறது

தீம்பொருள் தாக்குதல்கள் பல ஆண்டுகளாக உருவாகி மிகவும் அதிநவீனமாகிவிட்டன. இவை பல்வேறுபட்ட அச்சுறுத்தல்களை ஏற்படுத்திடுவதுடன் உங்களது சுய மற்றும் நிறுவன உட்கட்டமைப்பு வசதிகளில் தாக்கங்களை ஏற்படுத்தலாம்.

தீம்பொருள் தாக்குதல்களானவை வைரஸ்கள், தகவல் திருட்டு , ransomware, trojans மற்றும் ரூட்கிட்கள் போன்ற வெவ்வேறுபட்ட வடிவங்களில் வருகின்றன. சில அச்சுறுத்தல்களாக : கணினிகள் செயலிழக்கச் செய்தல், தரவுத் திருட்டு (அதாவது: முக்கியமான கணக்குச் கடவுச் சொல் குறியீடுகள், நிதித் தகவல், வங்கிக் கணக்கு உள்நுழைவுகள்) காணப்படுகின்றன, இத் தாக்குதல்காரர்கள் உங்கள் சாதனத்தின் கட்டுப்பாட்டை எடுத்துக்கொள்வதன் மூலம் அல்லது உங்கள் சாதனத்தின் கட்டுப்பாட்டை எடுத்துக்கொண்டு அதைப் பயன்படுத்துவதன் மூலம், நீங்கள் ஆன்லைனில் செய்யும் அனைத்தையும் உளவு பார்ப்பதன் மூலம் அல்லது DDoS தாக்குதல்களைத் மேற்கொள்ளுதல் மூலம் கப்பத் தொகையைச் செலுத்தும்படி அச்சுறுத்தல் மேற்கொள்ளுவார்.

உங்களையும் உங்கள் சாதனங்களையும் கையகப்படுத்திக்கொள்ள தாக்குதல்காரர்கள மேற்கொள்ளப்படும் செயல்கள் வழமையான விடயங்களாகவே தோன்றுகின்றன. அவற்றில் சில:

- இணைப்பைத் திறக்க அல்லது இணைப்பைக் கிளிக் செய்ய உங்களைத் தூண்டும் மின்னஞ்சல் அல்லது சமூக ஊடகத்தில் ஒரு இடுகையினை இடுதல்.

- நம்பத்தகாத மூலமொன்றிலிருந்து மென்பொருளைப் பதிவிறக்கி நிறுவ மக்களைத் தூண்டுதல்.

- சட்டப்பூர்வமானதாக தோன்றுகின்ற அனால் உண்மையில் அவ்வாறல்லாத , இணையதளத்தில் ஒருவரின் உள்நுழைவு பெயர் மற்றும் கடவுச்சொல்லை உள்ளிடுமாறு தூண்டுதல்.

- உங்கள் சாதனத்தில் வணிகரீதியான வேவுபார் மென்பொருட்கள் செயலியை நிறுவுதல், அதை நீங்கள் கவனிக்காமல் மற்றும் பூட்டாமல் விட்டுவிடலாம்.

டிஜிட்டல் முதலுதவி பொதியின் இந்தப் பிரிவு, உங்கள் சாதனம் பாதிக்கப்பட்டுள்ளதா இல்லையா என்பதைக் கண்டறிய சில அடிப்படை அடிப்படைப் படிநிலையினூடாக உங்களை இட்டுச் செல்கின்றது.

உங்கள் கணினி அல்லது மொபைல் சாதனம் சந்தேகத்திற்கிடமான முறையில் செயல்படத் தொடங்கியுள்ளது என்று நீங்கள் நினைத்தால், அறிகுறிகள் என்ன என்பதை முதலில் சிந்திக்க வேண்டும்.

குறித்த அறிகுறிகள் பொதுவாக படித்தறிந்துகொள்ளக் கூடியவை, அது தொடர்பாக கவலையடைவதற்கான காரணமாக கொள்ளப்படலாகாது. அறிகுறிகளாக:

- தொலைபேசி அழைப்புகளின் போது சத்தங்களைக் கிளிக் செய்தல்

- எதிர்பாராத பேட்டரி இறங்குதல்

- சாதனம் பயன்பாட்டில் இல்லாத போதும் அதிகளவாக சூடாக்குதல்

- சாதனம்மெதுவாக இயங்குதல்

இவை சாதனம் தொரடர்பான கவலைக்குரிய நமபக்கமான குறிகாட்டிகளாக கருதப்படுகின்றன. இருப்ப்பினும் அது தொடர்பாக கவலையடைவதற்கான காரணமாக காணப்படாது.

