केन्द्रीय रिजर्व पुलिस बल

साइबर बाइट

- एनपीएम ट्रोजन यूएसी को बायपास करता है, ऑसकंपेटिबल पैकेज के साथ एनीडेस्क इंस्टाल करता है।
- यूट्यूब चैनल का उपयोग कर लुम्मा स्टीलर को वितरित करने वाला थ्रेट ग्रुप।

साइबर बाइट
फरवरी -2024
संस्करण

साइबर धोखाधडी अपडेट

सुरक्षित सोशल मीडिया अकाउंट

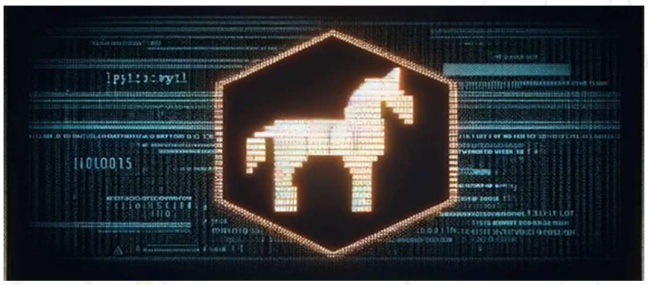
ऑनलाइन वितीय धोखाधड़ी की रिपोर्ट करने के लिए
1930
पर कॉल करें

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

संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ

1.साइबर गीक समाचार

क) एनपीएम ट्रोजन यूएसी को बायपास करता है, ओसकम्पैटिबल पैकेज के साथ एनीडेस्क इंस्टाल करता है।



एनपीएम (नोड पैकेज मैनेजर) रजिस्ट्री पर अपलोड किया गया एक दुर्भावनापूर्ण पैकेज कोम्प्रोमाइज्ड विंडो मशीन पर एक परिष्कृत रिमोट एक्सेस ट्रोजन को तैनात करता पाया गया है। पैकेज को “ओसकम्पैटिबल” नाम दिया गया है।

सॉफ्टवेयर आपूर्ति श्रृंखला सुरक्षा फाइलम के अनुसार ओसकम्पैटिबल में कुछ अजीब बायनेरिज शामिल है, जिसमें एक निष्पादन योग्य फाइल, एक डायनमिक लिंक लाइब्रेरी (डीएलएल) और एक जावास्क्रिप्ट फाइल के साथ एक एन्क्रिप्टेड डीएटी फाइल शामिल है।

यह जावास्क्रिप्ट फाइल (“index.js”) एक “autorun.bat” बैच स्क्रिप्ट निष्पादित करती है, लेकिन यह निर्धारित करने के लिए संगतता जांच चलाने बाद ही कि लक्ष्य मशीन माइक्रोसाफ्ट विंडोज पर चलती है या नहीं।

यदि प्लेटफॉर्म विंडोज नहीं है तो यह यूजर को एक त्रुटि संदेश प्रदर्शित करता है जिसमें बताया गया है कि स्क्रिप्ट लिनक्स या एक गैर-मान्यता प्राप्त ऑपरेटिंग सिस्टम पर चल रही है और उनसे इसे “विंडोज सर्वर ओएस” पर चलाने का आग्रह किया जाता है। बैच स्क्रिप्ट अपनी तरफ से सत्यापित करता है कि यह प्रशासक से विशेषाधिकार रखता है या नहीं तो यह पॉवरशेल कमांड के माध्यम से एक वैध माइक्रोसोफ्ट ऐज घटक जिसे "cookie_exporter.exe" कहा जाता है, को रन करता है।

बाइनरी कोड को चलाने का प्रयास एक यूजर एकाउंट कंट्रोल (यूएसी) को ट्रिगर करेगा जो लक्ष्य को प्रशासक के साथ इसे निष्पादित करने के लिए कहेगा।

ऐसा करने पर थ्रेट एक्टर डीएलएल सर्च आर्डर हाईजैकिंग नामक तकनीक का लाभ उठाकर डीएलएल (“msedge.dll”) चलाकर हमले के अगले चरण को अंजाम देता है।

