केन्द्रीय रिजर्व पुलिस बल

साइबर बाइट

साइबर बाइट
अगस्त-2024
संस्करण

- टेलीग्राम ऐप की खामी का फायदा उठाकर वीडियो में छिपे मैलवेयर को फैलाया जा रहा है।
- फेक क्राउडस्ट्राइक रिपेयर मैनुअल नए इन्फोस्टीलर मैलवेयर को आगे बढ़ाता है।
- jRAT जावा मैलवेयर का विकास.

- साइबर धोखाधड़ी अपडेट्स

ऑनलाइन वितीय धोखाधड़ी की रिपोर्ट करने के लिए

1930
पर कॉल करें

https://cybercrime.gov.in
पर अपनी शिकायत दर्ज करें

1. साइबर गीक्स समाचार

क) टेलीग्राम ऐप की खामी का फायदा उठाकर वीडियो में छिपे मैलवेयर को फैलाया जा रहा है।

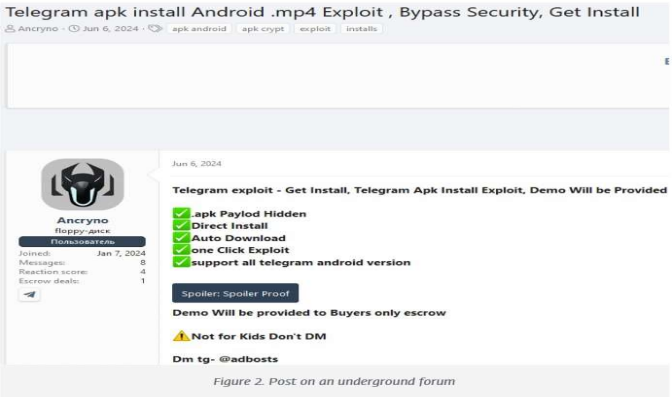
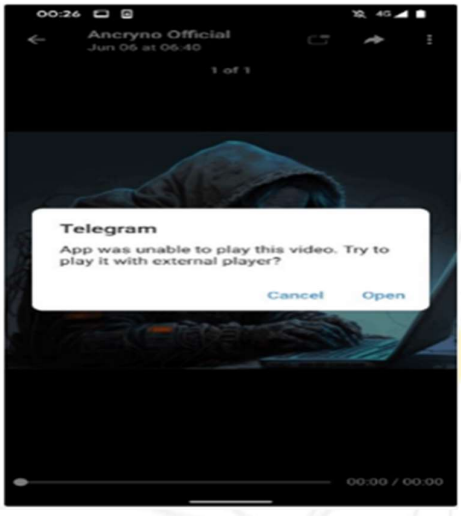


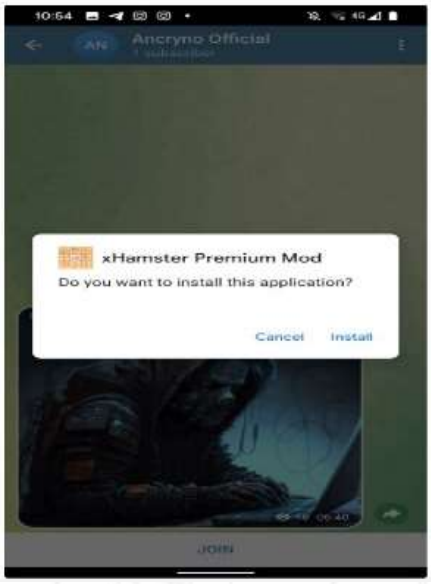
Figure 2. Post on an underground forum

एंड्रॉइड के लिए टेलीग्राम के मोबाइल ऐप में एक जीरो-डे सुरक्षा दोष, जिसे एविल वीडियो कहा जाता है, ने हमलावरों के लिए हानिरहित दिखने वाले वीडियो के रूप में छिपी हुई दुर्भावनापूर्ण फ़ाइलों को संभव बना दिया है। यह कारनामा एक भूमिगत बाज़ार में अज्ञात कीमत पर बिक्री के लिए दिखाई दिया; इस मुद्दे को **टेलीग्राम द्वारा संस्करण 10.14.5 में संबोधित किया गया था।**

