केन्द्रीय रिजर्व पुलिस बल

साइबर बाइट

- स्टीलिंग मैलवेयर
- एसओजीयू या प्लगएक्स मैलवेयर परिवार

साइबर बाइट
मार्च -2024
संस्करण

साइबर धोखाधडी
अपडेट

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

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

संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ

1.साइबर गीक समाचार

ए) स्टीलिंग मैलवेयर

(i) रेडलाइन (ii) रैकून iii)विडार

i) रेडलाइनः- एक अपेक्षाकृत नये प्रकार का मैलवेयर रेडलाइन स्टीलर ने सुरक्षा उत्साहियों को सतर्क कर दिया है। यह कपटपूर्ण है और विभिन्न सुरक्षा उपकरणों से पता लगाना कठिन है। रेडलाइन स्टीलर एक दुर्भावनापूर्ण जानकारी चुराने वाला एक सॉफ्टवेयर है जो वेब ब्राउजर, एप्लिकेशन, ई-मेलिंग और मैसिजिंग ऐप्स और क्रिप्टोकरेंसी वैलेट से से पीड़ित का डेटा एकत्र करने के लिए अनुकूलन योग्य फाइल ग्रेबर का उपयोग करता है। यह मैलवेयर संक्रमित डिवाइस के बारे में विस्तृत जानकारी इकट्ठा कर सकता है, जैसे कि उसका प्रोग्राम, एंटीवायरस उत्पाद और रनिंग प्रोसेस और रैंसोमवेयर अटैक को सुपरिष्कृत कर आगे बढ़ाता है।

संक्षेप में रेडलाइन स्टीलर एक रिमोट एक्सेस ट्रोजन के रूप में काम करता है जो डेटा को बाहर निकालता है और यूजर्स की संवेदनशील जारकारी को हैकर्स को ट्रांसफर करता है जो इसे बाद में डार्कवेब पटल पर बेचते है। थ्रेट एक्टर्स रेडलाइन स्टीलर का आसानी से उपयोग कर सकते है क्योंकि यह मैलवेयर मैस ए सर्विस (एमएएएस) मॉडल पर कार्य करता है।

रेडलाइन स्टीलर कम्प्यूटर को कैसे संक्रमित करता है?

रेडलाइन स्टीलर पीड़ित के डिवाइस को कई प्रकार से संक्रमित कर सकता है। रेडलाइन स्टीलर को वितरित करने के लिए थ्रेट एक्टर द्वारा उपयोग की जाने वाली सबसे आम विधियां, जिसमें शामिल हैः-

फिशिंग ई-मेलः- हैकर्स द्वारा सोशल इंजीनियरिंग स्कीम के द्वारा डिवाइस को संक्रमित करना एक पंसदीदा तकनीक है और रेडलाइन स्टीलर कोई अपवाद नहीं है। साइबर अपराधी फिशिंग ई-मेल का उपयोग कर एक बार में दुर्भावनापूर्ण अटैचमेंट या लिंक को बहुत ज्यादा प्राप्तकर्ताओं को भेज सकते है।

कोम्प्रोमाइज्ड वेबसाइटसः- वेब यूजर को समझौता किए गए वेबसाइट पर दुर्भावनापूर्ण विज्ञापन के माध्यम से भेजा जा सकता है या जब हैकर्स प्रसिद्ध वेबसाइटों के जानबूझकर गलत वर्तनी वाले नामों के साथ डोमेन का प्रयोग करते है। एक आधिकारिक वेबसाइट से वैध दिखने वाले साफ्टवेयर को डाउनलोड करने के बजाय रेडलाइन स्टीलर प्राप्त होता है इसके लिए सिर्फ एक संक्रमित वेबसाइट पर जाने की आवश्यकता होती है।

