ISSUE 03

Cyber Guardian

2024

Publication for your online safety

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Redness Team
Coordination Centre

நம்பத்தகாத மொபைல் பயன்பாடுகள் உங்கள் பாதுகாப்பு மற்றும் தனியுரிமையை எவ்வாறு அச்சுறுத்துகின்றன.

நம்பத்தகாத மொபைல் பயன்பாடுகள் அவற்றின் தோற்றம், நடத்தை அல்லது சரிபார்ப்பு இல்லாததால் சாத்தியமான பாதுகாப்பு அபாயங்களை ஏற்படுத்தும் பயன்பாடுகள் ஆகும். இந்த Apps பயனர்களுக்கு தீங்கு விளைவிக்கும் வகையில் வடிவமைக்கப்பட்டிருக்கலாம், தனிப்பட்ட தரவை திருடலாம் அல்லது சாதனத்தின் பாதுகாப்பை சமரசம் செய்யலாம். நம்பத்தகாத மொபைல் பயன்பாடுகள் என்ன மற்றும் அவை ஏற்படுத்தும் அபாயங்கள் பற்றிய விரிவான பார்வை இங்கே:

நம்பத்தகாத மொபைல் பயன்பாடுகளின் சிறப்பியல்புகள்

1. அறியப்படாத அல்லது சரிபார்க்கப்படாத ஆதாரங்கள்:

அதிகாரபூர்வ ஆப் ஸ்டோர்களில் (Google Play Store, Apple App Store) பயன்பாடுகள் கிடைக்காது, அதற்குப் பதிலாக மூன்றாம் தரப்பு இணையதளங்கள் அல்லது மாற்று ஆப் ஸ்டோர்களில் காணப்படும்.

2. அதிகப்படியான அனுமதிகள்:

தொடர்புகள், செய்திகள், இருப்பிடம், கேமரா மற்றும் மைக்ரோ.்.போனுக்கான அணுகல் போன்ற அவற்றின் செயல்பாட்டிற்கு தேவையானதை விட அதிகமான அனுமதிகளைக் கோரும் பயன்பாடுகள்.

3. தீங்கிழைக்கும் நோக்கம்:

பயனரின் சாதனத்தில் malware, spyware, adware, ransomware ஐ நிறுவ வடிவமைக்கப்பட்ட பயன்பாடுகள்.

4. ஆள்மாறாட்டம் அல்லது குளோனிங்:

பயனர்களை ஏமாற்றி தகவல்களைத் திருடுவதற்கு முறையான பயன்பாடுகளைப் பிரதிபலிக்கும் போலியான பயன்பாடுகள்.

5. பாதுகாப்பற்ற குறியீட்டு முறை:

தற்செயலாக பயனர் தரவு அல்லது சாதன பாதிப்புகளை வெளிப்படுத்தக்கூடிய மோசமாக குறியிடப்பட்ட பயன்பாடுகள்

நம்பத்தகாத மொபைல் பயன்பாடுகளைப் பயன்படுத்துவது குறிப்பிடத்தக்க பாதுகாப்பு அபாயங்களை ஏற்படுத்தலாம். அத்தகைய பயன்பாடுகளைப் பயன்படுத்துவதில் தொடர்புடைய முதன்மையான பாதுகாப்புக் கவலைகள் இங்கே உள்ளன.

தரவு திருட்டு மற்றும் தனியுரிமை படையெடுப்பு

தனிப்பட்ட தகவலுக்கான அணுகல்: நம்பகமற்ற பயன்பாடுகள் தொடர்புகள், செய்திகள், புகைப்படங்கள் மற்றும் இருப்பிடம் போன்ற தனிப்பட்ட தரவை அணுக அனுமதி கோரலாம். இந்தத் தரவுகள் சேகரிக்கப்பட்டு தவறாகப் பயன்படுத்தப்படலாம்.