"हमलावर, टेलीग्राम चैनलों, समूहों और चैट के माध्यम से दुर्भावनापूर्ण एंड्रॉइड पेलोड साझा करके, उन्हें मल्टीमीडिया फ़ाइलों के रूप में प्रदर्शित कर सकते हैं। ऐसा माना जाता है कि पेलोड को टेलीग्राम के एप्लिकेशन प्रोग्रामिंग इंटरफ़ेस (API) का उपयोग करके तैयार किया गया है, जो चैट और चैनलों पर मल्टीमीडिया फ़ाइलों के प्रोग्रामेटिक अपलोड की अनुमति देता है। ऐसा करने से, यह हमलावर को दुर्भावनापूर्ण **ऐपीके** फ़ाइल को 30 सेकंड के वीडियो के रूप में छिपाने में सक्षम बनाता है।



वीडियो पर क्लिक करने वाले उपयोगकर्ताओं को एक वास्तविक चेतावनी संदेश दिखाया जाता है जिसमें कहा जाता है कि वीडियो नहीं चलाया जा सकता है और उन्हें बाहरी प्लेयर का उपयोग करके इसे चलाने का प्रयास करने का आग्रह किया जाता है। यदि वे इस चरण के साथ आगे बढ़ते हैं, तो उन्हें बाद में टेलीग्राम के माध्यम से एक एपीक फ़ाइल की स्थापना की अनुमति देने के लिए कहा जाता है। विचाराधीन ऐप का नाम 'एक्स हम्स्टर प्रीमियम मॉड " है।



"डिफ़ॉल्ट रूप से, टेलीग्राम के माध्यम से प्राप्त मीडिया फ़ाइलें स्वचालित रूप से डाउनलोड करने के लिए सेट की जाती हैं। " इसका मतलब यह है कि सक्षम विकल्प वाले उपयोगकर्ता उस वार्तालाप को खोलने के बाद स्वचालित रूप से दुर्भावनापूर्ण पेलोड डाउनलोड कर लेंगे जहां इसे साझा किया गया था। हालाँकि इस विकल्प को मैन्युअल रूप से अक्षम किया जा सकता है, फिर भी कथित वीडियो के साथ डाउनलोड बटन को टैप करके पेलोड को डाउनलोड किया जा सकता है। यह ध्यान देने योग्य है कि हमला वेब या समर्पित विंडोज ऐप के लिए टेलीग्राम क्लाइंट पर काम नहीं करता है। फिलहाल यह स्पष्ट नहीं है कि इस शोषण के पीछे कौन है और वास्तविक दुनिया के हमलों में इसका कितना व्यापक उपयोग किया गया था। हालाँकि, उसी एक्टर ने जनवरी 2024 में पूरी तरह से पता न लगाने योग्य एंड्रॉइड क्रिप्टर (उर्फ क्रिप्टोर) का विज्ञापन किया , जो कथित तौर पर गूगल प्ले प्रोटेक्ट को बायपास कर सकता है।

हैम्स्टर कोम्बैट की वायरल सफलता ने दुर्भावनापूर्ण नकल (कोपीकेट) को जन्म दिया#

यह घटनाक्रम ऐसे समय में सामने आया है जब साइबर अपराधी पैसे कमाने के लिए टेलीग्राम आधारित क्रिप्टोकरेंसी गेम 'हैम्स्टर कोम्बैट' का लाभ उठा रहे हैं। ईसेट ने ऐप को बढ़ावा देने वाले नकली ऐप स्टोर, गेम के लिए ऑटोमेशन टूल के रूप में विंडोज के लिए लुम्मा स्टीलर होस्ट करने वाले गिटहब रिपॉजिटरी और रैटल नामक एंड्रॉइड ट्रोजन को वितरित करने के लिए इस्तेमाल किए जाने वाले एक अनौपचारिक टेलीग्राम चैनल का पता लगाया है।