वैध दिखने वाली ऐप्लिकेशनः- ट्रोजन होने के नाते, रेडलाइन स्टीलर मैलवेयर खुद को सॉफ्टवेयर प्रोग्राम के वैध दिखने वाले ऐप के रूप में छिपा सकता है जो वास्तव में क्रेक हो गया है और मैलवेयर को छुपाता है। सबसे विचित्र मामलों में, पीड़ित यह सोचकर मैलवेयर डाउनलोड कर सकते है कि वे अपने डिवाइस के लिए नया एंटीवायरस सॉफ्टवेयर डाउनलोड कर रहे है या अपने ऑपरेटिंग सिस्टम को अपडेट कर रहे है।

ii) रैकूनः- रैकून मेलवेयर बुनियादी जानकारी चुराने वाला है जो रेडलाइन की तरह कार्य करता है और यह स्वयं में किसी भी प्रकार की एंटीवायर सुरक्षा से रहित होता है। ऐसे कोई भी फंक्शन नहीं है जो मैलवेयर के विश्लेषण को जटिल बना दे। हालांकि रैकून डवलपर्स तीसरे पक्ष के क्रिप्टर (एक प्रकार का मैलवेयर) का उपयोग करने का सुझाव देता है।

जब मुख्य कार्यक्षमता की बात आती है तो यह हमलावल द्वार सक्षम किए गए कॉन्फिगरेशन के आधार पर सिस्टम सेटिंग्स की जांच कर सकता है, स्क्रीनशॉट कैप्चर कर सकता है, सामान्य जानकारी जैसे ओएस संस्करण, आईपी और उपयोगकर्ता नाम को संग्रह कर सकता है, पासवर्ड और लॉगिन को विभिन्न ब्राउजरों से चुरा सकते है। इसके अलावा चोरी करने वाला (ट्रोजन) माइक्रोसॉफ्ट आउटलुक से जानकारी पुनः प्राप्त कर सकता है और साथ ही क्रिप्टोकरेंसी वॉलेट भी चुरा सकता है। डेटा संग्रह प्रक्रिया समाप्त होने पर डेटा को जिप संग्रह में पैक किया जाता है और फिर इसे अटैकर के सर्वर पर भेजा जाता है।

iii) विडारः- विडार एक प्रकार का जानकारी चुराने वाला मैलवेयर है जो विशेषत व्यक्तिगत और वित्तीय संवेदनशील जानकारी संक्रमित सिस्टम से चुराने के लिए डिजाइन किया गया है। विडार मैलवेयर आमतौर पर ई-मेल के माध्यम से वितरित किया जाता है, हाल ही में आईएसओ फाइल के रूप में, कई अभियानों में जो एक डिस्क छवि फाइल प्रारूप है, जिसका उपयोग आमतौर पर मैलवेयर बनाने वालों द्वारा मैलवेयर को पैकेज करने के लिए उपयोग किया जाता है। विडार के मामले में दुर्भावनापूर्ण आईएसओ को एडोब फोटोशॉप और माइक्रोसॉफ्ट टीम्स जैसे वैध साफ्टवेयर के लिए नकली इंस्टॉलरों में एम्बेड किया गया है जो फॉलआउट एक्सपलोइट हिट के माध्यम से दिया गया है और फिशिंग ई-मेल के अनुलग्नक के रूप में भेजा गया है।

विडार एक जानकारी चुराने वाला है और अपने कमांड और कंट्रोल (सी2) बुनियादी ढ़ाचे के हिस्से के रूप में अक्सर सोशल मीडिया का उपयोग करता है। सी2 इन्फ्रास्ट्रक्चर का आई.पी. एड्रेस पता मास्टोडन या ट्विटर प्लेटफार्म पर उपयोगकर्ता प्रोफाइल में एम्बेड किया जाएगा। मैलवेयर इस प्रोफाइल तक पहुंच सकता है, संकेतित आईपी पते से संपर्क कर सकता है और कॉन्फिगरेशन फाइलें, निर्देश और अतिरिक्त मैलवेयर डाउनलोड कर

सकता है।

थ्रेट विडार मुख्य रूप से एक जानकारी चुराने वाला है जिसका अर्थ है कि इसे एक संक्रमित कंप्यूटर से बडी मात्रा में जानकारी एकत्र करने और इसे डेटा को एक हमलावार तक पहुंचाने के लिए डिजाइन किया गया है। जानकारी के कुछ उदाहरण जो विडार संक्रमित कम्प्यूटर ब्राउजर और डिजिटल वॉलेट से एकत्र करता है इसमें निम्नलिखित शामिल हैः- ओएस डेटा, खाता क्रेडेंशियल, क्रेडिट कार्ड डाटा, ब्राउजर इतिहास।