தாக்குதலுக்குட்பட்ட சாதனத்தின் பொதுவான நம்பத்தக்க அறிகுறிகளாக :

- சாதனம் அடிக்கடி தானாகவே மறுதொடக்கம் செய்தல்

- செயலிகள் செயலிழப்பு, குறிப்பாக உள்ளீடு செயல்பாட்டிற்குப் பின்னர்.

- இயக்க முறைமை மேம்படுத்தல்கள் மற்றும்/அல்லது பாதுகாப்பு இணைப்புகள் மீண்டும் மீண்டும் தோல்வியடைதல்.

- வலைத்தள கமரா பயன்பாட்டில் இல்லாத போது அதன் காட்டி ஒளி இயங்கிக்கொண்டிருத்தல்.

- மீண்டும் மீண்டும் ["மரணத்தின் நீலத் திரைகள்"](https://en.wikipedia.org/wiki/Blue\_Screen\_of\_Death) அல்லது கர்னல் பீதி

- ஒளிரும் சாரலன்கள்

- வைரஸ் எதிர்ப்பு எச்சரிக்கைகள்

## பணிப்பாய்வு

### தொடக்கம்

அறிமுகத்தில் வழங்கப்பட்டுள்ள தகவலின் அடிப்படையில், உங்கள் சாதனம் தாக்கப்பட்டிருக்கலாம் என்று நீங்கள் இன்னும் எண்ணினால், இந்த வழிகாட்டியானது உங்களது பிரச்சினைகளினைக் கண்டுணர உதவும்.

- [எனது மொபைல் சாதனம் சந்தேகத்திற்கிடமான முறையில் செயல்படுகிறது என்று நான் நம்புகிறேன்](#ஃபோன்-அறிமுகம்)

- [எனது கணினி சந்தேகத்திற்கிடமான முறையில் செயல்படுவதாக நான் நம்புகிறேன்](#கணினி அறிமுகம்)

- [எனது சாதனம் சமரசம் செய்யப்படலாம் என்று நான் இனி உணரவில்லை](#சாதனம்-சுத்தம்)

### சாதனம்-சுத்தம் செய்தல்

> சிறப்பு! எவ்வாறிருப்பினும், இந்த வழிமுறைகள் விரைவான பகுப்பாய்வை மட்டுமே செய்ய உதவும் என்பதை நினைவில் கொள்ளுங்கள். தென்படுகின்ற முரண்பாடுகளை அடையாளம் காண இது போதுமானதாக காணப்படும் அதேவேளை , ​​மேலும் அதிநவீன வேவுபார் மென்பொருட்களினால் இன்னும் சிறப்பாக ஒளித்து மறைக்க முடியும்.

சாதனம் தாக்கப்பட்டிருக்கலாமென என்று நீங்கள் இன்னும் சந்தேகித்தால், நீங்கள் இதனை செய்யலாம்:

- [மேலதிக உதவியை நாடுங்கள்](#மால்வேர்\_எண்ட்)

- [நேரடியாகச் சாதனத்தின் மீளமைப்பிற்கு செல்லவும்](#ரீசெட்)

### தொலைபேசி - அறிமுகம்

> உங்கள் சாதனம் எவ்வாறு தாக்கப்பட்டுள்ளது என்பதைக் கருத்தில் கொள்வது அவசியம்.

>

> - உங்கள் சாதனம் சந்தேகத்திற்கிடமான முறையில் செயல்படுவதாக எவ்வளவு காலத்திற்கு முன்பு நீங்கள் சந்தேகிக்க ஆரம்பித்தீர்கள்?

> - தெரியாத மூலங்களிலிருந்து ஏதேனும் இணைப்புகளைக் கிளிக் செய்தது உங்களுக்கு நினைவிருக்கிறதா?

> - நீங்கள் அடையாளம் காணாத கட்சிகளிடமிருந்து செய்திகளைப் பெற்றுள்ளீர்களா?

> - நம்பத்தகாத மூலங்களிலிருந்து பதிவிறக்கம் செய்யப்பட்ட மென்பொருளை நிறுவினீர்களா?

> - சாதனம் உங்கள் கைவசமின்றிக் காணப்பட்டதா?

உங்கள் சாதனம் தாக்கப்படுவதற்கேற்ற வழிவகுத்த சூழ்நிலைகள் ஏதேனும் காணப்பட்டால் , அவற்றை அடையாளம் காண முயற்சிக்க இந்தக் கேள்விகளுக்கு பதிலளிக்கவும்.