"हैम्स्टर_ईज़ी" नामक टेलीग्राम चैनल के माध्यम से पेश किया जाने वाला रैटल, गेम ("हैम्स्टर.apk") का प्रतिरूपण करने के लिए डिज़ाइन किया गया है और उपयोगकर्ताओं को इसे अधिसूचना एक्सेस देने और खुद को डिफ़ॉल्ट एसएमएस एप्लिकेशन के रूप में सेट करने के लिए प्रेरित करता है।

इसके बाद यह प्रतिक्रिया के रूप में फ़ोन नंबर प्राप्त करने के लिए रिमोट सर्वर से संपर्क शुरू करता है। अगले चरण में, मैलवेयर एक संदेश भेजता है उस फोन नंबर पर रूसी भाषा का एसएमएस संदेश भेजा गया , जो संभवतः मैलवेयर ऑपरेटरों का था, ताकि एसएमएस के माध्यम से अतिरिक्त निर्देश प्राप्त किए जा सकें।

"इसके बाद थ्रेट एक्टर्स एसएमएस के ज़रिए समझौता किए गए डिवाइस को नियंत्रित करने में सक्षम हो जाते हैं: ऑपरेटर के संदेश में किसी निर्दिष्ट नंबर पर भेजे जाने वाला टेक्स्ट हो सकता है, या डिवाइस को उस नंबर पर कॉल करने का निर्देश भी दिया जा सकता है। "मैलवेयर 900 नंबर पर баланс (अनुवाद: बैलेंस) टेक्स्ट के साथ एक संदेश भेजकर पीड़ित के सबैंक रूस के चालू बैंकिंग खाते की शेष राशि की जांच करने में भी सक्षम है।" रैटल अपने भीतर एम्बेडेड हार्ड-कोडेड सूची के आधार पर कम से कम 200 ऐप्स से नोटिफिकेशन छिपाने के लिए अपनी अधिसूचना एक्सेस अनुमतियों का दुरुपयोग करता है। यह संदेह है कि पीड़ितों को विभिन्न प्रीमियम सेवाओं की सदस्यता दिलाने और उन्हें अलर्ट होने से रोकने के प्रयास में ऐसा किया जा रहा है। स्लोवाकियाई साइबरसिक्यूरिटी फ़र्म ने कहा कि उसने नकली एप्लिकेशन स्टोरफ़्रंट भी देखे हैं जो डाउनलोड के लिए हैम्स्टर कोम्बैट की पेशकश करने का दावा करते हैं, लेकिन वास्तव में उपयोगकर्ताओं को अवांछित विज्ञापनों पर निर्देशित करते हैं, और गिटहब रिपॉजिटरी हैम्स्टर कोम्बैट ऑटोमेशन टूल की पेशकश करते हैं जो इसके बजाय लुम्मा स्टीलअर को तैनात करते हैं।

"हैम्स्टर कोम्बैट की सफलता ने साइबर अपराधियों को भी सामने ला दिया है, जिन्होंने गेम के खिलाड़ियों को निशाना बनाकर मैलवेयर का इस्तेमाल करना शुरू कर दिया है। "हैम्स्टर कोम्बैट की लोकप्रियता इसे दुरुपयोग के लिए उपयुक्त बनाती है, जिसका अर्थ है कि इस बात की बहुत अधिक संभावना है कि यह गेम भविष्य में और अधिक साइबर अपराधियों को आकर्षित करेगा।"

