घटना निवारण

1. इंटरनेट और अन्य अविश्वसनीय नेटवर्क के बीच एक बफर जोन बनाने के लिए फायरवॉल का उपयोग करें, जिसका उपयोग फायरवॉल नियम बनाकर किया जाता है ताकि नेटवर्क आधारित हमलों में सिस्टम के जोखिम को कम करने के लिए सीमा पार डेटा का आदान प्रदान करने के लिए-केवल अधिकृत प्रोटोकॉल, पोर्ट और एप्लिकेशन को व्हाइट करके ट्रैफिक को रोका जा सके।लिस्ट-
2. पार्श्व गति के साथ आक्रमण गतिविधियों को सीमित करने के लिएसाथ अन्य-, रिमोट प्रोसीजर कॉल नेटवर्क फायरवॉल का उपयोग करें।/को रोकने के लिए एंड पॉइंट (आरपीसी)
3. दुर्भावनापूर्ण कोड या अनधिकृत सॉफ्टवेयर को एंडपॉइंट पर निष्पादन प्राप्त करने से रोकने के लिए सभी एंडपॉइंट वर्कस्टेशन पर एप्लिकेशन व्हाइटलिस्टिंग नीति अपनाएं।
4. कंप्यूटर से अप्रयुक्त या अनपैच किए गए सॉफ्टवेयर, विशेष रूप से दूरस्थ डेस्कटॉप सॉफ्टवेयर, यदि कोई हो, को हटा दें।
5. सुनिश्चित करें कि एप्लिकेशन नियंत्रण कृत प्रोग्रामों को अस्वी (को चलाने के लिएकृत स्क्रिप्टकेवल स्वी) टेंशन के निरपेक्ष चलने से रोकता है।उनके फाइल एक्स
6. सुनिश्चित करें कि सभी एंड प्वांइट प्रणालियों पर एंटीवायरस या मैलवेयर सुरक्षा प्रोग्राम चल रहा हो और वह हमेशा नवीनतम संस्करणों से अद्यतित रहे।
7. दुर्भावनापूर्ण स्क्रिप्ट को क्लिक पर चलने से रोकने के लिए, नोटपैड प्रोग्रम को .hta, .js, .jse, .vbs, .vbe, .wsfand, psl जैसे स्क्रिप्ट फाइल एक्सटेंशन के साथ जोड़ा जा सकता है हमेशा इस ऐप विकल्प) ।(का उपयोग करें

घटना का पता लगाना

1. टनलिंग और डेटा एक्सफिल्ट्रेशन के संभावित संकेतों के लिए डीएनएस गतिविधि की निगरानी करें।
2. संभावित घुसपैठ के लिए कॉन्फिगरेशन परिवर्तनों और कॉन्फिगरेशन के उचित उपयोग की नियमित जांच करें।
3. ब्लॉक I विभिन्न सुरक्षा एजेंसियों द्वारा साझा किए गए दुर्भावनापूर्ण डोमेनएलपी से कनेक्टिविटी / प्रतिबंधित करें। आइसोलेट करने के बाद ऐसे डोमेन से जुड़ने वाली पहचानी गई मशीन की फोरेंसिक छवि लें।
4. अंतिम पितम को पुनर्स्था बैकअप पर सिस्टज्ञात अच्छे-करें या नया इंस्टॉलेशन करें।

घटना की प्रतिक्रिया

1. एलएएन करेंनेक्टटरों को तुरंत डिस्कक्रमित कंप्यूइंटरनेट से सं/;
2. कंप्यूटर से अप्रयुक्त या अप्रकाशित सॉफ्टवेयर, विशेष रूप से दूरस्थ डेस्कटॉप सॉफ्टवेयर, यदि कोई हो, को हटा दें;
3. किसी अन्य सुरक्षित कंप्यूटर से सभी ईमेल और ऑनलाइन सेवाओं के पासवर्ड बदलें :
4. संक्रमित कंप्यूटर की हार्ड डिस्क को डेटा फाइलों का बैकअप लेने के बाद फॉर्मेट किया जाए;
5. ऑपरेटिंग सिस्टम और एप्लिकेशन को क्लीन सॉफ्टवेयर से पुनः इंस्टाल किया जाना चाहिए ;
6. बैकअप डेटा को पुनर्स्थापित करने से पहले उसमें वायरस देखने के लिए स्कैन किया जाना चाहिए।