केंद्रीय रिजर्व पुलिस बल

साइबर बाइट

सस

साइबर बाइट
जुलाई-2024
संस्करण

- राफेल रैट, एंड्रॉयड मैलवेयर जासूसी से लेकर रैनसमवेयर ऑपरेशन तक।
- नई आक्रमण तकनीक 'स्लीपी पिकल' मशीन लर्निंग मॉडलों को लक्ष्य बनाती है।
- नया क्रेडिट कार्ड स्किमर वर्डप्रेस, मैगेंटो और ओपनकार्ट साइटों को लक्षित करता है।

- **साईबर धोखाधडी अपडेट**

ऑनलाइन वितीय धोखाधड़ी की रिपोर्ट करने के लिए
1930
पर कॉल करें

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

1.साइबर गीकस समाचार

ए) राफेल रैट, एंड्रॉयड मैलवेयर जासूसी से लेकर रैनसमवेयर ऑपरेशन तक ।

एंड्रॉइड, गुगल का सबसे लोकप्रिय मोबाइल ऑपरेटिंग सिस्टम है, जो दुनिया भर में अरबों स्मार्टफोन और टैबलेट को शक्ति प्रदान करता है। अपने ओपन-सोर्स स्वभाव और लचीलेपन के लिए जाना जाने वाला, एंड्रॉइड उपयोगकर्ताओं को गुगल प्ले स्टोर और अन्य स्रोतों के माध्यम से सुविधाओं, अनुकूलन विकल्पों और अनुप्रयोगों के विशाल पारिस्थितिकी तंत्र तक पहुंच की एक विस्तृत श्रृंखला प्रदान करता है।

हालाँकि, व्यापक रूप से अपनाए जाने और खुले वातावरण में दुर्भावनापूर्ण गतिविधियों का जोखिम होता है। एंड्रॉइड मैलवेयर, डिवाइस को लक्षित करने के लिए डिज़ाइन किया गया एक दुर्भावनापूर्ण सॉफ़्टवेयर है, जो उपयोगकर्ताओं की गोपनीयता, सुरक्षा और डेटा सुरक्षा / गोपनीयता के लिए एक महत्वपूर्ण खतरा है। ये दुर्भावनापूर्ण प्रोग्राम विभिन्न रूप में आते हैं, जिनमें वायरस, ट्रोजन, रैनसमवेयर, स्पाइवेयर और एडवेयर शामिल हैं, और वे ऐप डाउनलोड, दुर्भावनापूर्ण वेबसाइट, फ़िशिंग हमले और यहां तक कि सिस्टम की कमजोरियों जैसे कई वैक्टरों के माध्यम से डिवाइस में घुसपैठ कर सकते हैं।

एंड्रॉइड मैलवेयर का विकसित परिदृश्य उपयोगकर्ताओं, डेवलपर्स और सुरक्षा विशेषज्ञों के लिए चुनौतियां पैदा करता है। चूंकि हमलावर पहचान से बचने और डिवाइस से तालमेल करने के लिए तेजी से परिष्कृत तकनीकों का उपयोग करते हैं, इसलिए एंड्रॉइड मैलवेयर की प्रकृति, इसके वितरण के तरीके और प्रभावी रोकथाम और शमन रणनीतियों को समझना सर्वोपरि हो जाता है।

राफेल आरएटी एक ओपन-सोर्स मैलवेयर उपकरण/औजार है जो एंड्रॉइड डिवाइस पर गुप्तरूप से काम करता है । यह मैलिसियस ऐक्टर के कार्यो को दूर से नियंत्रित करने के लिए एक शक्तिशाली उपकरण प्रदान करता है, जो डेटा चोरी से लेकर डिवाइस में हेरफेर तक की कई तरह की दुर्भावनापूर्ण गतिविधियों को सक्षम बनाता है ।

राफेल आरएटी का उपयोग करते हुए नोडल ऐजेंसी ने एपीटी-सी-35 / डोनॉट टीम की पहचान की । राफेल की विशेषताएं और क्षमताएं, जैसे कि रिमोट एक्सेस, निगरानी, डेटा चुराना और सुदृढ तंत्र, इसे गुप्त क्रियाएं करने और उच्च-क्षमता वाले/ सुरक्षित निशानों में घुसपैठ करने के लिए एक सुदृढ़/ मजबूत उपकरण बनाते हैं।