सुझावः-

- **सॉफ्टवेयर को अपडेट रखें :-** संभावित खतरों से बचने के लिए नियमित रूप से अपने ऑपरेटिंग सिस्टम, एंटीवायरस सॉफ्टवेयर और सभी ऐप्लिकेशन को अपडेट करें।
- **प्रतिष्ठित सुरक्षा सॉफ्टवेयर का उपयोग करें :-** संभावित खतरों का पता लगाने और रोकने के लिए प्रतिष्ठित एंटीवायरस और एंटीमैलवेयर साफ्टवेयर इंस्टाल करें।
- **ई-मेल के साथ सावधानी बरतें :-** अज्ञात और संदिग्ध स्त्रोतों से प्राप्त ई-मेल अटैचमेंट को खोलने और क्लिक करने से बचें। फिशिंग प्रयासों से सतर्क रहें।
- **मजबूत पासवर्ड और मल्टी फैक्टर प्रमाणीकरण (एमएफए) :-** जटिल पासवर्ड का उपयोग करें और जहां तक संभव हो अकाउंट की सुरक्षा बढ़ाने के लिए एमएफए सक्षम करें।
- **नियमित बैकअपः-** अपने महत्वपूर्ण डेटा का नियमित बैकअप रखें और यह सुनिश्चित करें कि वह सुरक्षित रूप से भंडारित कर लिया गया है। यह रैंसमवेयर जैसे संभावित हमलों से बचने में सहायता करेगा।
- **नेटवर्क सुरक्षा उपायः-** अपने नेटवर्क को सुरक्षित रखने में सहायता के लिए फायरवॉल और घुसपैठ का पता लगाने/रोकथाम संबंधी प्रणाली को कॉन्फिगर करें।
- **नेटवर्क विभाजनः-** अपने नेटवर्क में मैलवेयर के संभावित प्रसार को सीमित करने के लिए नेटवर्क विभाजन लागू करें।
- **सिस्टम गतिविधि की निगरानी करें:-**किसी भी असामान्य या संदिग्ध गतिविधियों को रोकने के लिए सिस्टम लॉग और नेटवर्क ट्रैफिक की नियमित निगरानी करें।
- **जानकारियों से अद्यतन रहें :-** संभावित खतरों और जोखिमों से सूचित रहने के लिए नवीनतम साइबर सुरक्षा समाचार और सलाह से अपडेट रहें।

बी) एसओजीयू या प्लगएक्स मैलवेयर श्रेणीः-

एसओजीयू या प्लगएक्स एक प्रकार का मैलवेयर है जो उन्नत और परिष्कृत क्षमताओं के लिए जाना जाता है। प्लगएक्स मूल नाम है जबकि एसओजीयू इस मैलवेयर के उपनाम के लिए प्रायः प्रयोग किया जाता है। यहां एसओजीयू/प्लगएक्स से संबंद्ध मुख्य विशेषताएं दी गई हैः-

रिमोट एक्सेस ट्रोजन (आरएटी) :- एसओजीयू/प्लगएक्स एक रिमोट एक्सेस ट्रोजन या आरएटी है जिसका तात्पर्य है कि यह हमलावरों को संक्रमित सिस्टम का अनाधिकृत रिमोट एक्सेस प्रदान करने के लिए डिजाइन किया गया है।

जासूसी और लक्षित हमले :- एसओजीयू/प्लगएक्स अक्सर लक्षित साइबर जासूसी अभियानों से जुड़ा होता है। इसका उपयोग उन्नत लगातार खतरे (एपीटी) समूहों द्वारा सरकारी संगठनों, सैन्य संस्थानों और नाजुक आधारभूत संरचना सहित विशिष्ट लक्ष्यों से जोखिम में डालने के लिए किया गया है।

