सायबर गुन्हे आणि आपण

रोहास नागपाल
अक्षय फडके

कॉपीराईट नोटीस

हि रचना लेक्सकोड लीप (LEAP) परवाना अंतर्गत समाविष्ट आहे,म्हणजेच ह्या रचनेबाबत वाटप, प्रत(नवीन), सुधारणा, रुपांतर किंवा पुनरुत्पादन अव्यवसायीक कारणासाठी केले जाऊ शकते, पण ती योग्य प्रकारे लेखकाला समर्पित केली असली पाहिजे.

कायदेशीर नोटीस

या पुस्तकात दिलेली माहिती हि ज्ञानार्जनासाठी दिलेली आहे आणि हा कोणताही कायदेशीर सल्ला नाही.

हे प्रकाशन लेक्स्कोड एजुकेशन आणि असेसमेंट प्ल्याटफोर्म (LEAP) **चा भाग आहे.:**

लेक्सकोड

रेग्युलेटरी कम्प्लायन्स टेक्नोलॉजीज प्रा.लि.
इनक्युबेटेड बाय सायन्स ॲण्ड टेक्नोलॉजी पार्क
प्रमोटेड बाय डिपार्टमेंट ऑफ सायन्स ॲण्ड टेक्नोलॉजी
गव्हर्रमेंट ऑफ इंडिया

संपर्क: सायन्स ॲण्ड टेक्नोलॉजी पार्क, युनिव्हर्सिटी ऑफ पुणे, पुणे - ०७
info@lexcode.in | www.lexcode.in

एशियन स्कूल ऑफ सायबर लॉज

सायबर लॉ आणि सायबर क्राईम तपासामधील जागतिक प्रणेता असलेली एशियन स्कूल ऑफ सायबर लॉज हि संस्था १९९९ साली स्थापन झाली.आम्ही भारत सरकारला माहिती तंत्रज्ञान कायद्याच्या नियम व अटी, सायबर कॅफेसाठीची मार्गदर्शक तत्वे, माहिती जगतातील गुन्हेगारी कायद्याची आखणी करण्यासाठी मदत केलेली आहे.

आम्ही फॉरेन सर्टीफाइंग अथॉरीटीजचे आकलन करण्या संबंधातील नियमांची आखणी करण्यासाठी सर्टीफाइंग अथॉरीटीजच्या कंट्रोलरनां मदत केली आहे.

ASCL कॉम्प्युटर क्राईम आणि छळ रिपोर्ट (इंडिया) अशा प्रकारचा अभ्यास प्रथमच झाला आहे, असे युनायटेड नेशनच्या ई- कॉमर्स आणि डेव्हलपमेंट रिपोर्टमध्ये (२००३) नमुद केले आहे. वर्ल्ड कॉग्रेस ऑन इन्फोरमेटीक्स ॲण्ड लॉ, स्पेन (२००२), क्युबा (२००३), आणि पेरू (२००४) झालेल्या परिषदेमध्ये आम्ही सहभागी होतो

.

संपर्क:

६ वा मजला, प्राईड कुमार सेनेट, सिग्मा हाउसच्या पाठीमागे,

सेनापती बापट मार्ग, पुणे- ४११०१६ (भारत)

info@asianlaws.org | www.asianlaws.org

सर्वात खतरनाक गुन्हेगार तो असतो ज्याच्याकडे तर्काचे वरदान आहे,
पण कोणत्याही नैतिकते शिवाय..

मार्टिन लुथर किंग, ज्यु.
द परपज ऑफ एज्युकेशन, मरून टायगर, जानेवारी- फेब्रुवारी १९४७

अनुक्रमणिका

1. अनोनीमायझर

बऱ्याच वेळेस लोकांचा असा गैरसमज असतो कि इंटरनेटचा वापर करताना त्यांच्या कृती हया वैयक्तिक अथवा निनावी स्वरूपाच्या असतात. परंतु दुर्दैवाने सत्य परिस्थिती काही वेगळीच आहे. प्रत्येक वेळी आपण जेव्हा एखाद्या संकेतस्थळाला भेट देता, आपण एक नोंद पाठीमागे सोडता, ज्याद्वारे आपण कोठून आहात, कोणत्या प्रकारचा कॉम्प्युटर वापरता इत्यादी तपशील समजतो. तुमच्या प्रत्येक भेटीची नोंद ठेवली जाते.

एक अनोनीमायझर अथवा अनोनिमीस प्रोक्झी अशा साधनांचा वापर करून आपल्या इंटरनेट वरील हालचाली गुप्त राखण्यात मदत होते. यामुळे इंटरनेटवर आपली वैयक्तिक माहिती उघड न करता सर्फ करू शकतो. हे साधन आपला IP अड्रेसच नाही तर इंटरनेट हिस्ट्री हि लपवते. आणि निषिद्ध असलेल्या संकेतस्थळाला हि आपण भेट देऊ शकता. पण समस्या अशी आहे कि, जेव्हा काही लोक गुन्हेगारी अथवा समाजास विघातक अशी कृत्य करण्यासाठी अशा साधनांचा वापर करतात तेव्हा त्याचा शोध घेणे अवघड होऊन बसते.

उदाहरण: समीर अनोनीमायझरचा वापर करून एका ई मेल स्पुफिंग संकेतस्थळावरून लॉग इन करतो आणि एक फसवा ई मेल शेकडो

लोकांना पाठवतो. पण जेव्हा पोलिस ह्या फसव्या ई मेलचा IP अड्रेस शोधण्याचा प्रयत्न करतात तेव्हा त्यांच्या हाती काहीच लागत नाही. कारण समीरने अनोनीमायझरचा वापर केला होता.