- [என்னிடம் Android சாதனம் உள்ளது](#android-intro)

- [என்னிடம் iOS சாதனம் உள்ளது](#ios-intro)

### android-intro

>முதலில் உங்கள் Android சாதனத்தில் ஏதேனும் அறிமுகமில்லாத செயலிகள் நிறுவப்பட்டுள்ளதா என்பதை உறுதிப்படுத்திக்கொள்ளவும்.

>

> அமைப்புகள் மெனுவின் "செயலிகள்" பிரிவில் செயலிகளின் பட்டியலைக் காணலாம். உங்கள் சாதனத்தில் முன்பே நிறுவப்படாத மற்றும் பதிவிறக்கியதாக உங்களுக்கு நினைவில் இல்லாத செயலிகளினைக் கண்டறியவும்.

>

> பட்டியலில் உள்ள செயலிகளில் ஏதேனும் சந்தேகம் இருந்தால், மேலும் குறித்த செயலியானது தீங்கிழைக்கும் பயன்பாட்டைக் கண்டறியும் ஆதாரங்களைத் காணப்படுகின்றனவா என்பதனை கண்டறிய வலைத் தேடலை செய்யவும்.

சந்தேகத்திற்கிடமான பயன்பாடுகள் ஏதேனும் காணப்படுகின்றதா?

- [இல்லை, காணப்படவில்லை](#android-unsafe-settings)

- [ஆம், தீங்கிழைக்கக்கூடிய பயன்பாடுகளை நான் அடையாளம் கண்டுள்ளேன்](#android-badend)

### android-பாதுகாப்பற்ற-அமைப்புகள்

> பயனர்கள் தங்கள் சாதனத்திற்கு குறைந்த அளவிலான அணுகலை இயக்குவதற்கான விருப்பத்தை ஆண்ட்ராய்டடானது வழங்குகிறது. இது மென்பொருள் உருவாக்குநர்களுக்கு பயனுள்ளதாக இருக்கும், ஆனால் அதிகப்படியான தாக்கங்களுக்கு சாதனைகளினை உட்படுத்தக்கூடும்.இந்த பாதுகாப்பு அமைப்புகளை நீங்கள் மீளாய்வு செய்தல் வேண்டும்

அவை பாதுகாப்பான தெரிவுகளுக்கு அமைக்கப்பட்டுள்ளன என்பதை உறுதிப்படுத்தவும். உற்பத்தியாளர்கள் பாதுகாப்பற்ற இயல்புநிலைகளுடன் சாதனங்களை அனுப்பலாம். நீங்களே மாற்றங்களைச் செய்யாவிட்டாலும், இந்த அமைப்புகளை மீளாய்வு செய்தல் வேண்டும்.

>

> #### நம்பகமற்ற மூலங்களிலிருந்து வருகின்ற செயலிகள்

>

> ஆண்ட்ராய்டு பொதுவாக கூகுள் ப்ளே ஸ்டோரிலிருந்து ஏற்றப்படாத ஆப்ஸின் நிறுவலைத் தடுக்கிறது. Play Store இல் உள்ள தீங்கிழைக்கும் பயன்பாடுகளை மதிப்பாய்வு செய்து அடையாளம் காண்பதற்கான செயல்முறைகளை Google கொண்டுள்ளது. தீங்கிழைக்கும் பயன்பாடுகளை நேரடியாகப் பயனருக்குச் செய்தியின் மூலம் அல்லது நிறுவல் கோப்புடன் இணைப்பதன் மூலம் தாக்குதல் நடத்துபவர்கள் இந்தச் சோதனைகளைத் தவிர்க்க முயல்கின்றனர். நம்பத்தகாத மூலங்களிலிருந்து பயன்பாடுகளை நிறுவ உங்கள் சாதனம் அனுமதிக்கவில்லை என்பதை உறுதிப்படுத்துவது முக்கியமானதாகும்.

>

> அறிமுகமில்லாத மூலங்களிலிருந்து செயலிகளினை நிறுவும் செயற்பாடானது உங்கள் தொலைபேசியில் தடுக்கப்பட்டுக் காணப்படுவதனை உறுதிசெய்து கொள்ளுங்கள். பல ஆண்ட்ராய்டு பதிப்புகளில் நீங்கள் பாதுகாப்பு அமைப்புகளில் இந்த விருப்பத்தைக் காண்பீர்கள், ஆனால் நீங்கள் இயங்கும் ஆண்ட்ராய்டின் வகையினைப் பொறுத்து இது வேறு பகுதிகளில் காணப்படலாம், மேலும் புதிய தொலைபேசிகளில் இந்த விருப்பம் ஒவ்வொரு பயன்பாட்டிற்கும் அனுமதி பகுதிகளில் காணக்கூடியயதாக இருக்கும் .