मॉडयूलर डिजाइनः- एसओजीयू/प्लगएक्स एक मॉडयूलर आर्किटेक्चर है जो हमलावरों को उनके उद्देश्य के आधार पर इसकी कार्यक्षमता को अनुकूलित करने की अनुमति देता है। यह मॉडयूलर डिजाइन इसे अनुकूलनीय बनाता है और बदलते सुरक्षा उपायों के जवाब में मैलवेयर को विकसित करने में सक्षम बनाता है।

कमांड और कंट्रोल (सी2) सर्वर – मैलवेयर हमलावरों द्वारा संचालित कमांड और कंट्रोल सर्वर के साथ संचार स्थापित करता है। इस संचार चैनल का उपयोग संक्रमित सिस्टम में निर्देश भेजने और संवेदनशील डेटा की चोरी करने के लिए किया जाता है।

नियंत्रणः- एसओजीयू/प्लगएक्स अक्सर संक्रमित सिस्टमों पर नियंत्रण बनाए रखने के लिए विभिन्न तकनीकों का उपयोग करता है। इसमें एंटरिज, शेडयूल किए गए कार्य या अन्य तंत्र बनाना शामिल हो सकता है जो सिस्टम रीबूट के बाद भी मैलवेयर सक्रिय रहता है।

अंतरविश्लेषण तकनीकः- सुरक्षा शोधकर्ताओं द्वारा पता लगाने और विश्लेषण से बचने के लिए एसओजीयू/प्लगएक्स में अंतरविश्लेषण तकनीकें शामिल की गई है। इसमें कोड अस्पष्टता, एन्क्रिप्शन और बहुरूपी तत्व शामिल हो सकते है जिससे इसके व्यवहार को पहचानना और समझना अधिक कठिन हो जाता है।

डिलीवरी के तरीकेः- मैलवेयर आम तौर पर दुर्भावनापूर्ण अनुलग्नकों या लिंक वाले स्पीयर फिशिंग ई-मेल के माध्यम से वितरित किया जाता है। एक बार जब उपयोगकर्ता दुर्भावनापूर्ण सामग्री के साथ इंटरैक्ट करता है तो मैलवेयर लक्ष्य किए गए सिस्टम पर निष्पादित होता है।

सूचना चोरी:- सओजीयू/प्लगएक्स संक्रमित सिस्टम से संवेदनशील जानकारी चुराने में सक्षम है। इसमें लॉग-इन जानकारी, आंतरिक विशेषताएं और अन्य गोपनीय डेटा शामिल हो सकते है।

सुझाव:-

- सिस्टम, ऐप्लिकेश और सॉफ्टवेयर के नवीनतम संस्करण में अपडेट करें और नवीनतम सुरक्षा पैच डाउनलोड करें।
- एंटीवायरस/एंटी मैलवेयर सॉफ्टवेयर इंस्टाल करे और सॉफ्टवेयर (और इसकी डेफिनेशन फाइलों) को अपडेट करें।
- सिस्टम और नेटवर्क का नियमित रूप से स्कैन करें और सभी प्राप्त फाइलों को स्कैन करें।
- जटिल पासवर्ड और प्रमाणीकरण के मजबूत तरीकों का उपयोग करें।
- अविश्वसनीय स्रोतों के लिंक पर क्लिक करते समय सावधान रहें।
- उन पाप-अप विंडो पर भरोसा न करें जो आपसे सॉफ्टवेयर डाउनलोड करने के लिए कहते है।
- सभी उपयोगकर्ता खातों की नियमित निगरानी करें और निष्क्रिय खातों को अक्षम करें।
- सभी उपयोगकर्ता खातों के पासवर्ड अपडेट करें जिनसे जानकारी लीक हो सकती है।