அங்கீகரிக்கப்படாத தரவு சேகரிப்பு: இந்த பயன்பாடுகள் பயனர் அனுமதியின்றி முக்கியமான தகவல்களைச் சேகரித்து மூன்றாம் தரப்பினருடன் பகிர்ந்து கொள்ளலாம், இது தனியுரிமை மீறல்களுக்கு வழிவகுக்கும்.

மால்வேர் மற்றும் ஸ்பைவேர்

தீங்கிழைக்கும் மென்பொருள்: நம்பகமற்ற பயன்பாடுகளில் வைரஸ்கள், trojans மற்றும் spyware உள்ளிட்ட தீம்பொருள் இருக்கலாம், அவை உங்கள் சாதனத்தைப் பாதிக்கலாம் மற்றும் தரவைத் திருடலாம் அல்லது சேதத்தை ஏற்படுத்தலாம்.

Keyloggers: சில தீங்கிழைக்கும் பயன்பாடுகள், கடவுச்சொற்கள் மற்றும் பிற முக்கியத் தகவல்கள் உட்பட நீங்கள் தட்டச்சு செய்யும் அனைத்தையும் கைப்பற்றும் keyloggers களை நிறுவலாம்.

நிதி அபாயங்கள்

Phishing Attacks: நம்பகமற்ற பயன்பாடுகள் phishing attacks களை எளிதாக்கலாம், கிரெடிட் கார்டு விவரங்கள் மற்றும் வங்கிச் சான்றுகள் போன்ற நிதித் தகவல்களை வழங்க பயனர்களை ஏமாற்றலாம்.

அங்கீகரிக்கப்படாத பரிவர்த்தனைகள்: இந்த பயன்பாடுகள் அங்கீகரிக்கப்படாத பரிவர்த்தனைகளைத் தொடங்கலாம், இது நிதி இழப்புக்கு வழிவகுக்கும்.

சாதனம் மற்றும் நெட்வொர்க் சமரசம்

ரூட் அணுகல் சுரண்டல்கள் (Root Access Exploits): சில ஆப்ஸ் பாதிப்புகளை பயன்படுத்தி உங்கள் சாதனத்திற்கான Root அணுகலைப் பெறலாம், தாக்குபவர்களுக்கு உங்கள் சாதனத்தின் மீது முழுக் கட்டுப்பாட்டை வழங்குகிறது.

நெட்வொர்க் தாக்குதல்கள்: தீங்கிழைக்கும் பயன்பாடுகள் பிணைய அமைப்புகளை கையாளலாம் அல்லது உங்கள் நெட்வொர்க்கில் தாக்குதல்களை நடத்தலாம், மற்ற இணைக்கப்பட்ட சாதனங்களை சமரசம் செய்யலாம்.

Ransomware

தரவு குறியாக்கம்: Ransomware பயன்பாடுகள் உங்கள் தரவை என்க்ரிப்ட் செய்து அதன் வெளியீட்டிற்கு மீட்கும் தொகையைக் கோரலாம், இது மீட்கும் தொகை செலுத்தப்படாவிட்டால் தரவு இழப்புக்கு வழிவகுக்கும்.

அடையாள திருட்டு

நற்சான்றிதழ் அறுவடை: நம்பகமற்ற பயன்பாடுகள் பல்வேறு சேவைகளுக்கான உள்நுழைவுச் சான்றுகளைத் திருடலாம், இது அடையாளத் திருட்டு மற்றும் உங்கள் கணக்குகளுக்கு அங்கீகரிக்கப்படாத அணுகலுக்கு வழிவகுக்கும்.

ஆட்வேர் மற்றும் தேவையற்ற விளம்பரங்கள்

ஊடுருவும் விளம்பரங்கள்: சில பயன்பாடுகள் ஊடுருவும் விளம்பரங்களைக் காட்டலாம் அல்லது ஆட்வேரை நிறுவலாம்,

→ Page 02

இது தீங்கிழைக்கும் இணையதளங்களுக்குத் திருப்பிவிடுவதன் மூலம் எரிச்சலூட்டும் மற்றும் தீங்கு விளைவிக்கும்.