लाइब्रेरी का ट्रोजन जेड संस्करण डेट फाइल (“msedge.dat”) को डिक्रिप्ट करने और “msedgedat.dll”, नामक एक और डीएलएल लांच करने के लिए डिजाइन किया गया है, जो बदले में एक नियंत्रित डोमेन एक्टर नामक “kdark1(.)com” से जिप एर्चिव पुनर्प्राप्ति के लिए कनेक्शन स्थापित करता है।

जिप फाइल ऐनीडेस्क रिमोट डेस्कटाप सॉफ्टवेयर के साथ-साथ एक रिमोट एक्सेस ट्रोजन (“verify.dll”) से सुसज्जित है जो वेबसॉकेट के माध्यम से कमांड-इन-कंट्रोल (सी2) सर्वर से निर्देश प्राप्त करने और होस्ट से संवेदनशील जानकारी एकत्र करने में सक्षम है।

यह सुरक्षित प्राथमिकताओं के लिए क्रोम एक्सटेंशन भी इंस्टॉल करता है, ऐनीडेस्क को कॉन्फिगर करता है, स्क्रीन को छुपाता है और विंडोज को बंद करना अक्षम करता है, कीबोर्ड और माउस इवेंट को कैप्चर करता है।

सुझावः-

- स्वचालित सेटिंग अक्षम रखें।
- इंटरनेट कनेक्शन को सुरक्षित रखने के लिए फ़ॉयरवॉल को सेट-अप करें और उसका उपयोग करें।
- जब भी संभव हो एक गैर-प्रशासक खाते का उपयोग करें।
- अविश्वसनीय पक्ष से कुछ भी डाउनलोड के लिंक पर क्लिक करने से पहले दो बार सोचें।
- अपनी फाइल साझाकरण को सीमित रखें।
- अपने कंप्यूटर और सॉफ्टवेयर को अपडेट रखें।
- थर्ड-पार्टी सॉफ्टवेयर डाउनलोड से बचें।
- हार्डवेयर आधारित फॉयरवाल का उपयोग करें और डीएनएस तैनात करें।
-

ख) यूट्यूब चैनल का उपयोग कर लुम्मा स्टीलर को वितरित करने वाला थ्रेट ग्रुप।

एक थ्रेट ग्रुप लुम्मा स्टीलर वैरिएंट को वितरित करने के लिए यूट्यूब चैनलों का उपयोग कर रहा है। अटैकर्स यूट्यूब खातों से छेडछाड करते है, क्रैक किए गए सॉफ्टवेयर वाले वीडियो अपलोड करते है, और विडियो विवरण में दुर्भावनापूर्ण यूआरएल एम्बेड करते है। ये यूआरएल यूजर्स को एक जिप फाइल डाउनलोड करने के लिए प्रेरित करता है जिसमे एक निजी .नेट लोडर होता है जो लुम्मा स्टीलर मैलवेयर लाने के लिए जिम्मेदार होता है।

लुम्मा स्टीलर वैरिएंट विभिन्न चोरी की तकनीकों को नियोजित

करता है जैसे "बायगोलार्चेन" पद्धति का उपयोग करके स्ट्रिंग्स को डिकोड करना और डिटेक्शन से बचने के लिए व्यापक स्थिति जांच करना। अंतिम पैलोड को "सस्पेंड थ्रेड" फंक्शन का उपयोग करके इंजेक्ट किया जाता है। लुम्मा स्टीलर एक कमांड और कंट्रोल (सी2) सर्वर के साथ संचार स्थापित करता है, निर्देशों का आदान-प्रदान करता है और चुराए गए डेटा को प्रसारित करता है।