2. साइबर धोखाधड़ी :-

ऑनलाइन ट्रेडिंग स्कैम :- गुरुग्राम का डॉक्टर बना शिकार, गंवाएँ 2.5 करोड़ रूपये।

ऑनलाइन ट्रेडिंग स्कैम देशभर में बढ़ती चिंता का विषय बनते जा रहे है। पिछले कुछ हफ्तों में दर्सो लोग इसका शिकार हुए और लाखों गंवाएँ। अभी हाल ही में गुरुग्राम का एक डॉक्टर साइबर स्कैम का शिकार हो गया, जिसमें उसने अज्ञात साइबर अपराधियों से 2.5 करोड़ रूपये गंवाएँ। दि ट्रिब्युन में छपे एक मामले के अनुसार, केन्द्रीय विहार सोशायटी, सेक्टर-56 के निवासी पीड़ित ने 4 जनवरी 2024 को इंटरनेट पर एक आकर्षक विज्ञापन देखा। विज्ञापन में एक स्टॉक मार्केटिंग निवेश योजना की पेशकश की गई थी जिसमें ऑनलाइन स्टॉक और आरंभिक सावर्जनिक पेशकश (आईपीओ) के माध्यम से महत्वपूर्ण लाभ का वायदा किया गया था। आसान लाभ के स्त्रोत से आकर्षित होकर पीड़ित ने विज्ञापन में दिए गए नंबर पर संपर्क किया। पूछताछ के बाद कॉल करने वाले द्वारा उसे व्हाट्सएप के माध्यम से एक लिंक भेजा गया जिसके माध्यम से उसे एक शेयर खरीदने वाला ऐप डाउनलोड करने को कहा गया जो पीड़ित को वैध लगा। ऐप की कार्यात्मकता पर भरोसा करते हुए पीड़ित ने निवेश करना शुरू कर दिया, शुरूआत में शेयर खरीदने के लिए रूपये 50000/- का निवेश किया गया। जब शुरूआती निवेश में उसे लाभ मिलता दिखाई दिया तो पीड़ित को जल्द ही आईपीओ में भाग लेने के लिए राजी कर लिया गया। ऐप ने धोखे से उनके खाते का बैलेंस बढ़ा दिया जिसमें 3.19 करोड़ रूपये का पर्याप्त लाभ दिखाया गया। हाँलांकि जब उसने अपना मुनाफा वापस लेने का प्रयास किया तो उसे निकासी के लिए मना कर दिया गया। अपने फंड तक पहुंचने में असमर्थ पीड़ित ने स्कैमर्स से संपर्क किया तो उसके साथ और धोखाधड़ी की गई। उन्होंने उसे निकासी प्रक्रिया को सुविधाजनक बनाने के लिए सुरक्षा जमा की आड़ में अतिरिक्त पैसा जमा करने के लिए मना लिया। उनकी विस्तृत योजना का शिकार होकर पीड़ित ने कई लेन-देन में कुल 1.36 करोड़ रूपये स्थानांतरित किए। दुर्भाग्यवश, डॉक्टर से बडी रकम सफलतापूर्वक ठगने के बाद स्कैमर्स गायब हो गए। पीड़ित ने सभी उपलब्ध प्रणाली के माध्यम से उनसे संपर्क करने की कोशिश की। सभी उपलब्ध प्रणाली के माध्यम से उसने प्रयास किया परंतु धन पुनर्पाप्ति के सभी प्रयास असफल रहने के पश्चात पीड़ित ने आखिरकार पुलिस से संपर्क किया और औपचारिक शिकायत दर्ज की।

3. महीने की टिप

एंड्रायड सुरक्षा।

डिवाइस सुरक्षा:-

सॉफ़्टवेयर अपडेट रखें:- सुरक्षा संबंधी कठिनाईयों से बचने के लिए अपने एंड्रायड ऑपरेटिंग सिस्टम और ऐप्स को नियमित रूप से अपडेट करें।

मजबूत लॉक स्क्रीन का उपयोग करें :- अनाधिकृत एक्सेस के विरूद्ध सुरक्षा के लिए सुरक्षित लॉक स्क्रीन पद्धति जैसे कि पिन, पासवर्ड या पैटर्न का उपयोग करें।

फाइंड मॉय डिवाइस सक्षम करें :- फाइंड मॉय डिवाइस फीचर सक्षम करें ताकि आवश्यकता पड़ने पर अपनी डिवाइस को दूर से ढूंढ सके, लॉक या वाइप कर सकें।