குறைக்கப்பட்ட சாதன செயல்திறன்

ஆதார வடிகால்: தீங்கிழைக்கும் பயன்பாடுகள் குறிப்பிடத்தக்க அமைப்பு வளங்களை உட்கொள்ளலாம், உங்கள் சாதனத்தை மெதுவாக்கலாம் மற்றும் பேட்டரியை விரைவாக வடிகட்டலாம்.

உங்களை எவ்வாறு பாதுகாத்துக் கொள்வது

1. அதிகாரப்பூர்வ Apps ஸ்டோர்களில் இருந்து பதிவிறக்கம் செய்யுங்கள்: Google Play Store மற்றும் Apple App Store போன்ற நம்பகமான ஆதாரங்களில் இருந்து மட்டுமே பயன்பாடுகளைப் பதிவிறக்கவும்.

2. ஆப்ஸ் அனுமதிகளைச் சரிபார்க்கவும்: Apps கோரும் அனுமதிகளை மதிப்பாய்வு செய்து, அதன் செயல்பாட்டிற்கு அவை அவசியம் என்பதை உறுதிப்படுத்தவும்.

3. மதிப்புரைகள் மற்றும் மதிப்பீடுகளைப் படிக்கவும்: பயன்பாட்டின் நம்பகத்தன்மையை அளவிட பயனர் மதிப்புரைகள் மற்றும் மதிப்பீடுகளைச் சரிபார்க்கவும்.

4. பாதுகாப்பு மென்பொருளை நிறுவவும்: உங்கள் சாதனத்தை ஸ்கேன் செய்து பாதுகாக்க, புகழ்பெற்ற வைரஸ் தடுப்பு மற்றும் மால்வேர் எதிர்ப்பு பயன்பாடுகளைப் பயன்படுத்தவும்.

5. உங்கள் சாதனத்தைப் புதுப்பித்த நிலையில் வைத்திருங்கள்: அறியப்பட்ட பாதிப்புகளை சரிசெய்ய உங்கள் இயக்க முறைமை மற்றும் பயன்பாடுகளை தொடர்ந்து புதுப்பிக்கவும்.

6. Jailbreaking அல்லது Rooting செய்வதைத் தவிர்க்கவும்: இது உங்கள் சாதனத்தை கூடுதல் பாதுகாப்பு அபாயங்களுக்கு ஆளாக்கும்.

7. இணைப்புகள் மற்றும் பதிவிறக்கங்கள் குறித்து எச்சரிக்கையாக இருங்கள்: சந்தேகத்திற்கிடமான இணைப்புகளைக் கிளிக் செய்வதையோ சரிபார்க்கப்படாத மூலங்களிலிருந்து பயன்பாடுகளைப் பதிவிறக்குவதையோ தவிர்க்கவும்.

எச்சரிக்கையாக இருப்பதன் மூலமும், தடுப்பு நடவடிக்கைகளை மேற்கொள்வதன் மூலமும், நம்பத்தகாத மொபைல் பயன்பாடுகளுடன் தொடர்புடைய பாதுகாப்பு மீறல்களின் அபாயத்தைக் கணிசமாகக் குறைக்கலாம்

ETF அதிகாரிகளுக்கான சைபர் பாதுகாப்பு விழிப்புணர்வு திட்டத்தை CERT நடத்துகிறது

CERT சமீபத்தில் பணியாளர்களின் நம்பிக்கை நிதி வாரியத்தின் (ETF) தேர்ந்தெடுக்கப்பட்ட அரசாங்க அதிகாரிகளுக்கு ஏற்ப சைபர் பாதுகாப்பு விழிப்புணர்வு திட்டத்தை வழிநடத்தியது. இம்முயற்சியானது, NextGenGov அறக்கட்டளையின் திறன் மேம்பாட்டுத் திட்டத்துடன் இணைந்து ஒருங்கிணைக்கப்பட்ட திறன் மேம்பாட்டுத் திட்டத்தின் (ICBA) கீழ், இலங்கை தகவல் மற்றும் தொடர்பாடல் தொழில்நுட்ப முகவர் நிறுவனத்தால் (ICTA) ஏற்பாடு செய்யப்பட்டுள்ளது.