बैडपैक एंड्रॉयड मैलवेयर सिस्टम द्वारा नोटिस नहीं किया जाता है#

टेलीग्राम के अलावा, एंड्रॉइड डिवाइसों को लक्षित करने वाली दुर्भावनापूर्ण एपीके फ़ाइलों ने भी बैडपैक का रूप ले लिया है, जो विशेष रूप से तैयार की गई पैकेज फ़ाइलों को संदर्भित करता है जिसमें स्थैतिक विश्लेषण को बाधित करने के प्रयास में ज़िप संग्रह प्रारूप में उपयोग की गई हेडर जानकारी को बदल दिया गया है।

सुझाव

- टेलीग्राम अपडेट: सुनिश्चित करें कि आप ऐप का नवीनतम संस्करण उपयोग कर रहे हैं।
- मैलवेयर के लिए स्कैन करें: अपने डिवाइस की जांच करने के लिए एंटीवायरस सॉफ़्टवेयर का उपयोग करें।
- सावधान रहें: संदिग्ध वीडियो पर क्लिक करने या डाउनलोड करने से बचें।
- 2FA सक्षम करें : अपने टेलीग्राम खाते में दो-कारक प्रमाणीकरण जोड़ें।
- समस्या की रिपोर्ट करें: यदि आपको संदिग्ध गतिविधि का सामना करना पड़े तो टेलीग्राम सहायता को सूचित करें।

ख) फेक क्राउडस्ट्राइक रिपेयर मैनुअल नए इन्फोस्टीलर मैलवेयर को आगे बढ़ाता है।

क्राउडस्ट्राइक ने चेतावनी दी है कि विंडोज डिवाइस को ठीक करने के लिए एक नकली रिकवरी मैनुअल, नई सूचना-चोरी करने वाला मैलवेयर इंस्टॉल कर रहा है जिसे डॉलपु कहा जाता है। बग वाले क्राउडस्ट्राइक फाल्कन अपडेट एक वैश्विक आईटी आउटेज का कारण बना, थ्रेट एक्टर्स ने फेक फ़िक्स के माध्यम से मैलवेयर वितरित करने के लिए जल्दी से इस खबर का लाभ उठाना शुरू कर दिया है। फ़िशिंग ईमेल के माध्यम से चलाया गया एक नया अभियान एक नए रिकवरी टूल का उपयोग करने के निर्देश होने का दिखावा करता है जो हाल ही में क्राउडस्ट्राइक फाल्कन क्रैश से प्रभावित विंडोज डिवाइस को ठीक करता है। सिस्टम पर सक्रिय होने के बाद स्टीलर्स- क्रोम, एज, फ़ायरफ़ॉक्स और Cốc Cốc वेब ब्राउज़र में संग्रहीत खाता क्रेडेंशियल, ब्राउज़र इतिहास और प्रमाणीकरण कुकीज़ को चुरा लेता है।

डोल्पू का प्रसार

ऐसा माना जाता है कि डेटा चोरी करने वाले लोग फ़िशिंग ईमेल के माध्यम से फैलते हैं, जिसमें एक दस्तावेज़ संलग्न होता है, जो माइक्रोसॉफ्ट रिकवरी मैनुअल के रूप में प्रच्छन्न होता है, जिसका नाम 'New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows. docm .' होता है।

यह दस्तावेज़ माइक्रोसॉफ्ट समर्थित बुलेटिन की एक प्रति है जो एक नए माइक्रोसॉफ्ट रिकवरी टूल का उपयोग करने के निर्देश प्रदान करता है जो विंडोस डिवाइस से समस्याग्रस्त क्राउडस्ट्राइक ड्राइवर को स्वचालित रूप से हटा देता है।

हालाँकि, इस दस्तावेज़ में मैक्रोज़ हैं, जो सक्षम होने पर, बाहरी संसाधन से एक बेस 64-एन्कोडेड डीडीएल फ़ाइल डाउनलोड करते हैं और इसे '% TMP%mscorsvc.dll' पर छोड़ देते हैं। इसके बाद, मैक्रोज़ बेस 64-एन्कोडेड डीडीएल को डीकोड करने के लिए विंडोज certutil का उपयोग करते हैं, जिसे समझौता किए गए डिवाइस पर डोल्पू स्टीलर को लॉन्च करने के लिए निष्पादित किया जाता है। डोल्पू सभी चल रही क्रोम प्रक्रियाओं को समाप्त कर देता है और फिर क्रोम, एज, फॉयरफॉक्स और अन्य क्रोमियम ब्राउज़र पर सहेजे गए लॉगिन डेटा और कुकीज़ को इकट्ठा करने का प्रयास करता है।

