केंद्रीय रिज़र्व पुलिस बल

साइबर बाइट

जुलाई–2025

फर्ज़ी "e-PAN" ईमेल से लाखों लोग पहचान की चोरी के शिकार बन रहे हैं

QUICK TIPS!

अनावश्यक ऐप्स से अपने मोबाइल की सुरक्षा कैसे करें

PDF दस्तावेज़ में छिपे मैलवेयर को कैसे पहचानें

उत्तराखंड एसटीएफ ने ₹750 करोड़ के अंतरराज्यीय साइबर ठगी के कथित मास्टरमाइंड को गिरफ्तार किया

COMN. & IT DIRECTORATE, CRPF

1. साइबर गीक्स समाचार

ए) मैकडॉनल्ड्स के एआई हायरिंग टूल के पासवर्ड '123456' ने 64 मिलियन आवेदकों का डेटा उजागर हुआ।

मैकहायर " में सुरक्षा चूक पाई गई, जिससे 64 मिलियन नौकरी चाहने वालों से संबंधित संवेदनशील आवेदक डेटा उजागर हुआ है।

जून 2025 के अंत में सुरक्षा शोधकर्ता द्वारा खोजी गई समस्या एक डिफ़ॉल्ट एडमिन लॉगिन और आंतरिक API में एक असुरक्षित डायरेक्ट ऑब्जेक्ट रेफरेंस (IDOR) थी, जो मैकहायर के स्वचालित रिक्रूटर बॉट 'ओलिविया' के साथ आवेदकों के चैट इतिहास तक पहुंच की अनुमति देती थी।

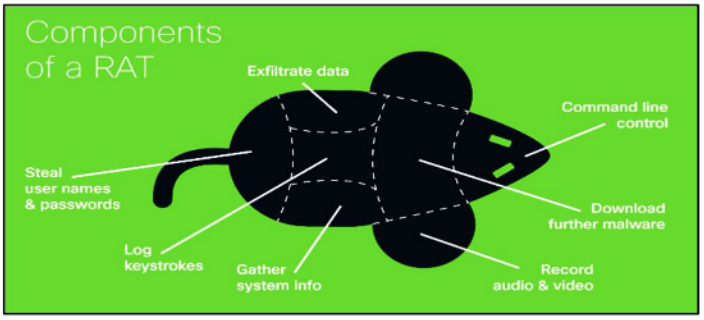
मैकडोनाल्ड्स ने एक घंटे के भीतर ही रिपोर्ट को स्वीकार कर लिया, तथा इसके तुरंत बाद डिफॉल्ट एडमिन क्रेडेंशियल्स को निष्क्रिय कर दिया गया।

मैकडोनाल्डस ने वायर्ड को इस शोध के संबंध में एक बयान में बताया कि "हम एक तृतीय-पक्ष प्रदाता, पैराडॉक्स.एआई की इस अस्वीकार्य कमजोरी से निराश हैं। जैसे ही हमें इस समस्या के बारे में पता चला, हमने पैराडॉक्स.एआई को तुरंत इस समस्या को दूर करने का निर्देश दिया, और जिस दिन हमें इसकी सूचना दी गई, उसी दिन इसका समाधान कर दिया गया"।

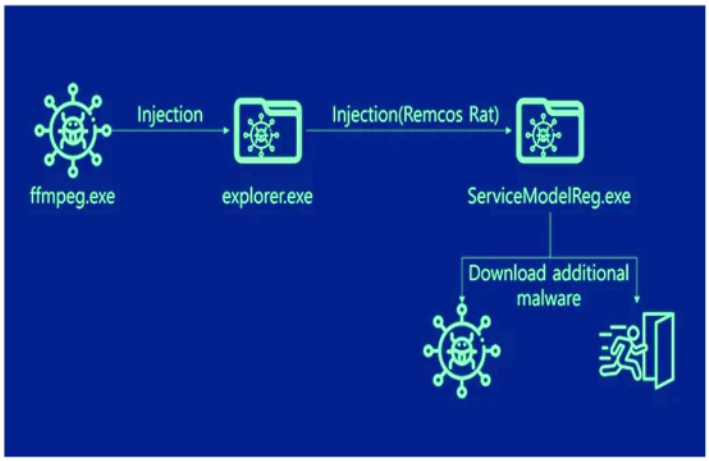
पैराडॉक्स ने असुरक्षित डायरेक्ट ऑब्जेक्ट रेफरेंस (IDOR) की खामी को दूर करने के लिए एक फिक्स लागू किया और पुष्टि की, कि भेद्यता कम हो गई है। Paradox.ai ने कहा है कि वह ऐसी बड़ी समस्याओं की पुनरावृति को रोकने के लिए अपने सिस्टम की समीक्षा कर रहा है।

बी) रेमकोस आरएटी (रिमोट कंट्रोल और सर्विलांस ट्रोजन)