डिवाइस का कोडीकरण: – अपने डेटा को सुरक्षित रखने के लिए डिवाइस कोडीकरण सक्षम करें यदि किसी स्थिति में आपका उपकरण किसी गलत हाथों में पड जाता है।

बायोमैट्रिक प्रमाणीकरण :- यदि उपलब्ध है तो, एक अतिरिक्त सुरक्षा परत के लिए फिंगरप्रिंट या चेहरे की पहचान वाले फीचर सक्षम करें।

ऐप सुरक्षाः-

विश्वसनीय स्रोतों से ऐप्स डाउनलोड करें :- मैलवेयर से बचने के लिए गूगल प्ले स्टोर जैसे प्रतिष्ठित ऐप से ही ऐप्स इंस्टाल करें।

ऐप्स ऑटो अपडेट की समीक्षा करें :- ऐप्स को इंस्टाल करने से पहले ऐप्स द्वारा अनुरोध की अनुमतियों को चैक करें और समझें।

ऐप स्वअद्यतनः- स्वचलित ऐप्स अपडेट को सक्षम करें तथा सुनिश्चित करें कि आपके पास नवीनतम सुरक्षा पैच है।

सुरक्षा ऐप्स का उपयोग करें :- मैलवेयर के विरूद्ध सुरक्षा एवं स्कैन हेतु विश्वसनीय एंटीवायरस या सुरक्षा ऐप इंस्टाल करें।

ऐप अनुमति ऑडिटः- निजता को बढ़ाने के लिए पाक्षिक समीक्षा करें और अनावश्यक ऐप्स अनुमतियों को हटाये।

नेटवर्क और कनेक्टिविटीः-

सुरक्षित वाई-फाई का उपयोग करें :- खुले या असुरिक्षित वाई-फाई नेटवर्क से कनेक्ट करने से बचें, अतिरिक्त सुरक्षा के लिए वीपीएन का उपयोग करें।

ब्लूटूथ सुरक्षाः- अप्राधिकृत एक्सेस से रोकथाम के लिए ब्लूटूथ को अक्षम करें जब वह प्रयोग में न हो।

गूगल खाता सुरक्षाः- दो फैक्टर प्रमाणीकरण सक्षम करें। दो फैक्टर प्रमाणीकरण के साथ अपने गूगल खाता में सुरक्षा की एक अतिरिक्त परत जोडें।

पासवर्ड नियमित रूप से अपडेट करें :- सुरक्षा में बढ़ोत्तरी हेतु अपने गूगल खाता पासवर्ड को नियमित रूप से बदलें।

गूगल खाता गतिविधियों की समीक्षा करें :- किसी भी अप्राधिकृत एक्सेस से बचाव के लिए अपने खाता गतिविधियों की पाक्षिक जांच करें।

डाटा सुरक्षाः-

डिवाइस बैकअपः- महत्वपूर्ण डेटा को सुरक्षित रखने के लिए नियमित रूप से अपने डिवाइस का बैकअप रखें।

सुरक्षित क्लाउड स्टोरेजः- यदि क्लाउड सेवाओं का उपयोग कर रहे है तो दो फेक्टर प्रमाणीकरण सक्षम करें और संवेदशील फाइलों का कोडीकरण करें।

सुरक्षित ब्राउजिंगः –

सुरक्षित ब्राउजर का उपयोग करें :- एक विश्वसनीय ब्राउजर चुनें और नवीनतम सुरक्षा फिचर के लिए इसे अद्यतन रखें।

लिंक से सजग रहें :- फिशिंग से रोकथाम के लिए ई-मेल या संदेश में संदिग्ध लिंक पर क्लिक न करें।

सामान्य सुरक्षा अभ्यासः-

स्वयं को शिक्षित करें :- नवीनतम सुरक्षा खतरों और सर्वोत्तम प्रथाओं के बारे में सूचित रहें।

अपनी डिवाइस को रूट करने से बचें :- अपने डिवाइस को रूट करने से यह सुरक्षा जोखिम में पड़ सकता है, जब तक आवश्यक न हो तक इससे बचें।