ब्लीपिंग कंप्यूटर द्वारा किए गए विश्लेषण से पता चलता है कि यह Cốc Cốcm को भी लक्ष्य करता है, जो कि मुख्य रूप से वियतनाम में उपयोग किया जाने वाला एक वेब ब्राउज़र है, जो संभवतः मैलवेयर के उद्गम का संकेत देता है।

चोरी किया गया डाटा '% TMP%/result.txt पर अस्थाई रूप से संरक्षित किया जाता है और 'http[:]//172.104.160[.]126:5000/Uploadss' सर्वर का उपयोग करके हमलावरों को उनके C2 सर्वर पर वापस भेजने के बाद मिटा दिया जाता है।

नए मैलवेयर के बारे में क्राउडस्ट्राइक की सलाह में हमले की कलाकृतियों का पता लगाने के लिए वाईएआरए नियम शामिल है और समझौता के संबंधित संकेतकों को सूचीबद्ध करता है। क्राउडस्ट्राइक अपने ग्राहकों से आग्रह करता है कि वे अपने संचार की प्रामाणिकता की पुष्टि करने के बाद ही कंपनी की वेबसाइट या अन्य विश्वसनीय स्रोतों पर मिलने वाली सलाह का पालन करें।

दुर्भाग्य से, डोल्पू साइबर अपराधियों द्वारा क्राउडस्ट्राइक के फाल्कन अपडेट के कारण उत्पन्न अराजक स्थिति का लाभ उठाने के लिए बड़े पैमाने पर किए गए प्रयासों का नवीनतम उदाहरण है, जिसके कारण लगभग 8.5 मिलियन विंडोज सिस्टम क्रैश हो गए और उन्हें मैन्युअल रूप से पुनर्स्थापित करने के प्रयास की आवश्यकता पड़ी। क्राउडस्ट्राइक फाल्कन आउटेज का लाभ उठाने वाली दुर्भावनापूर्ण गतिविधि में ईरान समर्थक हैकटिविस्ट समूह 'हैंडाला' द्वारा फैलाए गए डेटा वाइपर और क्राउडस्ट्राइक हॉटफ़िक्स के रूप में प्रच्छन्न रेमकोस आरएटी को हाईजैकलोडर द्वारा छोड़ना शामिल है। सामान्य तौर पर, मैलवेयर वितरित करने के लिए क्राउडस्ट्राइक प्रतिनिधियों का प्रतिरूपण करने वाले फ़िशिंग प्रयासों में उल्लेखनीय वृद्धि हुई है और इन दुर्भावनापूर्ण अभियानों को संचालित करने के लिए नए डोमेन पंजीकृत करने का एक बड़ा प्रयास किया गया है।

सुझाव

- दस्तावेज़ की प्रामाणिकता सत्यापित करें।
- एंटीवायरस सॉफ़्टवेयर अपडेट करें।
- उपयोगकर्ताओं को फ़िशिंग खतरों के बारे में शिक्षित करें।
- उन्नत सुरक्षा उपायों का उपयोग करें।
- नियमित रूप से सिस्टम स्कैन करें।
- महत्वपूर्ण डेटा का बैकअप लें।
- असामान्य गतिविधि पर नज़र रखें।
- संदिग्ध ईमेल की रिपोर्ट करें।
- अद्यतन सिस्टम पैच।

ग) jRAT जावा मैलवेयर का विकास.