सुझाव

- अपने डिवाइस/ यंत्रों को अधतन रखें ।
- विश्वसनीय/ प्रतिष्ठित सुरक्षा सॉफ्टवेयर का उपयोग करें ।
- एप्लिकेशन अनुमतियों की सावधानीपूर्वक समीक्षा करें और उनका प्रबंधन करें ।
- फ़िशिंग और सोशल इंजीनियरिंग से सावधान रहें।
- क्लाउड स्टोरेज या बाहरी उपकरण को सुरक्षित रखने के लिए एंड्रॉइड डिवाइस पर संग्रहीत महत्वपूर्ण डेटा का नियमित रूप से बैकअप लें ।
- सशक्त प्रमाणीकरण का उपयोग करें ।
- डिवाइस पर संग्रहीत संवेदनशील डेटा की सुरक्षा के लिए डिवाइस एन्क्रिप्शन का उपयोग करें।
- किसी विश्वसनीय/प्रतिष्ठित मोबाइल सुरक्षा ऐप का उपयोग करके अपने डिवाइस को मैलवेयर से सुरक्षा के लिए नियमित रूप से स्कैन करें ।

बी) नई अटैक की तकनीक 'स्लीपी पिकल' मशीन लर्निंग मॉडल को निशाना बनाती है ।

स्लीपी पिकल नामक एक नई "हाइब्रिड मशीन लर्निंग (एमएल) मॉडल एक्सप्लॉइटेशन तकनीक" की खोज के साथ पिकल प्रारूप द्वारा उत्पन्न सुरक्षा जोखिम एक बार फिर सामने आए हैं ।

ट्रेल ऑफ बिट्स के अनुसार, यह अटैक विधि, मशीन लर्निंग (एमएल) मॉडलों को पैकेज और वितरित करने के लिए प्रयुक्त सर्वव्यापी प्रारूप को हथियार बनाती है, जिससे मॉडल स्वयं क्रप्ट हो जाता है, तथा संगठन के अनुप्रवाह ग्राहकों के लिए आपूर्ति श्रृंखला में गंभीर जोखिम उत्पन्न होता है।

"स्लीपी पिकल एक गुप्त और नवीन अटैक तकनीक है जो अंतर्निहित प्रणाली के बजाय एमएल मॉडल को ही लक्ष्य बनाती है।

पिकल एक व्यापक रूप से प्रयोग होने वाली क्रमांकन प्रारूप है , जो एम् एल लाइब्रेरीज़ द्वारा उपयोग किया जाता है जैसे पाईटोर्च, इसका उपयोग केवल पिकल फ़ाइल लोड करके (अर्थात, अक्रमांकन के दौरान) स्वयंरचित कोड हमलों को निष्पादित करने के लिए किया जा सकता है।

स्लीपी पिकल, पिकल फाईल में पेलोड डालकर कर ओपन-सोर्स टूल का उपयोग करके काम करता है और फिर चार तकनीकों में से किसी एक का उपयोग करके इसे टारगेट होस्ट तक पहुंचाता है, जैसे कि एडवर्सरी-इन-द-मिडिल (एआईटीएम) अटैक, फ़िशिंग, आपूर्ति श्रृंखला से समझोता करके या सिस्टम की कमजोरी का फायदा उठाना।

सुझाव

- सिस्टम की नियमित सुरक्षा जांच करें।
- नियमित रूप से एक्सेस लॉग की निगरानी करें ।
- एंडपॉइंट के लिए एचटीटीपीएस(HTTPS) का उपयोग करें ।
- आकस्मिक प्रतिक्रिया योजनाएँ विकसित और अधतन करें।
- निरंतर सुरक्षा प्रशिक्षण प्रदान करें।
- सॉफ़्टवेयर पैच को नियमित रूप से अपडेट करें ।

सी) नया क्रेडिट कार्ड स्किमर वर्डप्रेस, मैगेंटो और ओपनकार्ट साइटों को लक्षित करता है।

वर्डप्रेस, मैगेंटो और ओपनकार्ट जैसे कई कंटेंट मैनेजमेंट सिस्टम (सीएमएस) प्लेटफॉर्म को सीज़र सिफर स्किमर नामक एक नए क्रेडिट कार्ड वेब स्किमर द्वारा निशाना बनाया जा रहा है ।