उदाहरण: कोचीन मधील शाळेने त्यांच्या कॉम्प्युटर प्रयोग शाळेत फेसबुक वापरावर बंदी केली होती, शाळेच्या अधिकाऱ्यानी फायरवावॉलचा वापर करून त्या संकेतस्थळाचा ॲक्सेस बंद केला होता. पण समीर नावाच्या एका ८ वीतील मुलाने शाळेच्या कॉम्प्युटरवरून, अनोनीमायझरद्वारे फेसबुकचा वापर केला होता.

hidemyass.com आणि anonymous.org हि दोन प्रसिद्ध संकेतस्थळ आहेत.

2. ARP *कॅशे पोयझनींग*

नेटवर्क उपकरण अड्रेस रिझोलुशन प्रोटोकॉलचा (ARP) **वापर करून** MAC **अड्रेस आणि** IP **अड्रेस यांची जुळवणी करतात,यामुळे स्थानिक कॉम्प्युटर वरील उपकरण एकमेकास शोधतात**. ARP **हे शाळेतील अनुक्रमांकसारखे आहे**. **प्रत्येक नेटवर्कड कॉम्प्युटरला दोन अड्रेस असतात** MAC **आणि** IP **अड्रेस**. MAC **अड्रेस (मिडिया ॲक्सेस कंट्रोल) हा एक युनिक आयडेंटिफायर आहे. उदा: ००-००-०c -३४-११-४e जो नेटवर्क इंटरफेस कार्ड च्या निर्मात्याकडून उपकरणात हार्ड कोडेड असतो, जो बदलत नाही**. ARP **कॅशे पॉयझनिंग**, ARP **स्पुफिंग म्हणुनही ओळखले जाते, हे एक तंत्र आहे ज्याद्वारे हल्लेखोर एक फसवा** ARP **मेसेज** LAN **वरून पाठवतो. या पाठीमागे उद्देश असा आहे कि हल्लेखोराचा** MAC **अड्रेस दुसऱ्या होस्टच्या** IP **अड्रेसशी जुळवणे, ज्यामूळे गेटवेसाठीचे डाटा ट्र्याफिक हे हल्लेखोरास पाठवले जाईल**.

APR **स्पुफिंगमुळे हल्लेखोर नेटवर्क वरील डाटा संपादित करू शकतो**.

उदा: पूजा तिच्या ऑफिसच्या कॉम्प्युटरवरून एका संकेतस्थळावरून खरेदी करते व त्यासाठी आपल्या क्रेडीट कार्डचा वापर करते. तिला वाटते कि तिच्या क्रेडीट कार्डची माहिती संबंधित संकेतस्थळाच्या पेमेंट गेटवेला मिळाली आहे , पण तिच्या नकळत समीर ऑफिसच्या नेटवर्कवरती ARP

पोयझनींगचा वापर करत असतो. ज्यामुळे तिची क्रेडीट कार्डची माहिती पेमेंट गेटवेला मिळण्याऐवजी समीरच्या कॉम्प्युटरला मिळते.

3. *बॅकडोर*

बॅकडोर म्हणजे सुरक्षा यंत्रणेला फाटा देऊन कॉम्प्युटर ॲक्सेस करणे. काही वेळेस प्रोग्र्यामर स्वतःच बॅकडोर इंस्टाल करतो, ज्यामुळे त्यास प्रोग्राममध्ये गरजेनुसार बदल करता यावेत. मात्र अनेक वेळेस बॅकडोरचा हेल्लेखोराकडून गैरवापर केला जातो. बॅकडोर जरी प्रोग्राममध्ये सुधारणा करण्यासाठी वापरल जात असले तरी हा एक सुरक्षेच्या दृष्टीने मोठा धोका आहे, जो यंत्रणेला कमकुवत बनवतो. एकदा गुन्हेगाराकडून बॅकडोर स्थापन केला गेल्यावर त्याला सहज सिस्टममध्ये प्रवेश मिळतो ज्यामुळे त्यांना सर्व प्रकारची संवेदनशील माहिती मिळू शकते जसे कि आर्थिक माहिती, बँक खाते क्रमांक, इ. अशा प्रकारची माहिती हाती लागल्यास गुन्हेगार त्याचा वाटेल तसा गैरवापर करू शकतो.

4. बॅकस्क्याटर

हा प्रकार आऊट स्क्याटर या नावाने हि ओळखला जातो, बॅकस्क्याटर हा ई मेल, स्पॅम, वोर्म आणि व्हायरस यांच्या साइड इफेक्टमुळे तयार झालेला प्रकार आहे. हे आपण एका सध्या उदाहरणाने समजवून घेऊ, एक वोर्म समीरचा ई मेल अड्रेस वापरून लाखो लोकांना ई मेल पाठवतो. आणि हे सर्व ई मेल अड्रेस अस्तित्त्वात नसलेले आहेत,उदा: एक असा स्पॅम ई मेल pooja@example.com **पाठवला जो कि अस्तित्वातच नाही. पण** example.com **ई मेल सर्व्हरनी समीरला रिपलाय केला कि** pooja@example.com **नावाचा ई मेल अस्तित्वात नाही.अशा प्रकारचे समीरला हजारो ई मेल येतील**.

5. *द ब्लु - ब्लुबगिंग, ब्लु-ज्याकिंग आणि ब्लु-स्नारफिंग*

ब्लुबगिंग, ब्लु-ज्याकिंग आणि ब्लु-स्नारफिंग हे ब्लुटूथ वापरून करण्यात येणाऱ्या हल्ल्याचे प्रकार आहेत. सुरवातीस ब्लुटूथ सुविधा असलेल्या कॉम्प्युटरवरती हल्ले होत होते पण आता ब्लुटूथ सुविधा असलेल्या सर्व उपकरणावर हल्ले होऊ लागले आहेत.

