केंद्रीय रिजर्व पुलिस बल

साइबर बाइट

- नई वाई-फाई वर्नेबिलिटीज डाउनग्रेड अटैक के माध्यम से नेटवर्क इव्सड्रोपिंग को सक्षम बनाती है।
- रैनसमवेयर अपराधी अब अधिकारियों के बच्चों को सिम स्वैप का उपयोग कर माता-पिता पर दबाब बना रहे हैं।
- साइबर अपराधी एसएमएस फ़िशिंग स्कैम के लिए क्लाउड स्टोरेज का अनुचित फायदा उठाते हैं ।
- फर्जी ए.वी. वेबसाइटों का उपयोग सूचना चुराने वाले मैलवेयर वितरित करने के लिए किया जाता है।

साइबर बाइट
जून-2024
संस्करण

- साइबर फ्रॉड अपडेट्स

ऑनलाइन वित्तीय धोखाधड़ी
की रिपोर्ट करने के लिए

1930
पर कॉल करें

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

1.साइबर गीक समाचार

क) नई वाई-फाई वर्नेबिलिटीज डाउनग्रेड अटैक के माध्यम से नेटवर्क इव्सड्रोपिंग को सक्षम बनाती है।

IEEE 802.11 वाई-फाई मानक में डिज़ाइन दोष से उत्पन्न एक नई सुरक्षा भेद्यता, जो पीड़ितों को कम सुरक्षित वायरलेस नेटवर्क से कनेक्ट करने के लिए प्रेरित करती है, तथा उनके नेटवर्क ट्रैफ़िक पर नजर रखती है।

SSID कन्फ्यूजन अटैक, जिसे CVE-2023-52424 के रूप में ट्रैक किया गया है, सभी ऑपरेटिंग सिस्टम और वाई-फाई क्लाइंट को प्रभावित करता है, जिसमें WEP, WPA3, 802.11X/EAP और AMPE प्रोटोकॉल पर आधारित होम और मेश नेटवर्क शामिल हैं। इस विधि में "विश्वसनीय नेटवर्क नाम (SSID) को स्पूफ करके पीड़ितों को कम सुरक्षित नेटवर्क पर डाउनग्रेड करना शामिल है, ताकि वे अपने ट्रैफ़िक को बाधित कर सकें या आगे हमले कर सकें । एक सफल SSID कन्फ्यूजन अटैक भी विश्वसनीय नेटवर्क पर ऑटो-डिसेबल करने की कार्यक्षमता वाले किसी भी VPN को खुद को बंद कर देता है, जिससे पीड़ित का ट्रैफ़िक उजागर हो जाता है।

सुझावः-

- अपने डिवाइस और फ़र्मवेयर को अपडेट रखें ।
- WPA3 एन्क्रिप्शन सक्षम करें ।
- मजबूत एवं यूनिक पासवर्ड का उपयोग करें।
- नेटवर्क विभाजन को कार्यान्वित करना।
- नेटवर्क ट्रैफ़िक की निगरानी करें ।
- संवेदनशील डेटा के लिए मजबूत एन्क्रिप्शन का उपयोग करें।
- पुराने प्रोटोकॉल को अक्षम करें ।
- सुरक्षा सेटिंग्स की नियमित समीक्षा करें ।
- आपके वाई-फाई नेटवर्क का उपयोग करने वाले उपयोगकर्ताओं को सुरक्षा के सर्वोत्तम अभ्यास के बारे में शिक्षित करे ।
- अपने वाई-फाई राउटर या किसी अन्य नेटवर्क डिवाइस में वर्नेबिलिटीज की रिपोर्ट करें, इसकी रिपोर्ट तुरंत निर्माता या संबंधित सुरक्षा अधिकारियों को दें।

ख) रैनसमवेयर अपराधी अब अधिकारियों के बच्चों को सिम स्वैप का उपयोग कर माता-पिता पर दबाब बना रहे हैं।