JRat मैलवेयर, जिसे जावा रिमोट एक्सेस टूल के नाम से भी जाना जाता है, एक प्रकार का रिमोट एक्सेस ट्रोजन (RAT) है जो विंडोज और macOS सिस्टम को लक्षित करता है। यह जावा में लिखा गया है और अपने दुर्भावनापूर्ण कोड को निष्पादित करने के लिए जावा रनटाइम एनवायरनमेंट (JRE) का उपयोग करता है। JRat एक प्रकार का मैलवेयर (दुर्भावनापूर्ण सॉफ़्टवेयर) है जिसे विशेष रूप से जावा-आधारित एप्लिकेशन और सिस्टम को लक्षित करने और हमला करने के लिए डिज़ाइन किया गया है।

JRat मैलवेयर के बारे में कुछ प्रमुख विशेषताएं और तथ्य यहां दिए गए हैं:

1. रिमोट एक्सेस: JRat हमलावरों को संक्रमित सिस्टम तक दूरस्थ रूप से पहुँचने और उसे नियंत्रित करने की अनुमति देता है।
2. कीलॉगिंग: यह कीस्ट्रोक्स को लॉग कर सकता है, तथा पासवर्ड और क्रेडिट कार्ड नंबर जैसी संवेदनशील जानकारी को कैप्चर कर सकता है।
3. स्क्रीन कैप्चर: JRat संक्रमित सिस्टम की स्क्रीन का स्क्रीनशॉट ले सकता है।
4. फ़ाइल प्रबंधन: यह संक्रमित सिस्टम पर फ़ाइलों को अपलोड, डाउनलोड और हटा सकता है।
5. कमांड निष्पादन: JRat संक्रमित सिस्टम पर कमांड निष्पादित कर सकता है और प्रोग्राम चला सकता है।
6. दृढ़ता: यह संक्रमित सिस्टम पर रिबूट करने के बाद भी दृढ़ता बनाए रख सकता है।
7. संचार: JRat HTTP या HTTPS प्रोटोकॉल का उपयोग करके अपने कमांड और कंट्रोल (C2) सर्वर के साथ संचार करता है।
8. अस्पष्टीकरण: यह सुरक्षा सॉफ्टवेयर द्वारा पता लगाने से बचने के लिए अस्पष्टीकरण तकनीकों का उपयोग करता है।
9. वितरण: JRat अक्सर फ़िशिंग ईमेल, संक्रमित सॉफ़्टवेयर डाउनलोड या सुरक्षा संबंधी कमजोरियों के माध्यम से फैलता है।

सुझाव

- सॉफ्टवेयर को अद्यतन रखें।
- मजबूत एंटीवायरस सॉफ़्टवेयर का उपयोग करें।
- संदिग्ध डाउनलोड और ईमेल से बचें।
- मजबूत पासवर्ड का उपयोग करें और दो-कारक प्रमाणीकरण सक्षम करें।
- मैलवेयर के लिए नियमित रूप से सिस्टम को स्कैन करें।

2. साइबर धोखाधड़ी

1. पुणे पुलिस कांस्टेबल से स्टॉक मार्केट निवेश धोखाधड़ी में ₹ 7 लाख की ठगी।

शेयर बाजार में आकर्षक रिटर्न की आड़ में निवेश धोखाधड़ी बढ़ रही है, साइबर अपराधी नागरिकों से करोड़ों रुपये ठग रहे हैं। पता चला है कि पुणे सिटी पुलिस विभाग का एक पुलिस कांस्टेबल ऐसे ही एक घोटाले का शिकार हो गया, जिसमें उसे सात लाख रुपये का नुकसान हुआ। पुलिस कांस्टेबल ने घटना के संबंध में शिवाजी नगर पुलिस स्टेशन में शिकायत दर्ज कराई है। कांस्टेबल को सोशल मीडिया पर एक विज्ञापन दिखा, जिसमें शेयर बाजार में निवेश पर तीन गुना रिटर्न देने