मैलवेयर के लिए नियमित जांच करें :- मैलवेयर को नियमित रूप से स्कैन करने के लिए सुरक्षा ऐप्स का उपयोग करें।

अज्ञात स्रोतों को अक्षम करें :- अपने डिवाइस सेटिंग्स में अज्ञात स्रोतों से ऐप्स इंस्टाल करने को बंद करें।

निजता नियंत्रणः-

लोकेशन सेटिंग्स का प्रबंधनः- निजता में वृद्धि करने के लिए अपनी लोकेशन को ऐप्स में सीमित करें।

व्यक्तिगत डेटा साझा करने पर नियंत्रणः- सोशल मीडिया और अन्य प्लेटफार्म पर जो जानकारी आप साझा करते है, से सावधान रहें।

संचार सुरक्षाः-

कोडीकृत मैसेजिंग ऐप्स को उपयोग करें :- उन मैसेजिंग ऐप्स का चुनाव करें जो सुरक्षित संचार के लिए एंड टू एंड कोडीकरण उपलब्ध कराते है।

सुरक्षित ई-मेल खातेः- ई-मेल खातों के लिए मजबूत पासवर्ड का उपयोग करें और दो फैक्टर प्रमाणीकरण को सक्षम करने पर विचार करें।

भौतिक सुरक्षाः-

सार्वजनिक स्थानों में सचेत रहें :- अनाधिकृत उपयोग की रोकथाम के लिए सार्वजनिक स्थानों पर संवेदनशील जानकारी प्रदर्शित करने से बचें।

स्क्रीन सुरक्षा का उपयोग करें :- भीड-भाड वाले स्थानों पर अपनी स्क्रीन को दूसरों की ताक झांक से बचाएं।

अनुमति संबंधी बदलाव पर नजर रखें :- ऐप्स अनुमति में किसी भी प्रकार के अवांछित बदलाव से सतर्क रहें और यदि आवश्यक हो तो इसकी जांच करें।

केस का अध्ययनः-

मामले का विवरणः- PE filevarbaytsa.exe और ragihaca.exe का मैलवेयर विश्लेषण।

1. filevarbayrsa.exe का सारांश

CRIMSON आरएटी फैमिली का varbaytsa.exe (4MB) (vdhrh madtvin.exe) मैलवेयर के विश्लेषण से पता चलता है कि दिया गया मैलवेयर एक कीलॉगर है और क्रिमसोन आरएटी फैमिली का एक संस्करण है। दिया गया मैलवेयर दिनांक 14-06-2023 (12:57:19) को बनाया गया उच्च परिष्कृत मैलवेयर है जो मेटाडेटा (rebook vkolge.exe) के साथ माइक्रोसॉफ्ट.नेट में

बनाया गया है। मैलवेयर विभिन्न हिस्सों और बाहरी ड्राइव से नेटवर्क जानकारी, फाइल, डायरेक्टरी लिस्टिंग को पढ़ता है। यह मैलवेयर की-स्ट्रोक और क्लिपबोर्ड डेटा को वेरबेसटा फाइल में सहेजता है। मैलवेयर पॉवरशेल स्क्रिप्टस का उपयोग करके निष्पदान करता है।

इसमें एंटी डिबग कोड, एंटी वीएम कोड और एंटीवायरस इवेशन कोड जैसे अधिक स्लीप टाइम तक खुद को सुरक्षा उपायों से छुप सकने वाले शामिल है। यह 5.189.132.99 (कॉन्टेबे जीएमएसएच, जर्मनी), 82.146.34137 (रूस) से संचार कर रहा है। हमलावर कोबाल्ट स्ट्राइक एडवर्सरी सिमुलेशन टूल का उपयोग समझौता किए सिस्टम को पैलोड भेजने में कर रहा है।