सुझावः-

- सिस्टम, एप्लिकेशन और सॉफ्टवेयर को नवीनतम संस्करण में अपडेट करें और नवीनतम सुरक्षा पैच डाउनलोड करें।
- एंटी-वायरस/एंटी-मैलवेयर सॉफ्टवेयर स्थापित करें और सॉफ्टवेयर (और सकी परिभाषा फाइलें) को अद्यतन रखें।
- 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 पॉप-अप विंडो पर भरोसा न करें जो आपसे सॉफ्टवेयर डाउनलोड करने के लिए कहती है।
- सभी यूजर्स खातों की नियमित रूप से निगरानी करें और निष्क्रिय खातों को अक्षम करें।
- उन खाता स्वामियों के लिए पासवर्ड अपडेट लागू करें जिनके क्रेडेंशियल लीक हो सकते है।

2. साइबर धोखाधड़ी :-

क) गूगल सर्च :- झारखंड गूगल सर्च में दो गिरफ्तार।

स्कैमर डीपफेक कॉल और विडियो के साथ गूगल विज्ञापनों का उपयोग उनसे मीलों दूर बैठे लोगों से पैसे चुराने में कर रहे हैं। ताजा मामले में दिल्ली की एक महिला ने गूगल पर पंजाब नेशनल बैंक का कस्टमर केयर नंबर खोजा और वेबसाइट पर दिखे मोबाइल नंबर पर कॉल की। लाइन के दूसरी तरफ मौजूद व्यक्ति ने उसे एक ऐप डाउनलोड करने के लिए कहा, जिससे उसे उसके खाते से 5 लाख रूपये से अधिक चुराने में मदद मिली।

पुलिस उपायुक्त के एक आधिकारिक बयान के अनुसार कथित व्यक्ति ने उसे रस्ट डेस्क ऐप डाउनलोड करने की सलाह दी और उसके फोन और खाते से संबंधित जानकारी तक पहुंच प्राप्त की। बाद में, उसके केनरा बैंक खाते से कुल रूपये 5,45,000/- डेबिट कर लिए गए।

ख) एक 45 वर्षीय डॉक्टर ने रूपये 1.8 करोड़ गवाँए।

धारवाड़ के एक 45 वर्षीय डॉक्टर साइबर अपराधियों का शिकार बन गए और उन्होंने 1.79 करोड रूपये गवाँए। साइबर क्राइम पुलिस उस धोखाधड़ी की जांच कर रही है जो तब हुई जब डॉक्टर को दो महीने पहले एक अज्ञात व्यक्ति का फोन आया। जालसाज ने खुद को वित्तीय सलाहकार बताकर शेयर बाजार में निवेश पर आकर्षक रिटर्न का वादा करके डॉक्टर को धोखा दिया। कॉल करने वाले ने अच्छे मुनाफे के लिए प्लैनेट इमेज इंटरनेशनल कंपनी के आईपीओ में निवेश करने का सुझाव दिया। कॉल करने वाले के कहने पर डॉक्टर स्वेच्छा से एक सोशल मिडिया साइट से जुड़ गया।

बातचीत ने एक भयानक मोड ले लिया क्योंकि साइबर अपराधियों नें डॉक्टर के बैंक खाते से संबंधित संवेदनशील डेटा को सफलतापूर्वक प्राप्त कर लिया। तत्पश्चात पीड़ित के विभिन्न बैंक खातों से रूपये 1.79 करोड़ की धनराशि स्थानांतरित कर ली गई। जिस तरीके से अपराधियों ने वह जानकारी प्राप्त की अभी तक अस्पष्ट बनी हुई है जो पुलिस को आगे की जांच करने के लिए प्रेरित कर रही है। कॉल करने वाले के विरूद्ध पुलिस में मामला दर्ज कर लिया गया है।

3. महीने की टिप

सुरक्षित सोशल मीडिया अकाउंटस ।

1. **मजबूत पासवर्ड नीतियाँ** :- मजबूत पासवर्ड नीतियों को कार्यान्वित करें और लागू करें जिसमें नियमित परिवर्तन और विभिन्न प्लेटफार्मों पर पासवर्ड के पुनः उपयोग से बचना शामिल है।
2. **मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए)** :- जहां भी संभव हो सभी सोशल मीडिया खातों के लिए एमएफए इनेबल करें।
3. **एक्सेस कंट्रोलः-** आधिकारिक सोशल मीडिया खातों तक