वेब स्किमर से तात्पर्य ऐसे मैलवेयर से है जिसे ई-कॉमर्स साइट्स में वित्तीय और भुगतान संबंधी जानकारी चुराने के उद्देश्य से डाला जाता है । नवीनतम अभियान में क्रेडिट कार्ड विवरण चुराने के लिए वर्डप्रेस वूकॉमर्स प्लगइन ("फॉर्म- चेकआउट. पीएचपी ") से जुड़े चेकआउट पीएचपी पेज में दुर्भावनापूर्ण संशोधन करना शामिल है।

गुगल एनालाईटिक्स और गुगल टैग मैनेजर के रूप में मैलवैयर के प्रयास को ध्यान में रखते हुए लंबे समय से अस्पष्ट स्क्रिप्ट की तुलना में इन्जेक्शन को कम संदिग्ध दिखने के लिए बदल दिया गया है । विशेष रूप से, यह सीजर सांकेतिक (साईफर) में नियोजित समान प्रतिस्थापन तंत्र का उपयोग करता है ताकि दुर्भावनापूर्ण कोड के मद को एक विकृत स्ट्रिंग में एनकोड किया जा सके और पेलोड को होस्ट करने के लिए उपयोग किए जाने वाले बाहरी डोमेन को छिपाया जा सके । यह माना जाता है कि सभी वेबसाइटों को पहले अन्य तरीकों से छेड़छाड़ की गई है ताकि एक पीएचपी स्क्रिप्ट को स्थान दिया जा सके जो "style.css" और " css.php " नामों से जाती है, जो एचटीएमएल स्टाइल शीट की नकल करने और पहचान से बचने के स्पष्ट प्रयास में है। बदले में, ये स्क्रिप्ट एक और अस्पष्ट जावास्क्रिप्ट कोड लोड करने के लिए डिज़ाइन की गई हैं जो एक वेबसॉकेट बनाता है और वास्तविक स्किमर को लाने के लिए दूसरे सर्वर से जुड़ता है । स्क्रिप्ट वर्तमान वेब पेजों का यूआरएल भेजती है, जो अटैकर्स को प्रत्येक संक्रमित साइट के लिए अनुकूलित प्रतिक्रियाएँ भेजने की अनुमति देता है। दूसरी स्तर की स्क्रिप्ट के कुछ संस्करण यह भी जाँचते हैं कि क्या इसे लॉग-इन वर्डप्रेस उपयोगकर्ता द्वारा लोड किया गया है और उनके लिए प्रतिक्रिया को संशोधित करते हैं।

फॉर्म- चैकआउट वूकॉमर्स पीएचपी फ़ाइल स्किमर को प्रसारित करने के लिए इस्तेमाल की जाने वाली एकमात्र विधि नहीं है, अटैकर्स को वेबसाइट डेटाबेस में इसे इंजेक्ट करने के लिए वैध डब्लूपी कोड प्लगइन का दुरुपयोग करते हुए भी देखा गया है । मैजेटों का उपयोग करने वाली वेबसाइटों पर, जावास्क्रिप्ट इंजेक्शन डेटाबेस टेबल जैसे कोर कनफिंग डाटा आदि पर किए जाते हैं । वर्तमान में यह ज्ञात नहीं है कि ओपर कार्ट साइटों पर यह कैसे संपादित किया जाता है । वेबसाइटों के लिए एक आधार के रूप में इसके व्यापक उपयोग के कारण, वर्डप्रेस और लार्ज प्लगइन पारिस्थितिकी तंत्र, मैलिसियस ऐक्टर के लिए एक आकर्षक लक्ष्य बन गया है, जिससे उन्हें एक विशाल अटैक की सतह तक आसानी से पहुँचा जा सकता है ।

यह जरूरी है कि साइट ऑनर अपने सीएमएस सॉफ्टवेयर और प्लगइन्स को अपडेट रखें, सकठिन /सुरक्षित पासवर्ड को लागू करें, तथा संदिग्ध एडमिनिस्ट्रेटर खातों की उपस्थिति के लिए समय-समय पर उनका ऑडिट करें ।