खबर है कि रेमकोस आरएटी (रिमोट कंट्रोल एंड सर्विलांस ट्रोजन) नामक एक मैलवेयर, जो एक परिष्कृत रिमोट एक्सेस ट्रोजन (आरएटी) है। यह जासूसी, क्रेडेंशियल चोरी और सिस्टम पर कब्ज़ा करने के लिए खतरा पैदा करने वाले तत्वों द्वारा इस्तेमाल किया जा रहा है। रेमकोस (रिमोट कंट्रोल एंड सर्विलांस) एक रिमोट एक्सेस ट्रोजन (आरएटी) है जिसे ब्रेकिंग सिक्योरिटी द्वारा बनाया गया है और शुरुआत में इसे रिमोट सिस्टम प्रबंधन के लिए एक वैध उपकरण के रूप में प्रचारित किया गया था हालाँकि, बाद में साइबर अपराधियों और एडवांस्ड पर्सिस्टेंट सटेंट थ्रेट (एपीटी) समूहों द्वारा दुर्भावनापूर्ण गतिविधियों के लिए इसका व्यापक रूप से उपयोग किया जाने लगा ।



हाल ही में हुए एक अभियान में यह देखा गया कि साइबर अपराधियों ने रेमकोस को वितरित करने के लिए एक गुप्त, फ़ाइल-रहित विधि का उपयोग किया । हमलावर एक विशेष रूप से तैयार किए गए पावरशेल लोडर का उपयोग करते हैं जो पूरी तरह से मेमोरी में चलता है और अन्य उन्नत गतिविधियाँ करता है। यह तकनीक मैलवेयर को एंटीवायरस सॉफ़्टवेयर द्वारा पता लगाए जाने से बचाती है और हमलावरों को संक्रमित सिस्टम तक पहुँच बनाए रखते हुए छिपे रहने की अनुमति देती है ।



2. साइबर अपराध

(ए) उत्तराखंड एसटीएफ ने 750 करोड़ रुपये के अंतरराज्यीय साइबर धोखाधड़ी के कथित मास्टरमाइंड को गिरफ्तार किया: -

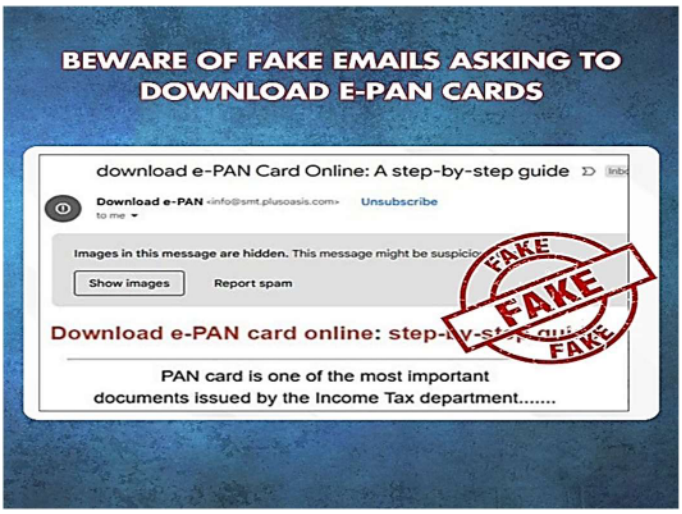
उत्तराखंड स्पेशल टास्क फोर्स (एसटीएफ) ने दिल्ली हवाई अड्डे पर 750 करोड़ रुपये के अंतरराज्यीय साइबर धोखाधड़ी के कथित मास्टरमाइंड को गिरफ्तार करने का दावा किया है।

फर्जी ऋण ऐप का उपयोग करके लोगों को फंसाने के लिए लगभग 35 से 40 फर्जी कंपनियां बनाई गई थी , जिनमें से लगभग 13 कंपनियां उसके नाम पर और 28 उसकी पत्नी के नाम पर थी।

आरोपी कथित तौर पर कंपनियों का प्रतिनिधि बनकर लोगों को परेशान करता था और इंस्ट लोन, मैक्सी लोन, केके कैश, रुपीगो, लेंडकर और अन्य फर्जी लोन ऐप्स के ज़रिए पैसे ऐंठता था। मामले की जाँच के बाद, पुलिस की एक टीम ने पश्चिमी दिल्ली निवासी आरोपी की पहचान इस योजना के मास्टरमाइंड के रूप में की। साइबर टीम ने कानूनी प्रावधानों के तहत आरोपी की तलाश शुरू की और चूँकि वह विदेश में था, इसलिए उसके खिलाफ लुकआउट सर्कुलर (एलओसी) जारी किया गया।

(बी) फर्जी "ई-पैन" ईमेल पहचान चोरी घोटाले के साथ लाखों लोगों को निशाना बनाते हैं:-