ब्लु - ब्लुबगिंगमूळे आपण लक्ष्य असलेल्या मोबाईलचा व्हरचुअल ताबा मिळवु शकता, ज्याद्वारे फोन मध्ये फेरफार करून त्याची सुरक्षा कमकुवत केली जाते, आणि फोनच्या वापरकर्त्याच्या नकळत एक बॅकडोर एन्ट्री तयार केली जाते ज्यामुळे पीडिताच्या फोनचा पूर्णपणे ताबा मिळवता येतो. आणि इतकेच नाही तर आपण त्या फोन वरून संदेश पाठवणे, क्यालेंडर पाहणे, फोन करणे इ. गोष्टी करता येतात. तसेच आपण पीडिताचे फोन वरील बोलणे चोरून ऐकू शकतो.

ब्लुबग प्रोग्राम, कॉल फोरवर्ड अप्लिकेशन तयार करण्यास सक्षम आहे , ज्याद्वारे हल्लेखोर पीडितासाठीचे आलेले कॉल्स स्वतःकडे वळवू शकतो, ब्लुबग वापर करता सहज पणे पीडित व्यक्तीच्या दैनंदिन जीवनातील संभाषण ऐकू शकतो. अगोदर अशा प्रकारच्या हल्ल्यांची कक्षा १० ते २० मीटर होती , पण कालांतराने त्याची कार्यक्षमता वाढत गेली.

ब्लुबगिंगचे सौम्य स्वरूप म्हणजे ब्लु-ज्याकिंग आहे. हे एक असे तंत्र आहे ज्याद्वारे आपण निनावी आणि नको असलेले ब्लुटूथ वापरत

असलेल्या इतर लोकांना पाठवू शकतो. ब्लु-ज्याकिंग ब्लुटूथ फोनची इतर उपकरण शोधण्याच्या प्रयत्न करते आणि जे संपर्क साधण्याच्या क्षमतेवर अवलंबून आहे . माहितीची देवाणघेवाण करण्यासाठी असलेल्या सुविधेचा ब्लुज्याकर गैरफायदा उचलतो. ब्लुज्याकर फोनच्या अड्रेस बुक मध्ये एक नवीन नोंद करतो आणि मेसेज टाइप करून ब्लुटूथने पाठवतो, मग फोन इतर ब्लुटूथ फोनचा शोध घेतो, आणि जर तो मिळाला तर मेसेज पाठवून देतो. ह्याचे नाव ब्लु-ज्याकिंग असले तरी हे इतके घातक नाही, यामुळे वैयक्तिक माहिती चोरली जात नाही किंवा फोनचा ताबाही घेता येत नाही. पण जर ब्लु-ज्याकिंगचा वापर करून अश्लील मेसेज किंवा धमकीचा मेसेज पाठवल्यास ते धोकादायक ठरू शकत.

ब्लु-स्नारफिंग म्हणजे ब्लुटूथ फोन मधून डाटा चोरी करणे. यासाठी हल्लेखोर आपल्या कॉम्प्युटरवरती एक विशिष्ठ प्रकारचे सॉफ्टवेअर रन करतो जे नजीकचे फोन शोधून त्यांच्याशी अपोआप जोडून त्यावरील डाटा चोरी करतो, आणि मोबाईल फोनचा सिरिअल नंबर हि चोरून तो फोन क्लोन करू शकतो . जरी पीडितने त्याचे ब्लुटूथ बंद केले तरी तो सुरक्षित नाही कारण उपकरण जरी हिडन स्वरुपात असले तरी त्याचा MAC अड्रेसचा अंदाजाने किंवा ब्रुट फोर्स आटयक ने ब्लु-स्नारफिंग करता येते.

BT Crawler **हे स्कॅनर वापरून विंडोज आधारित मोबाईल उपकरणानवर ब्लु-ज्याकिंग आणि ब्लु-स्नारफिंग हल्ला करता येतो**.

6. *बफर ओवरफ्लो*

जेव्हा एखादा प्रोग्राम किंवा प्रोसेस बफरमध्ये(तात्पुरता डाटा स्टोर करण्याची जागा) त्याच्या क्षमतेपेक्षा जास्त डाटा स्टोर करण्याचा प्रयत्न करतो तेंव्हा बफर ओवरफ्लो होतो. बफर हे मर्यादित डाटा साठवण्यासाठी असते, जास्तीची माहिती लगतच्या बफरमध्ये जाते, ज्यामुळे त्या बफर मधील वैध डाटा करप्ट किंवा ओवरराईट होतो. बफर ओवरफ्लो हा अगदी साध्या प्रकारचा डाटा इनटीग्रीटीच्या सुरक्षेवर हल्ला आहे. बफर ओवरफ्लो हल्ल्यातील जास्तीच्या डाटा मध्ये काही विशिष्ट कृती करण्यासाठीचे कोड असू शकतात. ज्यामध्ये कॉम्प्युटरवरती हल्ला करण्याच्या सुचना देखील असू शकतात . ज्यात युझरचा डाटा नष्ट किंवा गोपनीय माहिती उघड करण्याचा हेतु असू शकतो.

c प्रोग्रामिंग भाषेने दिलेले फ्रेमवर्क आणि कमकुवत प्रोग्रामिंग सरावामुळे बफर ओवरफ्लो हल्ल्यांचा उदय झाला आहे.