Our Services

விரிவான மென்பொருள் பாதுகாப்பு சேவைகள்

விரிவான பாதுகாப்பு நடவடிக்கைகள் மற்றும் இணைய அச்சுறுத்தல்களிலிருந்து மென்பொருள் பயன்பாடுகளைப் பாதுகாப்பதில் நாங்கள் நிபுணத்துவம் பெற்றுள்ளோம் அதிநவீன தொழில்நுட்பங்கள், எங்கள் சேவைகளில் பின்வருவன அடங்கும்:

- **பாதிப்பு மதிப்பீடுகள்:** மொபைல் பயன்பாடுகளுக்கு (Android, iOS, Harmony), மென்பொருள் பயன்பாடுகள், இணைய பயன்பாடுகள் மற்றும் கட்டண நுழைவாயில்கள்.
- **குறியீடு மதிப்புரைகள் மற்றும் ஊடுருவல் சோதனை:** உங்கள் பயன்பாடுகளில் சாத்தியமான பலவீனங்களை அடையாளம் காணுதல்.
- **செயல்திறன் மிக்க பாதுகாப்பு நடைமுறைப்படுத்தல்:** வலுவான firewalls, ஊடுருவல் கண்டறிதல் அமைப்புகள் மற்றும் குறியாக்க நெறிமுறைகள்.
- **இணக்கம்:** பணம் செலுத்துதல் தொடர்பான மொபைலுக்கான VAPT CBSL வழிகாட்டுதல்களின் கீழ் விண்ணப்பங்கள்.
- **பாதுகாப்பு பயிற்சி மற்றும் விழிப்புணர்வு:** கல்வி மற்றும் பாதுகாப்பு அச்சுறுத்தல்களைக் கையாள உங்கள் குழுவைச் சித்தப்படுத்துதல்.
- **பாதுகாப்பு நிகழ்வு பதில்:** உடனடி நடவடிக்கை பாதுகாப்பு சம்பவங்களைத் தணிக்கவும் தீர்க்கவும்.

எங்களுடன் கூட்டுசேர்வதன் மூலம் உங்கள் மென்பொருள் பயன்பாடுகள் உருவாகும் இணைய அச்சுறுத்தல்களுக்கு எதிராக மீள்தன்மையுடன் இருப்பதை உறுதிசெய்கிறோம், உங்களின் மதிப்புமிக்க தரவு ஒருமைப்பாடு மற்றும் ரகசியத்தன்மையைப் பாதுகாக்கிறோம்.

ஒரு ISC2 CC பயிற்சி திட்டம்

இலங்கை அபிவிருத்தி நிர்வாக நிறுவனத்தில் அரசாங்க அதிகாரிகளுக்கு இணையப் பாதுகாப்பு தொடர்பான ISC2 CC பயிற்சித் திட்டத்தை இலங்கை CERT அண்மையில் நடத்தியது.

இந்தப் பயிற்சி ISC2 CC க்கு பங்கேற்பாளர்களுக்குத் தகுதி அளிக்கிறது சான்றிதழ். பொதுத்துறையில் இணைய பாதுகாப்பை மேலும் பராமரிக்க தேவையான ஆதரவை வழங்குவதே இதன் நோக்கம் தீவிரமாக. இந்த திட்டம் ISC2 ஆல் ஆதரிக்கப்பட்டது கொழும்பு அத்தியாயம்.