प्रेस सूचना ब्यूरो की तथ्य जाँच इकाई ने धोखाधड़ी वाले ईमेल की बढ़ती संख्या को देखते हुए रेड अलर्ट जारी किया है, जो प्राप्तकर्ताओं को नकली ई-पैन कार्ड डाउनलोड करने के लिए लुभाते हैं। ये ईमेल आयकर विभाग से नहीं हैं और दुर्भावनापूर्ण लिंक के ज़रिए बैंक, आधार और व्यक्तिगत जानकारी निकालने के लिए बनाए गए हैं। प्राप्तकर्ताओं से इन संदेशों को डिलीट करने और आधिकारिक अधिकारियों को सूचित करने का पुरज़ोर आग्रह किया जाता है।



फ़िशिंग संदेशों में आमतौर पर विषय पंक्तियां होती हैं, जैसे **"ई-पैन कार्ड ऑनलाइन डाउनलोड करें: चरण-दर-चरण मार्गदर्शिका"**, और दावा किया जाता है कि उन्हें आयकर विभाग ने भेजा है।

दरअसल, ये उपयोगकर्ताओं को साइबर अपराधियों द्वारा नियंत्रित नकली वेबसाइटों पर रीडायरेक्ट करते हैं। लिंक पर क्लिक करने या अटैचमेंट खोलने से मैलवेयर या पहचान की चोरी का खतरा होता है। विभाग ज़ोर देकर सलाह देता है: वह ईमेल के ज़रिए कभी भी व्यक्तिगत पिन, पासवर्ड या ओटीपी नहीं मांगता।

साइबर सुरक्षा विशेषज्ञ बताते हैं कि एक बार जब पीड़ित इन फर्जी ईमेल से जुड़ जाते हैं, तो उन्हें संवेदनशील जानकारी दर्ज करने के लिए कहा जाता है। यह जानकारी स्कैमर्स को बैंक और सरकारी खातों को हैक करने और फिर दूर से ही मैलवेयर तैनात करने में सक्षम बनाती है।

3. इस माह के टिप

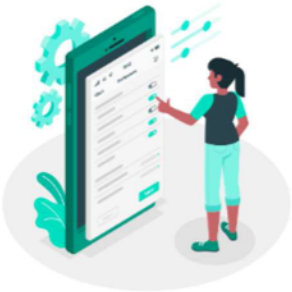
(A) अपने मोबाइल को अनावश्यक एप्लीकेशन से कैसे सुरक्षित रखें

1. **केवल विश्वसनीय स्रोतों से ही ऐप्स डाउनलोड करें।**

Google Play Store या Apple App Store जैसे आधिकारिक ऐप स्टोर से ही ऐप्स डाउनलोड करें। अनजान वेबसाइटों या थर्ड-पार्टी स्टोर से ऐप्स डाउनलोड करने से बचें।

2. **ऐप अनुमतियों की सावधानीपूर्वक समीक्षा करें।**

किसी ऐप को इंस्टॉल या अपडेट करने से पहले, यह देख लें कि वह किन अनुमतियों का अनुरोध करता है। अगर कोई ऐप ज़रूरत से ज़्यादा एक्सेस मांगता है (जैसे कोई कैलकुलेटर ऐप आपके कॉन्टैक्ट्स की अनुमति मांगता है), तो यह एक ख़तरे की घंटी है।



3. **ऐप समीक्षाएं और रेटिंग पढ़ें।**

इंस्टॉल करने से पहले उपयोगकर्ता की प्रतिक्रिया देखें। खराब समीक्षाएं या संदिग्ध व्यवहार की रिपोर्ट आपको चेतावनी दे सकती हैं।

4. **संदिग्ध लिंक या विज्ञापनों पर क्लिक करने से बचें।**

रैंडम पॉप-अप, स्पैम संदेश या संदिग्ध विज्ञापनों द्वारा प्रचारित ऐप्स इंस्टॉल न करें।

5. **अप्रयुक्त ऐप्स को नियमित रूप से अनइंस्टॉल करें।**

अपने इंस्टॉल किए गए ऐप्स की समीक्षा करें और उन ऐप्स को हटा दें जिनका आप अब उपयोग नहीं करते हैं। इससे आपके डिवाइस की सुरक्षा बनी रहती है और जगह भी खाली होती है।

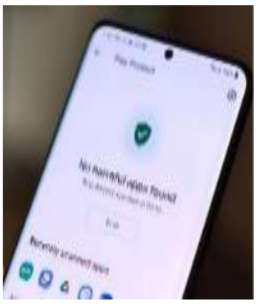
6. **मोबाइल सुरक्षा ऐप्स का उपयोग करें।**

रेपोटेबल एंटीवायरस या सुरक्षा ऐप्स इंस्टॉल करें जो हानिकारक या अनावश्यक ऐप्स को स्कैन करके ब्लॉक कर देते हैं।