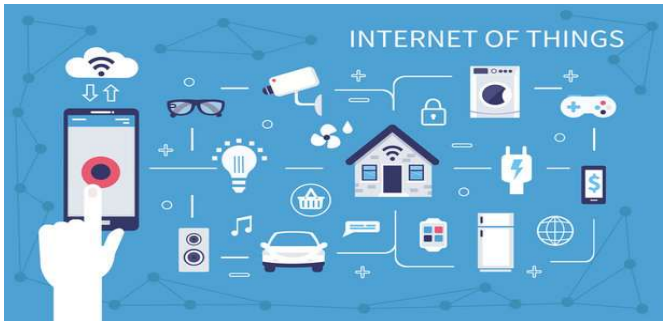
का वादा किया गया था। उत्सुकतावश उसने विज्ञापन में दिए गए फोन नंबर पर संपर्क किया। दूसरी तरफ साइबर अपराधियों ने उसे शेयर बाजार में निवेश पर उच्च रिटर्न का वादा करके लालच दिया। घोटालेबाजों ने उसे एक विशिष्ट ऐप डाउनलोड करने के लिए कहा और उसके बाद उसे इसके माध्यम से निवेश करने के निर्देश दिए। पिछले आठ महीनों में कांस्टेबल ने जालसाजों द्वारा बताए गए बैंक खातों में कुल सात लाख पैंतालीस हजार रुपये ट्रांसफर किए । ऐप ने धोखे से उसके निवेश पर पर्याप्त रिटर्न दिखाया, लेकिन जब उसने कथित लाभ निकालने का प्रयास किया, तो वह ऐसा करने में असमर्थ रहा। जब कांस्टेबल को पता चला कि ठगी करने वालों द्वारा इस्तेमाल किए गए मोबाइल नंबर अब निष्क्रिय हो चुके हैं, तो उसे लगा कि उसके साथ धोखा हुआ है और उसने पुलिस में शिकायत दर्ज कराई। वरिष्ठ पुलिस निरीक्षक फिलहाल मामले की जांच कर रहे हैं।

ii) भोपाल पुलिस ने क्रेडिट कार्ड बनाने के बहाने लोगों को ठगने के आरोप में 4 लोगों को गिरफ्तार किया।

आईसीआईसीआई बैंक का क्रेडिट कार्ड बनाने और आसान बैंक लोन देने के बहाने लोगों को ठगने के आरोप में भोपाल पुलिस ने चार लोगों को गिरफ्तार किया है। कार्रवाई में भोपाल पुलिस की साइबर क्राइम यूनिट ने कम से कम 10 मोबाइल फोन, नौ सिम कार्ड और कई बैंकों की बैंक पासबुक भी जब्त की। पुलिस के मुताबिक, आरोपी बैंक कर्मचारी बनकर लोगों को मुफ्त क्रेडिट कार्ड और आसान लोन देने का लालच देते थे। जब कोई व्यक्ति उनका प्रस्ताव स्वीकार कर लेता था, तो वे एक निजी बैंक की फर्जी वेबसाइट लिंक भेजते थे और उनसे अपनी निजी जानकारी देने को कहते थे। पुलिस को एक व्यक्ति से शिकायत मिली थी जिसने कहा था कि आईसीआईसीआई बैंक का क्रेडिट कार्ड बनाने की आड़ में फर्जी लिंक भेजकर आरोपियों ने उसे ठगा है। व्यक्ति ने अपनी शिकायत में कहा कि आरोपियों ने उसके बैंक खाते से 60,000 रुपये से अधिक की रकम भी निकाल ली।

3.इस माह की टिप

(इंटरनेट ऑफ थिंग्स) के लिए क्या करें और क्या न करें ।



क्या करें :-

डिफ़ॉल्ट पासवर्ड बदलें: प्रत्येक डिवाइस के लिए डिफ़ॉल्ट पासवर्ड को तुरंत मजबूत, यूनिक पासवर्ड से बदलें।