गूगल के स्वामित्व वाली कंपनी मैंडिएंट के अनुसार, आरएसएसी संक्रमण "पीड़ित संगठन के खिलाफ एक मनोवैज्ञानिक हमले" में बदल गया है, क्योंकि अपराधी को भुगतान करने के लिए मजबूर करने के लिए व्यक्तिगत और आक्रामक रणनीति का उपयोग कर रहे हैं। हमने ऐसी स्थितियां देखी हैं, जहां धमकी देने वाले अपराधी बच्चों के फोन का सिम स्वैप कर लेते हैं, और उनके बच्चों के फोन नंबरों से अभिभावको को फोन करना शुरू कर देते हैं। मनोवैज्ञानिक दुविधा जिससे कार्यकारी गुजरता है - बच्चों से फोन कॉल देखना, फोन उठाना और यह सुनना कि यह किसी और की आवाज है? कभी-कभी, यह कॉलर आईडी स्पूफिंग होती है। कभी - कभी, हम परिवार के सदस्यों का सिम स्वैप करते हुए देखते हैं।" किसी भी तरह से, यह भयावह है। बच्चों का फोन कॉल देखना, फोन उठाना और यह सुनना कि यह किसी और की आवाज है।

सुझावः-

- सिम कार्ड लॉक सक्षम करें:
- मजबूत एवं यूनिक पासवर्ड का उपयोग करें।
- बहु-कारक प्रमाणीकरण (MFA) लागू करना
- अभिभावको और उनके परिवारों को शिक्षित करें।
- सुरक्षा सेटिंग्स की नियमित समीक्षा और अद्यतन करें।
- संदिग्ध गतिविधि के लिए खातों की निगरानी करें।
- व्यक्तिगत जानकारी के प्रकटीकरण को सीमित करें।
- डिवाइस को नवीनतम सॉफ्टवेयर से सुरक्षित करें।
- संचार प्रोटोकॉल स्थापित करें।
- संदिग्ध गतिविधि की रिपोर्ट करें।

ग) साइबर अपराधी एसएमएस फ़िशिंग स्कैम्स के लिए क्लाउड स्टोरेज का फायदा उठाते हैं।

आपराधिक अभियानों की एक श्रृंखला जो **अमेज़न एस3, गूगल क्लाउड स्टोरेज, बैकब्लेज बी2 और आईबीएम क्लाउड ऑब्जेक्ट स्टोरेज** जैसी **क्लाउड स्टोरेज** सेवाओं का दोहन करती है। अज्ञात खतरनाक तत्वों द्वारा संचालित इन अभियानों का उद्देश्य उपयोगकर्ताओं को **मालीशियस** वेबसाइटों पर पुनर्निर्देशित करना है, जहां वे एसएमएस संदेशों का उपयोग करके उनकी जानकारी चुराना चाहते हैं। **हमलावरों के दो प्राथमिक लक्ष्य होते हैं।**

सबसे पहले, वे यह सुनिश्चित करना चाहते हैं कि नेटवर्क फायरवॉल द्वारा पता लगाए बिना ही जालसाज वाले टेक्स्ट संदेश मोबाइल हैंडसेटों तक पहुंच जाएं। **दूसरा,** वे उपयोगकर्ताओं को यह विश्वास दिलाना चाहते हैं कि उन्हें प्राप्त संदेश या लिंक विश्वसनीय हैं। क्लाउड स्टोरेज प्लेटफॉर्म का लाभ उठाकर, एम्बेडेड स्पैम यूआरएल के साथ स्थिर वेबसाइटों को होस्ट करके, हमलावर अपने संदेशों को सही दिखाते हैं और सामान्य सुरक्षा उपायों से बचते हैं। क्लाउड स्टोरेज सेवाएं संगठनों को फ़ाइलों को संग्रहीत और प्रबंधित करने तथा वेबसाइट परिसंपत्तियों को स्टोरेज बकेट में संग्रहीत करके स्थिर वेबसाइटों को होस्ट करने की अनुमति देती हैं। साइबर अपराधियों ने इन प्लेटफार्मों पर संग्रहीत स्थिर वेबसाइटों में स्पैम यूआरएल एम्बेड करके इस क्षमता का फायदा उठाया है।

सुझावः-

- एसएमएस फ़िल्टरिंग लागू करें।
- रेपुटबल क्लाउड स्टोरेज प्रदाताओं का उपयोग करें।
- संवेदनशील डेटा एन्क्रिप्ट करें।
- मल्टी-फ़ैक्टर प्रमाणीकरण (MFA) सक्षम करें।
- संदिग्ध गतिविधि पर नज़र रखें।
- नियमित रूप से एक्सेस कंट्रोल की समीक्षा करें।
- मोबाइल डिवाइस प्रबंधन (एमडीएम) लागू करें।
- एंटी-फ़िशिंग समाधान तैनात करें।
- फ़िशिंग प्रयासों की रिपोर्ट करें।