उदाहरणार्थ:

बऱ्याच वर्षापूर्वी मायक्रोसोफ्ट आऊटलुक आणि आऊटलुक एक्सप्रेस मध्ये बफर ओवरफ्लोचा शोध लागला. एका प्रोग्रामिंग दोषामुळे हल्लेखोर सहजपणे एक ईमेल मेसेज पाठवून कॉम्प्युटर इंट्रीग्रीटी धोक्यात आणणे शक्य झाले आहे. नेहमीच्या ईमेल व्हायरस प्रमाणे हा मेसेज ओपन करण्याचीसुद्धा गरज नाही तो आपोआप हल्ला करतो.

प्रोग्रामच्या मेसेज हेडर तंत्रामध्ये दोष असल्यामुळे सेंडरला डाटा ओवरफ्लो करणे शक्य आहे. यामुळे हल्लेखोर त्यास पाहिजे त्याप्रकारचा कोड ईमेल प्राप्तकर्त्याच्या कॉम्प्युटरवर चालवणे शक्य आहे. जसे कि प्राप्तकर्त्याने सर्व्हरवरून मेसेज डाऊनलोड केल्याकेल्या हि प्रोसेस सुरु होते, त्यामुळे अशा प्रकारचा बफर ओवरफ्लो हल्ला रोखणे खुप अवघड आहे. मायक्रोसोफ्टने ह्या समस्येसाठी एक पॅच पण तयार केला आहे.

7. बुलीयिंग इन सायबर स्पेस

इंटरनेट किंवा त्या प्रकारच्या टेक्नोलॉजीचा वापरकरून इतर लोकांना मुद्दामहून, सतत आणि विरोधी भुमिकेतून अरेरावी करणे म्हणजे सायबर बुलीयिंग होय. सायबर बुलीयिंग खालील गोष्टींद्वारे करता येते

१. टेक्स्ट मेसेज किंवा इमेज

२. ऑनलाईन वैयक्तिक शेरेबाजी करणे

३. तिरस्कारयुक्त भाषणबाजी

४. इतर लोकांना नापसंतीसाठी उक्सवणे, आणि एकत्रित पणे एखाद्यास लक्ष्य करून त्याची खिल्ली उडविणे

५. खोटी विधाने करून लोकांना बैचेन किंवा लोकांचा पाणउतारा करणे.

सायबर बुलीयिंग करणारे एखाद्याची वैयक्तिक माहिती संकेतस्थळावर उघड करू शकतात. पीडित व्यक्तीची ओळख वापरून पिग्गी बॅकिंग करणे आता सामान्य झाले आहे. याचा वापर एखाद्याबद्दल आक्षेपार्ह मजकूर पोस्ट करून बदनामी किंवा खिल्ली उडवण्यासाठी पण केला जाऊ शकतो.

सायबर बुलीयिंग शिक्षेस पात्र ठरवण्यासाठी अमेरिकेतील बऱ्याच राज्यात कायदा प्रक्रिया सुरु आहे यामधे न्यूयॉर्क, मिसूरी, हॉड आयलंड

आणि मेरीलँड या राज्यांचा समावेश आहे. २००७ मध्ये अमेरिकेतील कमीत कमी ७ राज्यांमध्ये डिजिटल छळा विरोधात कायदे करण्यात आलेले आहेत. ऑगस्ट २००७ मध्ये अमेरिकेतील कॅलिफोर्निया या राज्याचा विधिमंडळाने पहिल्यांदाच प्रत्यक्ष पणे सायबर बुलीयिंग हाताळण्यासाठी कायदा तयार करण्यात आला.

भारतीय कायद्यात सायबर बुलीयिंग, माहिती तंत्रज्ञान कायदा कलम ६६अ मध्ये समाविष्ट आहे. " संवाद साधनानद्वारे आक्षेपार्ह मेसेज पाठवणे" असे या प्रकरणाचे नाव आहे. या अंतर्गत ३ वर्षापर्यंतची कारावासाची शिक्षा आणि दंड आहे.

आक्षेपार्ह मजकुरात खालील प्रकार मोडतात:

१. मजकूर जो पूर्णतः आक्षेपार्ह आहे. (उदा. जो राग, द्वेष उत्पन्न करेल)

२. मजकूर जो धमकी वजा घातकी असेल.

३. मजकूर ज्या मधील माहिती चुकीची असेल , जिचा उद्देश राग , गैरसोय , अपमान , त्रास , द्वेष ,शत्रुत्व , अडवणूक ,करण्याचा हेतूने पाठवलेला असेल .

४. मजकूर जो फसवण्याच्या किंवा दिशाभूल करण्याच्या उद्देशाने पाठवलेला असेल.

उदाहरण :

मेगन टेलर मेइएर अमेरिकन युवक होता ज्याने आपल्या १४ व्या वाढदिवसाच्या ३ आठवडे अगोदर गळफास घेऊन आत्महत्या केली, एक वर्षानंतर मेइएरच्या पालकांनी या प्रकरणात चौकशीची मागणी केली, तर हि आत्महत्या MySpace **सोशल संकेतस्थळा वरील सायबर बुलीयिंग घडून आल्याचे निदर्शनास आले** .

UK **ची एक ८ वर्षाची मुलगी विमानातून प्रवास करत असताना तिचे दुसऱ्या एका मुली बरोबर भांडण झाले, ज्याचा परिणाम असा झाला कि त्या ८ वर्षाच्या मुली बरोबर ५ वर्ष सायबर बुलीयिंग झाले, जेव्हा ती १४ वर्षाची झाली तेव्हा तिने आपल्या पालकांना हि गोष्ट सांगितली व त्यांनी हा प्रकार थांबवला. पण लगेच बुलीयिंग करणाऱ्यान कडून तिच्यावर हल्ला झाल्याने तिला आठवडाभरासाठी रुग्णालयात दाखल करावे लागले.**

8. *क्लिक फ्रोड*

जेव्हा एखादा व्यक्ती किंवा स्वयंचलित कॉम्प्युटर प्रोग्राम "पे पर क्लिक" जाहिरातींवर क्लिक करतो तेव्हा क्लिक फ्रोड घडतो. यामागील खरा उद्देश जाहिरातीचा मजकूर नसून पैसे कमावण्याचा असतो. क्लिक फ्रोड कंपनीकडून प्रतिस्पर्ध्याचे जाहिरातीचे बजेट कमी करण्यासाठी किंवा संकेतस्थळासाठी महसुल मिळवण्यासाठी केला जातो.