एक्सेस को नामित अधिकारियों और प्रणालियों तक सीमित करें।

4. समर्पित सुरक्षित उपकरणः- विशेष रूप से आधिकारिक सोशल मीडिया खातों के प्रबंधन के लिए समर्पित और सुरक्षित उपकरण आवंटित करें। इन उपकरणों में उन्नत सुरक्षा सुविधाएं होनी चाहिए और समझौते के जोखिम को कम करने के आशय से इसका उपयोग करना चाहिए।

5. डेडिकेटिड ई-मेल खातेः- आधिकारिक सोशल मीडिया खातों के संचालन के लिए एक समर्पित और अलग ई-मेल खाते का उपयोग करें। सुनिश्चित करें कि इस ई-मेल और सोशल मीडिया खातों के क्रेडेंशियल अलग-अलग है और संगठन की पासवर्ड नीति का अनुपालन करते है।

6. सरकारी खातों के संचालन के लिए व्यक्तिगत ई-मेल से बचें :- संभावित सुरक्षा को रोकने के लिए सरकारी सोशल मीडिया खातों के प्रबंधन के लिए व्यक्तिगत ई-मेल खातों के उपयोग करने से बचें।

7. एकल सक्रिय सत्र :- सुनिश्चित करें कि किसी भी समय केवल एक ही सत्र सक्रिय हो। अनधिकृत पहुंच को रोकने के लिए खाता सेटिंग्स के तहत सक्रिय किसी भी अन्य सत्र की नियमित रूप से जांच करें और समाप्त करें।

8. कंटेंट अप्रूवल :- सुनिश्चित करें कि सरकारी सोशल मीडिया हैंडल पर पोस्ट की गई सामग्री संगठन के भीतर उपयुक्त प्राधिकारी द्वारा पूर्व अनुमोदित हो।

9. सोशल मीडिया प्रबंधन टूल तक नियंत्रित पहुंच :- यदि सोशल मीडिया प्रबंधन टूल का उपयोग कर रहे हैं तो इन टूल की नियंत्रित और सुरक्षित पहुंच सुनिश्चित करें साथ ही नियमित समीक्षा करें कि किसके पास एक्सेस है।

10. सार्वजनिक उपकरणों से बचें :- सरकारी सोशल मीडिया खातों तक पहुंच के लिए सार्वजनिक या अनधिकृत उपकरणों के उपयोग से बचें।

11. जियोलोकेशन अक्षम करें :- लोकेशन ट्रेकिंग को रोकने के लिए आधिकारिक सोशल मीडिया प्लेटफार्म के लिए जीपीएस एक्सेस बंद करें।

12. सॉफ्टवेयर अपडेट :- नवीनतम सुरक्षा पैच के साथ सोशल मीडिया एप्लिकेशन और उपकरणों को नियमित रूप से अपडेट करें।

13. एक्सेस रिवोकेशन :- यदि किसी कर्मचारी की भूमिका बदलती है या वे संगठन को छोड देते हैं तो सोशल मीडिया खातों तक उनकी एक्सेस को तुरंत निरस्त करें।

14. संबंद्ध ई-मेल खातों की निगरानी करें :- किसी भी असामान्य गतिविधि अलर्ट के लिए सोशल मीडिया खातों से जुड़े ई-मेल खाते की नियमित जांच करें।

15. लॉगइन अलर्ट :- सोशल मीडिया प्लेटफॉर्म की सुरक्षा सेटिंग्स में अपरिचित लॉगिन प्रयासों के लिए अलर्ट सक्रिय करें।

16. थर्ड पार्टी ऐप्स से सावधानी :- सोशल मीडिया प्रबंधन के लिए थर्ड-पार्टी एप्लिकेशन का उपयोग करते समय सावधानी बरतें।