घ) फर्जी ए.वी. वेबसाइटें, जिनका उपयोग सूचना चुराने वाले मैलवेयर वितरित करने के लिए किया जाता है।

विंडोज़ के लिए मुफ़्त बिटडिफ़ेंडर एंटीवायरस ।

विंडोज़ के लिए केवल एक ही मुफ्त एंटीवायरस सॉफ्टवेयर चुनें जो आपके कंप्यूटर को साफ, तेज और वायरस मुक्त रखता है और आपको नवीनतम ई-खतरों से बचाता है। खतरा पैदा करने वाले तत्वों ने मैलवेयर वितरित करने के लिए अवास्ट, बिटडिफेंडर और मालवेयरबाइट्स जैसे सही एंटीवायरस उत्पादों के रूप में नकली AV वेबसाइटों का उपयोग किया। अप्रैल 2024 के मध्य में, ट्रेलिक्स एडवांस्ड रिसर्च सेंटर टीम के शोधकर्ताओं ने सूचना-चोरी करने वालों को वितरित करने के लिए इस्तेमाल की जाने वाली कई नकली AV साइटों को देखा। **मालीशियस** वेबसाइटों ने APK, EXE और Inno सेटअप इंस्टॉलर जैसी परिष्कृत **मालीशियस** फ़ाइलें होस्ट कीं, जिनमें Spy भी शामिल है और चोरी करने की क्षमताएं। नकली वेबसाइटें एवास्ट, बिटडिफेंडर और मालवेयरबाइट्स के सही एंटीवायरस उत्पादों के रूप में प्रच्छन्न थीं। मैलवेयर होस्ट करने वाली साइटें हैं। avast-securedownload. Com (Avast.apk), bitdefender-app.com(set-up win x64 x64.exe.zip), malwarebytes.pro (mBsetup.rar).

मालीशियस वेबसाइटों की सूची।

avast-securedownload[.]com: स्पाइनोट ट्रोजन को एंड्रॉइड पैकेज फ़ाइल ("Avast. Apk") के रूप में वितरित करता है, जो एक बार इंस्टॉल होने के बाद एसएमएस संदेश और कॉल लॉग पढ़ने, ऐप्स इंस्टॉल करने और हटाने, स्क्रीनशॉट लेने, स्थान ट्रैक करने और क्रिप्टोकरेंसी माइनिंग जैसी घुसपैठ अनुमतियों का अनुरोध करता है।

bitdefender-app[.]com: एक ज़िप संग्रह फ़ाइल ("setup- win-x86-64.exe.zip") वितरित करता है जिसका उपयोग लुम्मा सूचना चुराने वाले को प्रसारित करने के लिए किया गया था।

malwarebytes[.]pro: एक rar संग्रह फ़ाइल ("MBSetup. rar") वितरित करता है जिसका उपयोग StealC सूचना चुराने वाले मैलवेयर को तैनात करने के लिए करते थे । विशेषज्ञों ने एक दुर्भावनापूर्ण ट्रेलिक्स बाइनरी भी खोजी जो वैध होने का दिखावा करती है **(AMCoreDat.exe)** ।

सुझावः-

- रेपुटबल एंटीवायरस सॉफ़्टवेयर का उपयोग करें ।
- वेब फ़िल्टरिंग लागू करें। ब्राउज़र सुरक्षा सुविधाएँ सक्षम करें।
- एंडपॉइंट सुरक्षा तैनात करें।
- नेटवर्क ट्रैफ़िक की निगरानी करें।
- नियमित सुरक्षा ऑडिट आयोजित करें।
- सॉफ्टवेयर को पैच और अपडेट करें।
- न्यूनतम पहुँच का प्रावधान लागू करें।
- घटना प्रतिक्रिया प्रक्रियाएँ स्थापित करें।

2. साइबर फ्रॉड

क) दिल्ली पुलिस ने जामताड़ा में फर्जी विज्ञापनों के जरिए लोगों को ठगने वाले एक साइबर जालसाज को गिरफ्तार किया है।