सुझाव

- सॉफ्टवेयर को नियमित रूप से अपडेट करें ।
- सुरक्षा प्लगइन्स का उपयोग करें ।
- मजबूत, अद्वितीय(युनिक) पासवर्ड का उपयोग करें और एडमिन एकाउंट के लिए दो-कारक प्रमाणीकरण (2एफए) सक्षम करें।
- किसी भी संदिग्ध गतिविधि के लिए सर्वर और एप्लिकेशन लॉग की नियमित समीक्षा करें ।
- प्रशासनिक पहुंच को केवल उन लोगों तक सीमित रखें जिनके आईपी पते ज्ञात है एवं जिन्हें इसकी आवश्यकता है ।
- सुनिश्चित करें कि आपकी साइट उपयोगकर्ता और आपकी वेबसाइट के बीच प्रेषित डेटा को एन्क्रिप्ट करने के लिए एचटीटीपीएस का उपयोग करती है ।
- अपनी वेबसाइट को मैलवेयर और भेदता (गोपनीयता) के लिए नियमित रूप से स्कैन करें ।

2.साईबर धोखाधड़ी

ए) एक बैंक मैनेजर ने ऑनलाइन साइबर धोखाधड़ी में 5.10 लाख रुपये गवा दिए, जब वह अपने कुछ घरेलू सामान बेचने की कोशिश कर रही थी ।

एक बैंक मैनेजर ने ऑनलाइन ठगी में साइबर धोखाधड़ी का शिकार होकर नागपुर में 5.10 लाख रुपये गंवाए जब वह अपने घर का कुछ सामान बेचने की कोशिश कर रही थी । 31 वर्षीय पीड़िता ने एक रेफ्रिजरेटर और सोफा का विवरण अपलोड किया था, जिसे वह बेचना चाहती थी । जैसे ही उसने विवरण भरा, उसे एक व्यक्ति का फोन आया जिसने कहा कि वह सामान खरीदना चाहता है।

आरोपी ने उसे शुरुआती लेनदेन सत्यापन के तौर पर 60 रुपये भेजने को कहा । ऐसा करने के बाद, उसने उसके खाते से 1.01 लाख रुपये निकाल लिए। इस राशि को वापस करने के नाम पर, उसने फिर से 9,000 रुपये का भुगतान किया और आरोपी ने कुल 5.10 लाख रुपये निकाल लिए । पुलिस के अनुसार, भारतीय दंड संहिता और सूचना

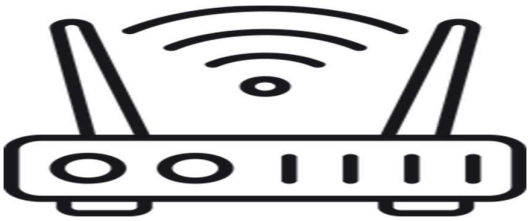
प्रौद्योगिकी अधिनियम के प्रावधानों के तहत मामला दर्ज किया गया है और अपराधी को पकड़ने के प्रयास जारी हैं ।

बी) वरिष्ठ नागरिक ने परिष्कृत वॉयस क्लोनिंग घोटाले में 3 लाख रुपये गंवाए।

एक 63 वर्षीय व्यक्ति एक परिष्कृत साइबर घोटाले का शिकार हो गया, जिसमें उसे 3 लाख रुपये की हानि हुई । जालसाज ने उनके बेटे का दोस्त बनकर फोन पर बेटे के दोस्त की आवाज की नकल करके उन्हें ठगा । बुजुर्ग व्यक्ति, जिनके बच्चे विदेश में रहते हैं, वे उस समय ठगे गए जब उन्हें एक अज्ञात नंबर से व्हाट्सएप के जरिए कॉल आया। फोन करने वाले ने बेटे के दोस्त की आवाज की नकल की, जिसे पीड़ित बचपन से जानता था, उसने तत्काल वित्तीय मदद की गुहार लगाई । कॉलर की जानी-पहचानी आवाज पर भरोसा करके पीड़ित ने दिए गए खाते में 2 लाख रुपये ट्रांसफर कर दिए और अपने दो दोस्तों को 50-50 हजार रुपये का योगदान करने के लिए राजी कर लिया। हालांकि, संदेह तब पैदा हुआ जब कॉलर ने और पैसे की मांग की और बाद में जालसाज को वीडियो कॉल करने के प्रयास असफल रहे । ठगी का एहसास होने पर पीड़ित को पता चला कि सगे बेटे के दोस्त ने ऐसी कोई कॉल नहीं की थी। पुलिस ने मामला दर्ज कर लिया है और आगे की जांच कर रही है।

3. इस माह की टिप

ब्रॉडबैंड सुरक्षा.