2. ragihaca.exe का सारांश

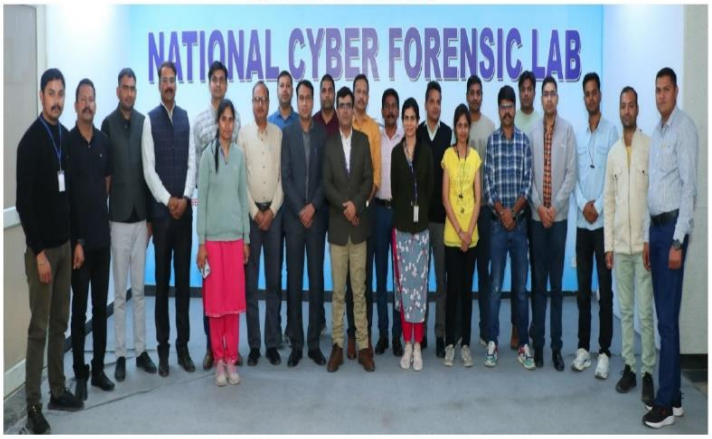
ragihaca.exe मैलवेयर के विश्लेषण से पता चलता है कि दिए गए मैलवेयर में उपयोगकर्ता को गुमराह करने के लिए एक नकली व्हाट्सएप आइकन है। दिया गया मैलवेयर एक ट्रोजन/बैकडोर है जो दिनांक 14-06-2023 (12:57:19) को बनाया गया उच्च परिष्कृत मैलवेयर है जो मेटाडेटा (rebook vkolge.exe) के साथ माइक्रोसॉफ्ट.नेट में बनाया गया है। मैलवेयर विभिन्न हिस्सों और बाहरी ड्राइव से नेटवर्क जानकारी, फाइल, डायरेक्टरी लिस्टिंग को पढ़ता है। यह प्रतीत होता है कि सीएनसी संचार के बाद मैलवेयर नकली पीडीएफ, पीपीटी फाइल (ब्लॉस्टॉम इंक फाइल में लिस्ट की गई) डाउनलोड करता है। मैलवेयर पॉवरशेल स्क्रिप्टस का उपयोग करके निष्पदान करता है।

दिया गया मैलवेयर एंटी डिबग कोड, एंटी वीएम कोड और एंटीवायरस इवेशन कोड जैसे अधिक स्लीप टाइम तक खुद को सुरक्षा उपायों से छुप सकने वाले शामिल है। यह 5.189.132.99 (कॉन्टेबे जीएमएसएच, जर्मनी), 82.146.34137 (रूस) से संचार कर रहा है। हमलावर कोबाल्ट स्ट्राइक एडवर्सरी सिमुलेशन टूल का उपयोग समझौता किए सिस्टम को पैलोड भेजने में कर रहा है।बिंदु है जिनका उपयोग स्कैमर विश्वास बनाने के लिए करते है।

NATIONAL CYBER FORENSIC LAB

ADVANCE COURSE IN CYBER FORENSIC INVESTIGATION TRAINING PROGRAMME

19.02.2024 TO 23.02.2024



SITTING CHAIR: SH. VIJAY GAHLAWAT (ACP/TRAINING-IFSO/NCFL) (M).

STANDING ROW (L TO R): CONST. VIJAY MISHRA (MADHYA PRADESH), INSPR. RAMESH C (KERALA), PROGRAMMER SURESH KUMAR (RAJASTHAN), HC JITENDRA SHARMA (RAJASTHAN), ANKIT KAUSHIK (CRPF), CONST. REENA YADAV (DELHI POLICE), INSPR. BIRENDER (CRPF), SI RAHUL SONKAR (UTTAR PRADESH), INSPR. RANDHIR KUMAR (CRPF), SI ANOOP YADAV (UTTAR PRADESH), INSPR. RAJESH R (KERALA), INSPR. SIVA KUMAR V (KERALA), SAPNA YADAV (DELHI POLICE), ASI SURJEET SINGH (CRPF), SI PRIYANKA AGRAWAL (MADHYA PRADESH), HC PRABHAT KUMAR JHA (CRPF), SI ANIL DAWAR (MADHYA PRADESH), SI VIPIN DAHERIYA (MADHYA PRADESH), SI SHAILENDRA RATHOR (MADHYA PRADESH), CONST. VIVEK PRATAP SINGH (MADHYA PRADESH), CONST. MANISH DAWDA (MADHYA PRADESH), HC SANJAY SHARMA (MADHYA PRADESH).