ऑनलाईन फर्जी विज्ञापन चलाकर लोगों से पैसे ऐंठने वाले 18 वर्षीय युवक को दिल्ली पुलिस ने झारखंड के जामताड़ा से गिरफ्तार किया है । आरोपी ने अपने पीड़ितों के कंप्यूटर पर नियंत्रण करने के लिए रिमोट डेस्कटॉप ऐप का इस्तेमाल किया। पुलिस ने पाया कि आरोपी ने अब तक 1 करोड़ रुपये से अधिक की ठगी की है। जालसाज ने सर्च इंजन वेबसाइटों पर इस तरह से फर्जी विज्ञापन डालना शुरू कर दिया कि यदि

कोई उपयोगकर्ता किसी विशेष सेवा प्रदाता की आधिकारिक ग्राहक सेवा हेल्पलाइन खोजता है, तो वेब लिंक उसकी वेबसाइट पर रीडायरेक्ट हो जाती है । इस तरह, एक बेखबर एयरलाइन टिकट धारक, जवाहरलाल नेहरू विश्वविद्यालय के एक प्रोफेसर ने रद्दीकरण रिफंड का लाभ उठाने के लिए वेबसाइट का नाम खोजा । उपयोगकर्ता ने वेबसाइट पर दिए गए नंबर पर डायल किया और आरोपी ने खुद को एयरलाइन का ग्राहक सेवा प्रतिनिधि बताया। इसके बाद पीड़ित को शिकायत दर्ज कराने के लिए रिमोट डेस्कटॉप कंट्रोल एप्लीकेशन डाउनलोड करने के लिए कहा गया, लेकिन उसे एक फिशिंग लिंक प्रदान किया गया। यह लिंक बैंक खाता विवरण फॉर्म जैसा था, जो बैंकों द्वारा उपयोग किए जाने वाले फॉर्म जैसा था। पीड़ित द्वारा बैंक विवरण दर्ज करने के बाद, जालसाज ने उसके नेटबैंकिंग में लॉग इन किया और 7 लाख रुपये से अधिक की रकम उड़ा ली। पुलिस में शिकायत दर्ज कराई गई। मनी ट्रेल की जांच से पता चला कि पैसा देश भर में अलग-अलग स्थानों, जैसे कोलकाता, मुंबई, लुधियाना और वाराणसी में चार खातों में भेजा गया था। पुलिस ने विज्ञापित मोबाइल नंबर का पता लगाया तो वह झारखंड के जामताड़ा का निकला। सुबह के समय पुलिस की छापेमारी में जालसाज को गिरफ्तार कर लिया गया और साइबर धोखाधड़ी में उसके भाई और सहयोगी को भी गिरफ्तार कर लिया गया।

ख) साइबर धोखेबाज माता-पिता के भावनात्मक पक्ष को निशाना बनाते हैं।

चेन्नई: साइबर अपराध शाखा या प्रवर्तन निदेशालय (ईडी) के अधिकारी बनकर पैसे ऐंठने वाले साइबर अपराधियों ने अब अपना रुख बदल लिया है और गंभीर आरोपों में उनके वयस्क बच्चों को हिरासत में लेने या गिरफ्तार करने का दावा करके संभावित पीड़ितों को धमकी देते है। हाल ही की एक घटना में, एक व्यवसायी को एक व्यक्ति का फोन आया जिसने खुद को एक पुलिस अधिकारी के रूप में पेश किया और उसकी बेटी को धोखाधड़ी जालसाजी में उसको और उसके दोस्तों से जुड़े मामले से मुक्त करने के लिए 1 लाख की मांग की । अपने बयान में, साइबर क्राइम पुलिस ने कहा कि जालसाज आमतौर पर पीड़ित के साथ एक फोन कॉल से संपर्क शुरू करता है जो पुलिस अधिकारी या सरकारी अधिकारी होने का दावा करते है । उनका कहना है कि पीड़िता के परिवार के सदस्य, आमतौर पर बेटा या बेटी, किसी गंभीर अपराध में शामिल रहे हैं और उन्हें गिरफ्तार किया जा सकता है । वे कहानी को विश्वसनीय बनाने के लिए केस संख्या जैसे विवरण गढ़ते है तथा कानूनी परिणामों का डर दिखाते है ।