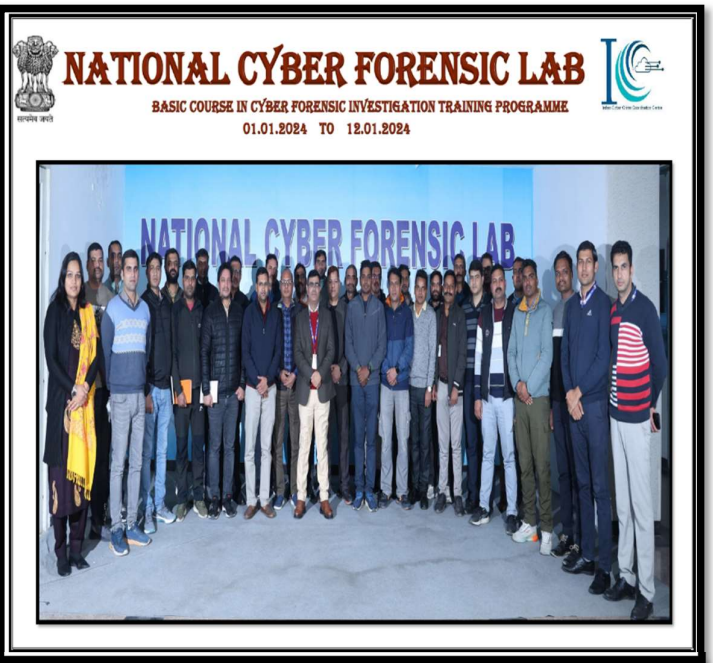
17. सूचनावान रहें :- सुरक्षा और गोपनीयता सेटिंग्स के संबंध में सोशल मीडिया कंपनियों के अपडेट से अवगत रहें और उन्हें उचित रूप से लागू करें।

18. फिशिंग और मैलवेयर से सावधान रहें :- फिशिंग लिंक पर क्लिक और क्रेडेंशियल सबमिट न करें और किसी भी मैलवेयर की उपस्थिति के लिए अपने सिस्टम को नियमित रूप से एंटीवायरस से स्कैन करें।

19. किसी लिंक पर क्लिक करते समय सावधान रहें :- कोई आपके किसी कनेक्शन के खाते पर कब्जा कर सकता है और आपको क्लिक करने के लिए प्रेरित करने का प्रयास कर सकता है। इसकी शुरूआत एक मासूम लगने वाले सवाल से हो सकती है जैसे आप क्या सोचते है जो आपको क्लिक करने के लिए प्रेरित करता है और आपको किसी भी चीज पर संदेह करने के लिए पर्याप्त संदर्भ नहीं देता है। लिंक आपको एक ऐसे पेज पर भेज सकता है जो आपके डिवाइस को संक्रमित कर देगा, या वह बिल्कुल एक वैध वेबसाइट (जैसे प्लेटफॉर्म का लॉगिन पेज) जैसा दिख सकता है लेकिन ऐसा नहीं है।

20. अपनी व्यक्तिगत जानकारी साझा न करें :- एक मित्र या फेक अकाउंट आपको आपकी व्यक्तिगत जानकारी साझा करने के लिए बरगलाने का प्रयास कर सकता है। पैसा कमाने, रोमांटिक रिश्ता शुरू करने या किसी व्यक्ति को उसके खाते से मदद करने से संबंधित संदेशों से सावधान रहें क्योंकि ये सामान्य शुरूआती बिंदु है जिनका उपयोग स्कैमर विश्वास बनाने के लिए करते है।

21. किसी भी किसी को अपना पासवर्ड या प्रमाणीकरण कोड न बताएं :- इसे साझा न करें, भले ही आपका कोई परिचित आपसे आपके फोन पर भेजा गया कोड साझा करने के लिए कह रहा हो। यदि उनके खातों से छेडछाड़ की गई है, तो स्कैमर्स संभवतः आपके किसी खाते में प्रवेश करने का प्रयास कर रहा है और आपसे एमएफए कोड साझा करने के लिए कह रहा है जो उन्हें एक्सेस प्रदान करेगा।



संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