>

> #### உற்பத்தியாளர் பயன்முறை (Developer Mode

)

>

> உற்பத்தியாளர் கள் "உற்பத்தியாளர் பயன்முறையில்" இருக்கும் போது அடிப்படை இயங்குதளத்தில் நேரடியாக கட்டளைகளை இயக்க ஆண்ட்ராய்ட் அனுமதிக்கிறது. இயக்கப்பட்டால், இது சாதனங்களை பௌதீக ரீதியான தாக்குதல்களுக்குட்படுத்தும். சாதனத்திற்கான பௌதீக அணுகலினைக் கொண்டுள்ள ஒருவரினால் சாதனத்தில் உள்ள தனிப்பட்ட தரவின் நகல்களைப் பதிவிறக்க அல்லது தீங்கிழைக்கும் பயன்பாடுகளை நிறுவ, சாதனத்திற்கான உற்பத்தியாளர் பயன்முறையைப் பயன்படுத்த முடியும்.

>

> உங்கள் சாதன அமைப்புகளில் உற்பத்தியாளர் பயன்முறை மெனுவைக் கண்டால், அது முடக்கப்பட்டிருப்பதை உறுதிசெய்ய வேண்டும்.

>

> #### Google Play Protect

>

> அனைத்து சமீபத்திய Android சாதனங்களிலும் Google Play Protect சேவை கிடைக்கிறது. இது உங்கள் சாதனத்தில் நிறுவப்பட்ட அனைத்து பயன்பாடுகளையும் வழக்கமான ஸ்கேன் செய்கிறது. Play Protect உங்கள் சாதனத்திலிருந்து அறியப்பட்ட தீங்கிழைக்கும் பயன்பாடுகளை தானாகவே அகற்றும். இந்தச் சேவையை இயக்குவது உங்கள் சாதனத்தைப் பற்றிய தகவலை (நிறுவப்பட்ட பயன்பாடுகள் போன்றவை) Googleக்கு அனுப்பும்.

>

> உங்கள் சாதன பாதுகாப்பு அமைப்புகளின் கீழ் Google Play Protectஐ இயக்கலாம். மேலும் தகவல் [Play Protect](https://www.android.com/play-protect/) தளத்தில் கிடைக்கும்.

பாதுகாப்பற்ற அமைப்புகளை அடையாளம் கண்டீர்களா?

- [இல்லை, காணப்படவில்லை](#android-bootloader)

- [ஆம், பாதுகாப்பற்ற அமைப்புகளை நான் அடையாளம் கண்டேன்](#android-badend)

### android-bootloader

> Android பூட்லோடர் என்பது உங்கள் சாதனத்தை இயக்கியவுடன் இயங்கும் ஒரு முக்கிய மென்பொருளாகும். வன்பொருளைத் தொடங்கவும் பயன்படுத்தவும் இயக்க முறைமையை செயல்படுத்துகிறது. ஒரு தாக்குதலுக்குட்பட்ட பூட்லோடரானது தாக்குபவருக்கு சாதன வன்பொருளுக்கான முழு அணுகலை வழங்குகிறது. பெரும்பாலான உற்பத்தியாளர்கள் தங்கள் சாதனங்களை பூட்டப்பட்ட பூட்லோடருடன் அனுப்புகிறார்கள். உற்பத்தியாளரின் கையொப்பமிடப்பட்ட பூட்லோடர் மாற்றப்பட்டுள்ளதா என்பதைக் கண்டறிய ஒரு பொதுவான வழி உங்கள் சாதனத்தை மறுதொடக்கம் செய்து துவக்க லோகோவைத் தேடுவதாகும். ஆச்சரியக்குறியுடன் மஞ்சள் முக்கோணம் தோன்றினால், அசல் பூட்லோடர் மாற்றப்பட்டது. உங்கள் சாதனம் திறக்கப்பட்ட பூட்லோடர் எச்சரிக்கைத் திரையைக் காட்டினால் அது தாக்கப்படலாம் மற்றும் LineageOS அல்லது GrapheneOS போன்ற தனிப்பயன் Android ROM ஐ நிறுவ நீங்கள் அதைத் திறக்கவில்லை. நீங்கள் எதிர்பார்க்காத பூட்லோடர் எச்சரிக்கைத் திரையைக் காட்டினால், உங்கள் சாதனத்தின் தொழிற்சாலை மீளமைப்பினைச் (factory reset) செய்தல் வேண்டும்.