काही संकेतस्थळ लोकांना खोटे क्लिक करण्यासाठी पैसे देतात व ग्राहकाची बिल वाढवतात.

क्लिक फ्रोड करण्यासाठी क्लिक बॉटचा हि वापर केला जातो. हा एक छोटा कोड आहे जो व्हायरस सारखा वेगवेगळ्या कॉम्प्युटरवरती पसरून विविध IP अड्रेसवरून क्लिक करतो. मालवेअर हे अजुन एक साधन आहे ज्याद्वारे आपण हे करू शकता, यामध्ये मालवेअर प्रत्येक कॉम्प्युटरवरून थोडयाच क्लिक करतो ज्यामुळे हा घोटाळा शोधणे अवघड बनते. हे बॉटस दूरस्थपणे (रिमोटली) नियंत्रित केले जातात.

क्लिक फ्रोड सुरवातीला ओळखणे खुप अवघड आहे पण कालांतराने ते दृष्टीस पडतात. अशा प्रकारच्या क्लिक जाहिरातकर्त्याचे पे पर क्लिकची फी वाढवते पण खप(सेल) नाही.

उदाहरण:

मागील वर्षी अनेक विक्रेत्यांना क्लिक फसवणूक केल्याबद्दल फेसबुक विरोधात फिर्याद दाखल केली. पण फेसबुकचा असा दावा आहे कि विक्रेत्यान त्यांच्या बरोबर असा करार केला कि त्यांनी सर्व क्लिकसाठी देय करणे आवश्यक आहे त्याच्या वैधतेची पर्वा न करता, म्हणून हि फिर्याद बाद ठरवावी असे फेसबुकचे म्हणणे आहे. फिर्यादीच्या आरोपाच्या उलट करारात असे कुठे हि म्हंटले नाही कि क्लिक फ्रोड तपासण्याची जबाबदारी फेसबुकची आहे , पण करारा प्रमाणे फेसबुक फिर्यादीच्या जाहिरातीवरील प्रत्येक क्लिकसाठी पैसे घेण्यास सक्षम आहे.

9. *कॉम्प्युटर ट्रेसपास*

एखादा माणूस कॉम्प्युटर ट्रेसपास केल्याबद्दल दोषी आहे असे आपण म्हणू शकतो जर त्याने जाणुनबुजून आणि परवानगीशिवाय कोणत्याही संगणक, संगणक प्रणाली, संगणक नेटवर्क, संगणक प्रोग्राम, किंवा डाटा संबंधित खालील पैकी कुठलीही कृती केली तर.

१. ॲक्सेस केला,

२. बदल केला,

३. डिलीट केल,

४. नुकसान केल,

५. नष्ट केल,

६. अडथळा निर्माण केला

यासंदर्भात प्रत्येक राज्यानुसार कायदे आहेत. तथापि सर्व कॉम्प्युटर ट्रेसपासचा मुख्य घटक हा परवानगीशिवाय संगणक, संगणक प्रणाली ॲक्सेस करणे हा आहे.

उदाहरण:

तेज आपली माजी पत्नी श्रीनीचा पासवर्ड वापरून तिची आर्थिक गोपनीय माहिती ॲक्सेस केली,तर आपण तेजने कॉम्प्युटर ट्रेसपास केला असे म्हणू शकतो. त्याचा पत्नीची आर्थिक गोपनीय माहिती सुरक्षित होती किंवा नाही अथवा त्याने पासवर्डचा अंदाज जरी लावला तरी या गोष्टीनी फरक पडत नाही, हा कॉम्प्युटर ट्रेसपास आहे.

विजयला त्याची बायको बसंतीच्या चारित्र्यावर संशय असल्या कारणाने त्याने तिच्या संमती शिवाय ईमेल तपासुन गैरकृत्यांच्या प्रिंट काढल्या आणि त्या कोर्टामधे त्यांच्या घटस्पोटासाठी पुरावा म्हणून सादर केल्या. पण हे ईमेल्स कोर्टात पुरावा म्हणून दाखल केले जाऊ शकत नाही आणि विजय कॉम्प्युटर ट्रेसपासच्या गुन्ह्यासाठी दोषी आहे.

10. *कुकी मॅनीपुलेशन*

कुकी हि वेब ब्राउझरच्या मेमरीमध्ये नोंद असलेली एक छोटी फाईल किंवा टेक्स्ट स्ट्रिंग असते. वेब साईटचा वापरकर्ता ओळखण्यासाठी त्याचा वापर होतो. या शब्दाचा उगम एका प्रख्यात कॉम्प्युटर विज्ञान शब्दापासुन झाला आहे ज्याचा वापर एखाद्या मध्यस्थाकडून अपारदर्शक डाटाचा भाग असेल तर त्याचे वर्णन करण्यासाठी होतो.

उदाहरण:

सान्या आपला युजर नेम आणि पासवर्ड वापरून example.com **ला लॉग इन करते.** Example.com **तिच्या ब्राउझरमध्ये एक कुकी तयार करेल. आता प्रत्येक वेळी सान्या जेव्हा या संकेतस्थळाशी जोडली जाईल,** example.com **तिचे लॉग इन स्टेटस आणि ओळख तिच्या कुकीशी पडताळून बघेल.**

एकदा का सान्या लॉग आऊट झाल्यावर कुकी नष्ट होईल.