फर्मवेयर को नियमित रूप से अपडेट करें: अपने आईओटी डिवाइस को नवीनतम फर्मवेयर और सुरक्षा पैच के साथ अपडेट रखें।

सशक्त एन्क्रिप्शन का उपयोग करें: सुनिश्चित करें कि आईओटी उपकरणों द्वारा प्रेषित डेटा एन्क्रिप्टेड है।

अपने नेटवर्क को सुरक्षित करें: अपने वाई-फाई नेटवर्क के लिए एक मजबूत, यूनिक पासवर्ड का उपयोग करें और WPA3 एन्क्रिप्शन सक्षम करें।

सेगमेंट नेटवर्क: संभावित उल्लंघनों को सीमित करने के लिए अपने आईओटी उपकरणों के लिए एक अलग नेटवर्क बनाएं।

अनावश्यक सुविधाएँ अक्षम करें: संभावित कमजोरियों को कम करने के लिए उन सुविधाओं और सेवाओं को बंद करें जिनका आप उपयोग नहीं करते हैं।

डिवाइस गतिविधि की निगरानी करें: अपने आईओटी डिवाइस पर किसी भी असामान्य व्यवहार के लिए नियमित रूप से गतिविधि लॉग की जांच करें।

गोपनीयता सेटिंग्स की समीक्षा करें: डेटा संग्रहण और साझाकरण को सीमित करने के लिए आईओटी डिवाइस पर गोपनीयता सेटिंग्स समायोजित करें।

दो-कारक प्रमाणीकरण सक्षम करें: अतिरिक्त सुरक्षा के लिए जब भी संभव हो दो-कारक प्रमाणीकरण (2FA) का उपयोग करें।

स्वयं को शिक्षित करें: नवीनतम आईओटी सुरक्षा प्रथाओं और खतरों के बारे में जानकारी रखें।

क्या न करें :-

अपडेट की अनदेखी न करें: अपने आईओटी उपकरणों के लिए फर्मवेयर और सॉफ्टवेयर अपडेट की अनदेखी न करें।

डिफ़ॉल्ट क्रेडेंशियल का उपयोग न करें: किसी भी आईओटी डिवाइस के लिए डिफ़ॉल्ट उपयोगकर्ता नाम और पासवर्ड का उपयोग करने से बचें।

अनावश्यक डिवाइस कनेक्ट न करें: उन डिवाइस को अपने नेटवर्क से कनेक्ट न करें जिनकी आपको आवश्यकता नहीं है।

गोपनीयता सेटिंग्स की अनदेखी न करें: गोपनीयता सेटिंग्स की अनदेखी न करें; सुनिश्चित करें कि वे आपके डेटा की सुरक्षा के लिए कॉन्फ़िगर की गई हैं।

नेटवर्क सुरक्षा की उपेक्षा न करें: अपने आईओटी उपकरणों के लिए असुरक्षित वाई-फाई नेटवर्क का उपयोग न करें।

पासवर्ड साझा न करें: अपने आईओटी डिवाइस और नेटवर्क के पासवर्ड साझा करने से बचें।

निगरानी करना न भूलें: अपने आईओटी उपकरणों की गतिविधि की नियमित निगरानी करना न भूलें।

सुरक्षा चेतावनियों को अनदेखा न करें: अपने आईओटी उपकरणों से संबंधित सुरक्षा चेतावनियों या चेतावनियों को अनदेखा न करें।

कमजोर पासवर्ड का उपयोग न करें: किसी भी डिवाइस के लिए कमजोर या आसानी से अनुमान लगाए जा सकने वाले पासवर्ड का उपयोग करने से बचें।

सार्वजनिक वाई-फाई से कनेक्ट न करें: उचित सुरक्षा उपायों के बिना अपने आईओटी डिवाइस को सार्वजनिक वाई-फाई नेटवर्क से कनेक्ट न करें।

संचार एवं सूचना प्रौधगिकी निदेशालय ,सीआरपीएफ