7. **अपने डिवाइस और ऐप्स को अपडेट रखें।**

अपडेट सुरक्षा खामियों को दूर करते हैं जिनका फायदा दुर्भावनापूर्ण या अनावश्यक ऐप्स उठा सकते हैं।

8. **एंड्रॉइड डिवाइस पर Google Play Protect सक्षम होना चाहिए।**



(बी) पीडीएफ फाइलों में मैलवेयर का पता कैसे लगाएं

1. पीडीएफ में संदिग्ध संकेतों की तलाश करें।

- पीडीएफ खोलते समय अप्रत्याशित संकेत या पॉप-अप आना।
- पीडीएफ आपसे मैक्रोज़, जावास्क्रिप्ट या अन्य सक्रिय सामग्री को सक्षम करने के लिए कहता है।
- आपकी अपेक्षा की तुलना में फ़ाइल का आकार असामान्य रूप से बड़ा या बहुत छोटा है।
- पीडीएफ में अज्ञात वेबसाइटों पर ले जाने वाले लिंक या बटन होते हैं।
- पीडीएफ व्यक्तिगत जानकारी या लॉगिन क्रेडेंशियल मांगता है।

2. स्रोत की जाँच करें

- केवल विश्वसनीय प्रेषकों या वेबसाइटों से प्राप्त पीडीएफ़ खोलें।
- अप्रत्याशित ईमेल संलग्न या डाउनलोडों से सावधान रहें, विशेष रूप से अज्ञात संपर्कों से।

3. एंटीवायरस या एंटी-मैलवेयर सॉफ़्टवेयर का उपयोग करें

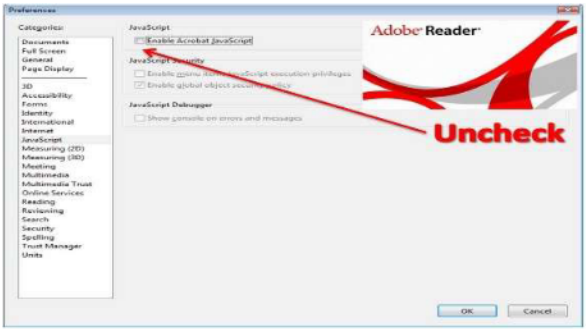
- खोलने से पहले पीडीएफ फाइल को अपडेटेड एंटीवायरस सॉफ्टवेयर से स्कैन करें।
- कई सुरक्षा सुइट्स PDF में एम्बेडेड मेलिशियस कोड का पता लगा सकते हैं।

9. **4. ऑनलाइन पीडीएफ स्कैनर का उपयोग करें।**

- पीडीएफ को वायरस टोटल जैसी सेवाओं पर अपलोड करें ताकि इसे कई एंटीवायरस इंजनों से स्कैन किया जा सके।
- ये उपकरण फ़ाइल का विश्लेषण करते हैं और मैलवेयर का पता चलने पर रिपोर्ट करते हैं।

5. पीडीएफ रीडर में जावा स्क्रिप्ट अक्षम करें

- पीडीएफ में एम्बेडेड अधिकांश मैलवेयर जावास्क्रिप्ट पर निर्भर करता है।
- जब तक आपको फ़ाइल पर पूर्णतः भरोसा न हो, तब तक अपनी पीडीएफ रीडर सेटिंग्स में जावास्क्रिप्ट को अक्षम करें।



6. पीडीएफ को सैंडबॉक्स या वर्चुअल मशीन में खोलें

- यदि आपको कोई संदिग्ध पीडीएफ खोलना ही है, तो अपने मुख्य सिस्टम को संक्रमित होने से बचाने के लिए इसे सैंडबॉक्स्ड वातावरण या वीएम में खोलें।

विश्व पुलिस एवं अग्निशमन खेल सम्मान समारोह 2025, शौर्या, नई दिल्ली।

CWA ने आदित्य बिड़ला प्रोजेक्ट एम-पावर के सहयोग से एक मानसिक स्वास्थ्य विशेष सत्र का आयोजन किया।

सीआरपीएफ के महानिदेशक ने श्री अमरनाथ जी यात्रा मार्ग पर तीर्थयात्रियों से मुलाकात की और उनका हालचाल जाना।

सीआरपीएफ की समर्पित टीमें श्री अमरनाथ जी यात्रा - 2025 के दौरान तीर्थयात्रियों की सहायता करते हुए।

सीआरपीएफ महानिदेशक ने शौर्या, नई दिल्ली में GCOs सम्मेलन की अध्यक्षता की।

सीआरपीएफ महानिदेशक ने वीर बलिदानी सहा0उ0नि0 / जीडी सत्यवान कुमार सिंह के पैतृक गांव रामपुर सोहरौना, यूपी का दौरा किया।