वेबसाइट कुकीचा वापर वापरकर्त्याची वैयक्तिक माहिती प्रमाणीकृत (अथोनथीकेट) करण्यासाठी, ऑन लाईन सेवेत ग्राहकाला मदत करण्यासाठी, किंवा सांख्यिकी आणि लोकसंख्याशास्त्राची माहिती गोळा करण्यासाठी करतात.

सध्या टेक्स्ट फाईलच्या स्वरुपात सेव्ह केलेल्या कुकी डिलीट करता येऊ शकतात. जर आपला ब्राउझर चालू असताना कुकी डिलीट केली तरी ब्राउझर बंद केल्यावर ती पुन्हा क्रिएट होईल. कारण कि सर्व कुकी ह्या ब्राउझर बंद करे पर्यंत त्याच्या मेमरीतच असतात.

इंटरनेट ब्राउझरने दिलेल्या पर्यायानुसार आपण किती व कोणत्या कुकी स्विकारायच्या हे ठरवू शकता.

एक नमुना कुकी:

```
WT_FPCid=2606225312.30232428:lv=1340297056862:ss=134
0297027078microsoft.com/108834925404163096677920584
1030930232533*MUID3EB7CCF35DD667392CFCCF7559D667
48microsoft.com/102425489404163037927919363512793302
32533*MC1GUID=34bf6934c01bf84b9ed7be056293a40e&HA
SH=3469&LV=20126&V=3&LU=1340255633975microsoft.com
/102415794008323096668319415992903023253 3*AI&I=AxU
FAAAAAAD1BgAAEBuCIaRDSYlMEQ+AVjfwww!!microsoft.com
/102441365664003243660019417552903023253 3*
```

अनेक संकेतस्थळ कुकीचा ॲक्सेस नियंत्रण स्किम राबवण्यासाठी वापर करतात. उदाहरणार्थ एक सद्यसता नोंदणी करणाऱ्या साईटला युझर नेम आणि पासवर्ड लागते,आणि आपण जेव्हा आपण प्रथम भेट देता तेव्हा आपल्या ब्राउझरला कुकी पाठवली जाऊ

शकते. आणि जर आपल्या ब्राउझरने वैध कुकी तयार केली तर संकेतस्थळ आपणास निषिद्ध वेबपेजेसला ॲक्सेस देईल, येथे कुकीचा प्रवेश दखला म्हणून वापर होतो. याचे संकेतस्थळला अनेक फायदे आहेत, यामुळे संकेतस्थळाला सारखे युझर नेम आणि पासवर्ड डाटाबेस मधून तपासण्याची गरज भासत नाही.

या प्रकारची जरी यंत्रणा सुरु केली तरी याचा गैरवापर केला जाऊ शकतो, उदा: हॅकर प्याकेट स्निफरचा वापर करून कुकी आपल्या ब्राउझर कडून सर्व्हरकडे जाताना संपादित करू शकतो ज्यामुळे त्यास वेबसाईटला ॲक्सेस मिळुन जाईल.

कुकीमध्ये खालील ६ प्रकारचे पॅरामीटर असतात:

१. कुकीचे नाव,

२. कुकीचे मुल्य,

३. कुकुची वैधता तारीख,

४. कुकीचा वैध पाथ,

५. कुकीचा वैध डोमेन,

६. कुकी वापरण्यासाठी लागणारे सुरक्षित कनेक्शन

यापैकी दोन अनिवार्य आहेत (नाव आणि मुल्य), स्वल्पविराम (;) प्रत्येक पॅरामीटर अलग करतो.

१. नाव; मुल्य :

कुकीचे नाव आणि मुल्य पेअरिंगकरून एकत्रित पणे ठरवता येते.

२. कालबाह्यता (एक्सपायरी):

या पॅरामीटरने आपण कुकीचा जीवनकाळ ठरवु शकतो उदा: expires=Sat, 25-Apr-2013 18:30:00 GMT

जर कालबाह्यता (एक्सपायरी) स्पष्टपणे दिली नसेल तर डीफॉल्टपणे कुकी सेशनच्या बरोबर संपते (एक्सपायर होते). सेशनचा काळ ब्राउझर आणि सर्व्हरवरती अवलंबुन असतो, सामान्यतः सेशनचा काळ म्हणजे ब्राउझर विंडो ओपन राहिलेला वेळ इतका असतो. आणि वापरकर्ता वेबसाईट वापरत नसला तरी हे असेच समजण्यात येते.

३. पाथ:

कुकीच्या चार पर्यायापैकी किंवा प्यरामीटरपैकी हे सर्वात जास्त उपयोगाचे आहे. ह्या प्यरामीटरमुळे URL पाथ स्थापित होतो ज्यामध्ये कुकी वैध राहते. जर वापरकर्त्याने अशा वेबपेजेसना भेट दिली कि जे या

पाथमध्ये येत नाहीत, तर ब्राउझर हि कुकी वापरु शकत नाही. उदा: path=/documents

जर कुकीचा पाथ स्पष्टपणे ठरवला गेला नसेल तर ज्या URL **नी कुकी तयार झाली आहे तिचा तो पाथ स्वीकारेल**.