பூட்லோடர் தாக்கப்பட்டுள்ளதா அல்லது உண்மையான பூட்லோடர் யைப் பயன்படுத்துகிறதா?

- [எனது சாதனத்தில் பூட்லோடர் தாக்கப்பட்டுள்ளது ](#android-badend)

- [எனது சாதனம் அசல் பூட்லோடரைப் பயன்படுத்துகிறது](#android-goodend)

### android- நல்ல முடிவு

> உங்கள் சாதனம் தாக்கப்பட்டுள்ளதாக த் தெரியவில்லை.

உங்கள் சாதனம் தாக்கப்பட்டுள்ளதாக நீங்கள் இன்னும் கவலைப்படுகிறீர்களா?

- [ஆம், நான் தொழில்முறை உதவியை நாட விரும்புகிறேன்](#மால்வேர்\_எண்ட்)

- [இல்லை, எனது பிரச்சினைகளை நான் தீர்த்துவிட்டேன்](#தீர்ந்தது\_முடிவு)

### android- மோசமான முடிவு

> உங்கள் சாதனம் தாக்குதலுக்குட்பட்டிருக்கலாம். தொழிற்சாலை அமைப்புகளுக்கு மீளமைப்பதன்மூலம் சாதனத்திலுள்ள அனைத்துவிதமான அபாயங்களும் அகற்றிவிடப்படும். எனினும், இது எப்போதும் ஒரு சிறந்த தீர்வுவல்ல. கூடுதலாக, உங்கள் வெளிப்பாட்டின் நிலை மற்றும் நீங்கள் தாங்கிய தாக்குதலின் துல்லியமான தன்மையை அடையாளம் காண நீங்கள் விஷயத்தை மேலும் துருவி ஆராய்தல் வேண்டும்.

>

> சுய-கண்டறிதலுக்கு நீங்கள் [அவசரநிலை VPN](https://www.civilsphereproject.org/emergency-vpn) அல்லது [PiRogue](https://pts-project.org/) என்ற கருவியைப் பயன்படுத்த விரும்பலாம் அல்லது உதவக்கூடிய ஒரு அமைப்பின் உதவியை நாடுங்கள்.

நீங்கள் என்ன செய்ய விரும்புகிறீர்கள்?

- [எனது சாதனத்தை தொழிற்சாலை அமைப்புகளுக்கு மீளமைக்க விரும்புகிறேன்](#ரீசெட்).

- [நான் தொழில்முறை உதவியை நாட விரும்புகிறேன்](#தீம்பொருள்\_எண்ட்)

- [என்னிடம் உள்ளூர் ஆதரவு வலையமைப்பு உள்ளது.

### ios- அறிமுகம்

> இந்தப் படிகளைப் பின்பற்றி, [உங்கள் iPhone அல்லது iPadக்கான அணுகல் யாரிடம் உள்ளது என்பதைப் பார்க்க](https://support.apple.com/en-gb/guide/personal-safety/ipsb8deced49/web). வழக்கத்திற்கு மாறான ஏதேனும் உள்ளதா என்பதைப் பார்க்க, iOS அமைப்புகளைச் சரிபார்க்கவும்.

>

> அமைப்புகள் பயன்பாட்டில், உங்கள் சாதனம் உங்கள் ஆப்பிள் ஐடியுடன் இணைக்கப்பட்டுள்ளதா என்பதைச் சரிபார்க்கவும். இடது புறத்தில் உள்ள முதல் மெனு உருப்படி உங்கள் பெயர் அல்லது உங்கள் ஆப்பிள் ஐடிக்கு நீங்கள் பயன்படுத்தும் பெயராக இருக்க வேண்டும். அதைக் கிளிக் செய்து சரியான மின்னஞ்சல் முகவரி காட்டப்பட்டுள்ளதா எனச் சரிபார்க்கவும். இந்தப் பக்கத்தின் கீழே இந்த ஆப்பிள் ஐடியுடன் இணைக்கப்பட்ட அனைத்து iOS சாதனங்களின் பெயர்கள் மற்றும் மாடல்களைக் கொண்ட பட்டியலைக் காண்பீர்கள்.