ब्रॉडबैंड इंटरनेट कनेक्शन हमेशा ऑन रहना और डिफ़ॉल्ट कॉन्फ़िगरेशन अत्यंत असुरक्षित है।

ब्रॉडबैंड इंटरनेट के लिए क्या करें

1. **डिफ़ॉल्ट एसएसआईडी (सर्विस सेट पहचानकर्ता) बदलें** : इसका दुरुपयोग अटैकर द्वारा नेटवर्क/कम्प्यूटर में सेंध लगाने के लिए किया जा सकता है।

2. **वायरलेस सुरक्षा सक्षम करें** : मॉडेम राउटर वायरलेस सुरक्षा का स्पोर्ट करते हैं। उपयोगकर्ता किसी एक प्रोटोकॉल और सुरक्षा कुंजी का चयन कर सकता है । कंप्यूटर में वही वायरलेस सुरक्षा प्रोटोकॉल और सुरक्षा कुंजी सक्षम होनी चाहिए।

3. **डिवाइस को स्टेटिक आईपी एड्रेस असाइन करें** : ज़्यादातर होम यूज़र्स को डायनेमिक आईपी एड्रेस आवंटित किए जाते हैं, क्योंकि डीएचसीपी तकनीक से सेटअप करना आसान है। राउटर या एक्सेस पॉइंट में डीएचसीपी ऑप्शन को बंद करें और फिक्स्ड आईपी एड्रेस रेंज का इस्तेमाल करें ।

4. फर्मवेयर (ड्राइवर कोड) को नियमित रूप से अपडेट करें ।

5. ब्रॉडबैंड ड्राइवर हमेशा निर्माता द्वारा अनुशंसित वैध वेबसाइटों से ही डाउनलोड करें।

6. उपयोगकर्ता का नाम और डिफ़ॉल्ट एडमिनिस्ट्रेटर पासवर्ड को बदलें।

7. **मैक एड्रेस फ़िल्टरिंग सक्षम करें** : हर डिवाइस का एक युनिक मैक एड्रेस होता है। डिवाइस तक सीमित पहुँच के लिए ब्रॉडबैंड एक्सेस पॉइंट को उपकरण के मैक एड्रेस के साथ जोड़ा जा सकता है।

8. **संगत डब्लूपीए /वेप एन्क्रिप्शन ऑन करें** : सभी वाई-फाई सक्षम मॉडेम / राउटर एन्क्रिप्शन तकनीक के कुछ रूप का समर्थन करते हैं, जिसे सक्षम करना होगा।

9. कंप्यूटर/लैपटॉप को ब्रॉडबैंड इंटरनेट सुरक्षा खतरों से बचाने के लिए प्रभावी एंड पॉइंट सुरक्षा समाधान (एंटी-वायरस, एंटी-स्पाइवेयर, डेस्कटॉप फ़ायरवॉल आदि) का उपयोग करें।

10. मॉडेम राउटर के साथ-साथ कंप्यूटर पर फ़ायरवॉल को सक्षम करें।

ब्रॉडबैंड इंटरनेट के लिए क्या न करें

1. जब ब्रॉडबैंड कनेक्टिविटी का उपयोग न हो तो उसे खुला न छोड़ें ।

2. असुरक्षित कंप्यूटर/लैपटॉप के साथ यूएसबी ब्रॉडबैंड मॉडेम का उपयोग न करें।

3. प्रत्येक ब्रॉडबैंड इंटरनेट लाइन के लिए बिना फिल्टर वाले कनेक्शन का उपयोग न करें।

4. रिमोट एक्सेस/एडमिनिस्ट्रेशन (इंटरनेट के माध्यम से) के विकल्प को सक्षम न करें, क्योंकि घरेलू उपयोगकर्ता के लिए यह आवश्यक नहीं है।

5. वाई-फाई नेटवर्क खोलने के लिए ऑटो-कनेक्ट को सक्षम न करें।

6. वाई-फाई के मामले में कभी भी अज्ञात या अविश्वसनीय नेटवर्क से कनेक्ट ना करें ।


केन्द्रीय रिजर्व पुलिस बल
शैक्षणिक उत्कृष्टता अलंकरण समारोह


CWA RAISING DAY-2024


29th CWA RAISING DAY
सार्थक सहयोग सर्वदा
CENTRAL RESERVE POLICE FORCE