४. डोमेन:

यामुळे पाथ प्यरामीटरची व्याप्ती जरा वाढते. जर एखादी वेबसाईट एकाच डोमेनसाठी अनेक सर्व्हरवरती काम करत असेल तर काय करयचे? आता इथे डोमेन प्यारमीटर स्पष्ट करणे महत्वाचे ठरते, अशाप्रकारे कि कोणत्याही सर्व्हरवरील पेजला कुकी ॲक्सेस करता येऊ शकेल उदा: domain=www.asianlaws.net

कुकी आपण एका मशीनला किंवा संपूर्ण इंटरनेट डोमेनशी सल्लग्न करू शकतो. लक्षात ठेवा कि जर डोमेनसाठी जर कुकी ठरवायची असेल तर सर्व्हर त्या डोमेनचा मेंबर असला पाहिजे.

जर डोमेन पॅरामीटर स्पष्ट केला नसेल तर डिफाल्ट पद्धतीने पूर्ण डोमेन ज्यामुळे कुकी तयार झाली आहे तो वापरण्यात येईल.

५. सिक्युअर:

हे प्यरामीटर असे दर्शविते कि, हे प्यरामीटर असलेल्या कुकीचा फक्त सिक्युर सर्व्हर कंडिशन असतानाच वापर करयचा. उदा:SSL (secure socket layer)

11. कॉपीराईट इनफ्रीजमेंट

US Federal Bureau of Investigation **च्या मते**:

चोरी: हा एक पुरातन काळापासुन चालत आलेला गुन्हा आहे.

पण हे पाकीटमारी किंवा बँक लुटण्यासारखे नसुन, लोकांच्या कल्पना, शोध,किंवा सर्जनशील काम (बौद्धिक मालमत्ता) चोरण्याला कॉपीराईट इनफ्रीजमेंट म्हणतात. यामध्ये व्यापार तंत्र पासून सर्व काही आणि चित्रपट, संगीत मालकी उत्पादने आणि भाग सॉफ्टवेअर यांचा समावेश होतो.

हा वाढत्या डिजीटल तंत्रज्ञान आणि इंटरनेट फाईल शेअरिंग नेटवर्क बरोबरचा वाढता धोका आहे. इंटरनेट कॉपीराईट इनफ्रीजमेंट हा एक इनटेलअक्चुल प्रोपरटी चोरीचा गुन्हा आहे ज्यामुळे महत्वाचे सेक्युरिटी प्रश्न उभे ठाकले आहेत. जर एखाद्या व्यक्तीने दुसऱ्या व्यक्तीचे काम ज्यावर त्या व्यक्तीचा विशेष हक्क आहे, असे काम त्याच्या संमतीशिवाय वापरले किंवा वितरीत केले तर ती कॉपीराईट इनफ्रीजमेंट ठरेल. सामान्यतः इंटरनेट कॉपीराईट इनफ्रीजमेंट मध्ये अवैध पणे सिनेमा, गाणी आणि पायरेटेड सॉफ्टवेअर डाऊनलोड करणे यांचा समावेश होतो. कॉपीराईटने प्रोटेकटेड काम परवानगी शिवाय ओनलाईन पोस्ट करणे कॉपीराईट इनफ्रीजमेंट आहे.

उदाहरण: **समीर एक खुप चांगला कुक आहे, त्याने एक वेबसाईट** (smartcooking.com) **बनवून त्यावर त्याची रेसिपी दिलेली होती.सिद्धार्थने एक दुसरी वेबसाईट** (cookingsmart.com) **तयार करून त्यावर समीरच्या रेसिपी दिल्या होत्या, हि एक कॉपीराईट इनफ्रीजमेंट आहे**.

12. *क्ऱ्याप फ्लोडिंग*

क्ऱ्याप फ्लोडिंग म्हणजे ऑनलाईन मिडियावरती मूर्खपणाचे,वेडपटपणाचे सततचे पोस्ट करत राहणे जेणे करून इतर लोकांना महत्वाचे पोस्ट वाचण्यास न मिळता त्यांना फक्त हया वायफळ पोस्ट दिसत राहतील. या मागील उद्देश संकेतस्थळाची बँडविड्थ किंवा स्टोरेज वाया घालवणे हा असतो. क्ऱ्याप फ्लोडिंग हे स्वयंचालीत सॉफ्टवेअर वापरून देखील करता येते जे जास्त सोपे आहे. एखाद्यास नेटवर्क वरून घालवण्यासाठी त्यास त्याच्या डाटा रिसीव करण्याच्या क्षमते पेक्षा जास्त वेगाने मेसेजेस पाठवून हे करता येते जेणे करून त्यास "max text exceeded" **असा मेसेज दिसेल**.

13. *सायबर स्टोकींग*

सायबर स्टोकींग म्हणजे इंटरनेट, ईमेल किंवा इतर संवाद साधनांचा वापर करून एखाद्याची अडवणुक करणे (पिच्छा पुरवणे). साधारणपणे अशा प्रकारात वारंवार त्रास देणारे किंवा धमकावणाऱ्या वर्तनाचा समावेश होतो.उदाहरणार्थ एखाद्याचा पाठलाग करणे,एखाद्याच्या घरी किंवा कामाच्या ठिकाणी सतत भेट देणे, फोन करून त्रास देणे, लेखी स्वरुपात मेसेज पाठवणे किंवा मालमत्तेतेचे नुकसान करणे.

बऱ्याच स्टोकींग कायद्यानुसार व्यक्तीने सढळपणे पिडीत व्यक्तीस हिंसा करण्याचा धोका निर्माण केला पाहिजे, किंवा पिडीत व्यक्तीच्या कुटुंबास तसा अनुभव आला पाहिजे, तर ते स्टोकींग होईल.

सायबर स्टोकींग हे ऑनलाईन छळवणूक म्हणून देखील ओळखले जाते. सायबर स्टोकर हे इंटरनेटचा वापर करून निनावी स्वरुपात पीडितास त्रास देतात.