>

> நீங்கள் அங்கீகரிக்காத மொபைல் சாதன மேலாண்மை (MDM) அமைப்புடன் உங்கள் சாதனம் இணைக்கப்படவில்லை என்பதைச் சரிபார்க்கவும்

இ. அமைப்புகள் > பொது > VPN & சாதன மேலாண்மை என்பதற்குச் சென்று, சுயவிவரங்களுக்கான பிரிவு உங்களிடம் உள்ளதா எனச் சரிபார்க்கவும். நீங்கள் [தெரியாத உள்ளமைவு சுயவிவரங்களை நீக்கலாம்](https://support.apple.com/en-gb/guide/personal-safety/ips41ef0e8c3/1.0/web/1.0#ips68379dd2e). உங்களிடம் சுயவிவரங்கள் பட்டியலிடப்படவில்லை என்றால், நீங்கள் MDM இல் பதிவுசெய்யப்படவில்லை.

- [அனைத்து தகவல்களும் சரியானவை மற்றும் எனது ஆப்பிள் ஐடியின் கட்டுப்பாட்டினைக் கொண்டுள்ளேன்](#ios-goodend)

- [பெயர் அல்லது பிற விவரங்கள் தவறானவை அல்லது பட்டியலில் என்னுடையது அல்லாத சாதனங்கள் அல்லது சுயவிவரங்களைப் காண்கிறேன் ](#ios-badend)

### ios-goodend

> உங்கள் சாதனம் தாக்கப்பட்டுள்ளதாகத் தெரியவில்லை.

உங்கள் சாதனம் தாக்கப்பட்டுள்ளதாக நீங்கள் இன்னும் கவலையடைகிறீர்களா?

- [ஆம், நான் தொழில்முறை உதவியை நாட விரும்புகிறேன்](#மால்வேர்\_எண்ட்)

- [இல்லை, எனது பிரச்சினைகளை நான் தீர்த்துவிட்டேன்](#தீர்ந்தது\_முடிவு)

### ios- மோசமான முடிவு

> உங்கள் சாதனம் தாக்குதலுக்குட்பட்டிருக்கலாம். தொழிற்சாலை அமைப்புகளுக்கு மீளமைப்பதன்மூலம் சாதனத்திலுள்ள அனைத்துவிதமான அபாயங்களும் அகற்றிவிடப்படும். எனினும், இது எப்போதும் ஒரு சிறந்த தீர்வுவல்ல. கூடுதலாக, உங்கள் வெளிப்பாட்டின் நிலை மற்றும் நீங்கள் தாங்கிய தாக்குதலின் துல்லியமான தன்மையை அடையாளம் காண நீங்கள் விஷயத்தை மேலும் துருவி ஆராய்தல் வேண்டும்.

> சுய-கண்டறிதலுக்கு நீங்கள் [அவசரநிலை VPN](https://www.civilsphereproject.org/emergency-vpn) அல்லது [PiRogue](https://pts-project.org/) என அழைக்கப்படுகின்ற கருவியினைப் பயன்படுத்தலாம் அல்லது உங்களுக்கு உதவக்கூடிய ஒரு அமைப்பின் உதவியை நாடுங்கள்.

நீங்கள் என்ன செய்ய விரும்புகிறீர்கள்?

- [எனது சாதனத்தை தொழிற்சாலை அமைப்புகளுக்கு மாற்றியமைக்க விரும்புகிறேன்](#ரீசெட்).

- [நான் தொழில்முறை உதவியை நாட விரும்புகிறேன்](#மால்வேர்\_எண்ட்)

- [என்னிடம் உள்ளூர் ஆதரவு வலையமைப்பு காணப்படுகின்றது.

### கணினி அறிமுகம்

> \*\*குறிப்பு: நீங்கள் ransomware தாக்குதலுக்கு உள்ளானால் நேரடியாக [No More Ransom!](https://www.nomoreransom.org/) க்குச் செல்லவும்.\*\*

>

> இந்த பணிப்பாய்வு உங்கள் கணினியில் சந்தேகத்திற்கிடமான செயல்பாட்டை விசாரிக்க உதவும். நீங்கள் ஒரு நபருக்கு தொலைதூரத்தில் உதவி செய்தால், [TeamViewer](https://www.teamviewer.com) போன்ற தொலைநிலை டெஸ்க்டாப் மென்பொருளைப் பயன்படுத்தி கீழே உள்ள இணைப்புகளில் விவரிக்கப்பட்டுள்ள படிகளைப் பின்பற்ற முயற்சி செய்யலாம் அல்லது தொலைநிலை தடயவியல் கட்டமைப்புகளைப் பார்க்கலாம். [Google Rapid Response (GRR)](https://github.com/google/grr). இதைச் சரியாகச் செய்ய நெட்வொர்க் தாமதம் மற்றும் நம்பகத்தன்மை அவசியம் என்பதை நினைவில் கொள்ளவும்.