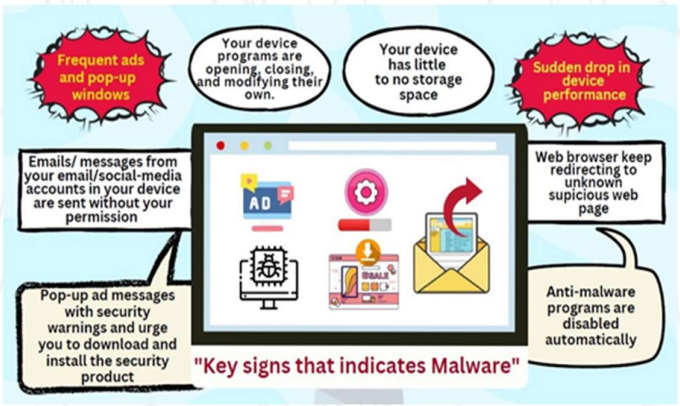
जालसाज फ़ोन नंबरों को सही साबित करने के लिए वो रोने या चिल्लाने जैसी परेशान करने वाली ध्वनियों के तकनीकों का उपयोग कर सकता है ।

पीड़ित पर जल्दी कार्रवाई करने के लिए जालसाज की मांगों को पूरा करने का दबाव होता है, जिसमें आम तौर पर धन या पैसे जैसे जानकारी का हस्तांतरण शामिल होता है। विज्ञप्ति में कहा गया है कि जालसाज पीड़ित को फोन पर बने रहने तथा किसी से भी, विशेषकर परिवार के सदस्य से संपर्क न करने का निर्देश देकर बाहरी संपर्क या सत्यापन से अलग कर देते है ।

जालसाज तब मनगढ़ंत संकट को हल करने या आगे के परिणामों को रोकने के लिए पीड़ित से तत्काल पैसे भुगतान या अन्य प्रकार के अनुपालन की मांग करता है। कुछ अनहोनी के डर से पीड़ित साइबर जालसाज को पैसे भुगतान कर देता है। हाल ही में, चेन्नई के एक निवासी को एक फोन आया जिसमें फोन करने वाले ने दावा किया कि उसकी बेटी को मनी लॉन्ड्रिंग के मामले में गिरफ्तार कर लिया गया है और उसकी पहचान मीडिया को उजागर कर दी जाएगी । फोन करने वाले ने 40 हजार ऑनलाइन ट्रांसफर करने की मांग की। जब पीड़ित ने कहा कि उसके पास इतने पैसे नहीं हैं तो फोन करने वाले ने उससे 5 हजार देने को कहा। उसने पैसे देने का प्रयास किया लेकिन पिन में गलती हो गई। हालाँकि, पीड़ित अपने दोस्त के फोन के जरिए अपने परिवार तक पहुंचने में कामयाब रहा और पुष्टि हो गई कि उनकी बेटी घर पर है, जिसके पश्चात उसने कॉल डिस्कनेक्ट कर दिया ।

3. इस माह के टिप

मैलवेयर के प्रमुख संकेत और सुरक्षात्मक उपाय:-



- अज्ञात स्रोत से प्राप्त संदिग्ध ईमेल, लिंक और साइटों पर क्लिक करने से बचें ।
- जैसे ही आप किसी भी मालीशियस लिंक पर क्लिक करते हैं, आपका मोबाइल हैक हो सकता है या आपका डेटा चोरी हो सकता है।
- केवल सुरक्षित और अधिकृत वेबसाइटें ही ब्राउज़ करें।
- अपने कंप्यूटर सॉफ़्टवेयर/ब्राउज़र को हमेशा अपडेट रखें।
- अपने डेटा का बैकअप नियमित रूप से बनाए रखें।
- वेबसाइटों पर प्रदर्शित होने वाले मालीशियस विज्ञापनों को रोकने के लिए पॉप-अप/एड-ब्लॉकर जैसे सॉफ़्टवेयर इंस्टॉल करें।
- अपने डिवाइस में एंटीवायरस और एंटीमैलवेयर समाधान इंस्टॉल करें और उन्हें अपडेट रखें।
- चैट या सोशल मीडिया पोस्ट के प्राप्त लिंक के माध्यम से कोई भी ऐप इंस्टॉल न करें।


9 अप्रैल 202


Celebrating Moments


PPT ON GRIEVANCE REDRESSAL OF MARTYRS' NOKs


DIRECTORATE GENERAL
SERVICE AND LOYALTY