நீங்கள் சரிபார்க்க விரும்பும் இயக்க முறைமையைத் தேர்ந்தெடுக்கவும்:

- [Windows](#windows-intro)

- [macOS](#mac-intro)

### windows- அறிமுகம்

> Windows சாதனங்களில் சந்தேகத்திற்கிடமான செயல்பாட்டை விசாரிக்க இந்த அறிமுக வழிகாட்டியைப் பின்பற்றலாம்:

>

> - [Tek மூலம் Windows இல் தடயவியல் வாழ்வது எப்படி](https://github.com/Te-k/how-to-quick-forensic/blob/master/Windows.md)

ஏதேனும் தீங்கிழைக்கும் செயல்பாட்டைக் கண்டறிய இந்த வழிமுறைகள் உங்களுக்கு உதவியதா?

- [ஆம், கணினி பாதிக்கப்பட்டுள்ளதாக நினைக்கிறேன்](#சாதனத்தால் பாதிக்கப்பட்டுள்ளது)

- [இல்லை, தீங்கிழைக்கும் செயல்பாடு எதுவும் கண்டறியப்படவில்லை](#சாதனம்-சுத்தம்)

### மேக்-அறிமுகம்

> MacOS கணினியில் சாத்தியமான தொற்றுநோயைக் கண்டறிய, நீங்கள் இந்தப் படிகளைப் பின்பற்ற வேண்டும்:

>

> 1. சந்தேகத்திற்குரிய புரோகிராம்கள் தானாகவே தொடங்குகிறதா எனச் சரிபார்க்கவும்

> 2. சந்தேகத்திற்கிடமான இயங்கும் செயல்முறைகளைச் சரிபார்க்கவும்

> 3. சந்தேகத்திற்கிடமான கர்னல் நீட்டிப்புகளைச் சரிபார்க்கவும்

>

> வலைத்தளம் [நோக்கம்-பார்க்க](https://objective-see.com) இந்த செயல்முறையை எளிதாக்கும் பல இலவச மென்பொருள் பயன்பாடுகளை வழங்குகிறது:

>

> - [KnockKnock](https://objective-see.com/products/knockknock.html) தானாகவே தொடங்குவதற்கு பதிவுசெய்யப்பட்ட அனைத்து நிரல்களையும் அடையாளம் காண பயன்படுத்தப்படும்.

> - [TaskExplorer](https://objective-see.com/products/taskexplorer.html) இயங்கும் செயல்முறைகளைச் சரிபார்க்கவும், சந்தேகத்திற்குரியதாகத் தோன்றுவதைக் கண்டறியவும் பயன்படுத்தப்படலாம் (எடுத்துக்காட்டாக, அவை கையொப்பமிடப்படாததால் அல்லது அவை கொடியிடப்பட்டதால் வைரஸ் மொத்தம்).

> - [KextViewr](https://objective-see.com/products/kextviewr.html) macOS கணினியில் ஏற்றப்படும் சந்தேகத்திற்கிடமான கர்னல் நீட்டிப்பைக் கண்டறியப் பயன்படுத்தலாம்.

>

> சந்தேகத்திற்கிடமான எதையும் இவை உடனடியாக வெளிப்படுத்தவில்லை என்றால், மேலும் சோதனையை மேற்கொள்ள விரும்பினால், நீங்கள் [pcQF](https://github.com/botherder/pcqf) ஐப் பயன்படுத்தலாம். pcQF என்பது கணினியில் சில தகவல்களைச் சேகரிக்கும் செயல்முறையை எளிதாக்கும் மற்றும் முழு நினைவக ஸ்னாப்ஷாட்டை எடுக்கும் ஒரு பயன்பாடாகும்.

>

> கூடுதல் விவரங்களைச் சேகரிக்க பயனுள்ளதாக இருக்கும் (ஆனால் டெர்மினல் கட்டளைகளுடன் சில பரிச்சயம் தேவை) கூடுதல் கருவி [AutoMacTC](https://www.crowdstrike.com/blog/automating-mac-forensic-triage/) அமெரிக்க சைபர் செக்யூரிட்டி நிறுவனம் CrowdStrike.

ஏதேனும் தீங்கிழைக்கும் செயல்பாட்டைக் கண்டறிய இந்த வழிமுறைகள் உங்களுக்கு உதவியதா?

- [ஆம், கணினி பாதிக்கப்பட்டுள்ளதாக நினைக்கிறேன்](#சாதனத்தால் பாதிக்கப்பட்டுள்ளது)

- [இல்லை, தீங்கிழைக்கும் செயல்பாடு எதுவும் கண்டறியப்படவில்லை](#சாதனம்-சுத்தம்)

### சாதனம் - பாதிப்படைந்துள்ளது

உங்கள் சாதனம் பாதிக்கப்பட்டுள்ளது போல் தெரிகிறது. இத்தாக்கத்திலிருந்து விடுபட, நீங்கள் செய்ய வேண்டியவை:

- [கூடுதல் உதவியை நாடுங்கள்](#மால்வேர்\_எண்ட்)

- [நேரடியாகச் சாதனத்தின் மீளமைப்பிற்கு செல்லவும்](#ரீசெட்).

### மீளமைப்புச் செய்தல்

> கூடுதல் எச்சரிக்கை நடவடிக்கையாக உங்கள் சாதனத்தை மீட்டமைப்பதை நீங்கள் பரிசீலிக்க விரும்பலாம். கீழே உள்ள வழிகாட்டிகள் உங்கள் சாதன வகைக்கு பொருத்தமான வழிமுறைகளை வழங்கும்:

>

> - [Android](https://support.google.com/android/answer/6088915?hl=ta)

> - [iOS](https://support.apple.com/en-us/HT201252)

> - [Windows](https://support.microsoft.com/en-us/windows/reinstall-windows-d8369486-3e33-7d9c-dccc-859e2b022fc7)

> - [மேக்](ம

ttps://support.apple.com/en-us/HT201314)

உங்களுக்கு கூடுதல் உதவி தேவையென எண்ணுகிறீர்களா?

- [ஆம்](#தீம்பொருள்\_முடிவு)

- [இல்லை](#தீர்க்கப்பட்டது\_முடிவு)

### தீம்பொருள்\_முடிவு

பாதிக்கப்பட்ட சாதனத்தைக் கையாள்வதில் கூடுதல் உதவி தேவைப்பட்டால், கீழே பட்டியலிடப்பட்டுள்ள நிறுவனங்களைத் தொடர்புகொள்ளலாம்.

:[](நிறுவனங்கள்?services=vulnerabilities\_malware)

### தீர்க்கப்பட்ட\_முடிவு

இந்த டிஜிட்டல் முதலுதவி கிட் பணிப்பாய்வு பயனுள்ளதாக இருந்தது என நம்புகிறோம். தயவுசெய்து எங்களுக்கு கருத்து தெரிவிக்கவும் [மின்னஞ்சல் வழியாக](mailto:incoming+rarenet-dfak-8220223-issue-@incoming.gitlab.com)

### இறுதியான\_உதவிக்குறிப்புகள்

உங்கள் சாதனங்கள் மற்றும் தரவை கைப்பற்றுவதற்கான தாக்குதல் காரர்களின் முயற்சிக்கு நீங்கள் பலியாவதனைத் தடுப்பதற்கான சில குறிப்புகள் காணப்படுகின்றன:

- நீங்கள் பெறும் மின்னஞ்சல், நீங்கள் பதிவிறக்கிய கோப்பு அல்லது உங்கள் கணக்கு உள்நுழைவு விவரங்களைக் கேட்கும் இணைப்பு ஆகியவற்றின் சட்டபூர்வமான தன்மையை எப்போதும் இருமுறை உறுதிப்படுத்திக் கொள்ளவும்.

- தீம்பொருள் தொற்றுகளிலிருந்து உங்கள் சாதனத்தை எவ்வாறு பாதுகாப்பது என்பது பற்றி தெரிந்துகொள்ள வளங்களில் இணைக்கப்பட்டுள்ள மூலங்களை வாசியுங்கள்.

#### வளங்கள்

- Security in a Box: [Protect your device from malware and phishing attacks](https://securityinabox.org/en/phones-and-computers/malware)

- Further tips for protecting [Android](https://securityinabox.org/en/phones-and-computers/android), [iOS](https://securityinabox.org/en/phones-and-computers/ios), [Windows](https://securityinabox.org/en/phones-and-computers/windows), [MacOS](https://securityinabox.org/en/phones-and-computers/mac), and [Linux](https://securityinabox.org/en/phones-and-computers/linux) devices

- [Security Self-Defense: How to avoid Phishing Attacks](https://ssd.eff.org/en/module/how-avoid-phishing-attacks)

- [Security without borders: Guide to Phishing](https://github.com/securitywithoutborders/guide-to-phishing/blob/master/SUMMARY.md)