सर्वप्रथम १९९९ मध्ये US **सायबर स्टोकींग कायदा क्यालिफोर्निया राज्यात लागू झाला. बाकी राज्यात याचा समावेश त्यांच्या छळवणूक आणि अडवणुकीसाठी असलेल्या कायद्याच्या अंतर्गत आहे. फ्लोरिडा, २००३ मध्ये** HB **४७९ नुसार सायबर स्टोकींगवर बंदी घालण्यात आली.**

युनायटेड किंगडममध्ये दुर्भावनायुक्त संवाद कायदा (१९९८) नुसार सायबर स्टोकींग हा गुन्हा आहे.

भारतात सायबर स्टोकींग, माहिती तंत्रज्ञान कायदा कलम ६६अ अंतर्गत येते. त्या भागाचे नाव " संवाद साधनांद्वारे आक्षेपार्ह मजकूर पाठवणे इ." असे आहे.

माहिती तंत्रज्ञान कायदा कलम ६६अ अन्वये आक्षेपार्ह इलेक्ट्रोनिक संदेश पाठवणे हा गुन्हा आहे .

आक्षेपार्ह मजकुरात खालील प्रकार मोडतात:

१. मजकूर जो पूर्णतः आक्षेपार्ह आहे. (उदा. जो राग, द्वेष उत्पन्न करेल)

२. मजकूर जो धमकी वजा घातकी असेल.

३. मजकूर ज्या मधील माहिती चुकीची असेल , जिचा उद्देश राग , गैरसोय , अपमान , त्रास , द्वेष , शत्रुत्व , अडवणूक ,करण्याचा हेतूने पाठवलेला असेल .

४. मजकूर जो फसवण्याच्या किंवा दिशाभूल करण्याच्या उद्देशाने पाठवलेला असेल.

उदाहरण:

२००३ मध्ये कोणीतरी अमेरिकी नागरिक महिलेची वैयक्तिक माहिती ऑनलाईन डेटिंग सेवेद्वारे एका तिऱ्हाईक माणसाला पुरवल्या करणाने तिला सुरक्षा प्रदान करण्यात आली. जेंव्हा त्या माणसाने तिला संपर्ककरून असे सांगितले कि आपली एकदा lavalife.com या डेटिंग संकेतस्थळावर भेट झालीये, तेव्हा पिडीत व्यक्तीने तिची झालेली ओळख चोरी ओळखली. लगेचच तिला अशाच प्रकारचा आणखीन एका दुसऱ्या माणसाने संपर्क केला.

उदाहरण :

श्रीमती रितू कोहिलीयांनी पोलिसांकडे तक्रार दाखल केली कि, एक व्यक्ती ओळख चोरून (वापरून) www.mirc.com या संकेतस्थळावरून इतरांशी संपर्क साधत आहे.

श्रीमती रितू कोहिली यांनी परत एक तक्रार दाखल केली कि, ती व्यक्ती त्याच्या नावाने संपर्कच साधत नाहीतर त्यांचा पत्ता इतरांना देतो आणि इंटरनेटवरती अश्लील भाषेत संभाषण करत आहे. तिच व्यक्ती मुद्दामहून श्रीमती रितू कोहिलीचा फोन नंबर इतरांना देऊन त्यांना वेळीअवेळी फोन करण्यासाठी सांगत होता. त्यामुळे श्रीमती रितू कोहिलीना तीन दिवसात वेगवेगळ्या ठिकाणांवरून ४० फोन आले. ज्यामुळे त्यांचे मानसिक स्वास्थ्य बिघडले त्यामुळे त्यांनी तक्रार दाखल केली.

कालांतराने IP अड्रेसचा मागोवा घेऊन पोलिसांनी त्या व्यक्तीस शोधले , त्याचे नाव मनीष कथुरिया होते, मनीषने गुन्हा कबुल केला व त्यास अटक झाली .

उदाहरण:

क्यालिफोर्निया (USA) मधील प्रथम यशस्वी सायबर स्टोकींग खटला हा ५० वर्षीय माजी सुरक्षा रक्षका विरुद्ध होता. ज्याने त्याचे प्रेम नाकारणाऱ्या महिलेस बलात्काराचा अनुभव घ्यायचा आहे असे इंटरनेटवरती प्रसिद्ध केले. २८ वर्षीय पीडितास त्याने इंटरनेट चॅट रूम आणि ऑनलाईन बुलेटीन बोर्डचा वापरकरून दहशत बसवली होती. त्याच बरोबर त्याने पीडिताचा फोन व पत्ता ऑनलाईन पोस्ट केला व ती तिच्या वरच्या बलात्काराची कल्पना करत असते असे सांगितले . यामुळे कमीतकमी सहावेळा मध्य रात्री तिच्या दरवाज्यावर काही माणस आली आणि ते म्हणत होते कि त्यांना तिच्यावर बलात्कार करायचा आहे.

उदाहरण:

स्यान दिएगो विद्यापीठाच्या पदवीधराने विद्यापीठाच्या पाच विद्यार्थिनींना एक वर्षापेक्षा जास्त काळ इंटरनेटवरती दहशतीत ठेवले होते. पीडिताना शेकडो हिंसेचे आणि धमकीचे ईमेल आले, काही वेळेस दिवसातून चार ते पाच मेसेज यायचे. ज्या विद्यार्थाने गुन्हा कबूल केला

त्याने पोलिसांना सांगितले कि त्यांनी असे केले कारण कि त्याला असे वाटले कि त्यामुली त्याच्याकडे पाहून हसत होत्या त्यामुळे तो इतरांच्या चेष्टेचा विषय बनत होता.

सत्य परिस्थिती अशी होती पीडित विद्यार्थिनी त्यास कधीच भेटलेल्या नव्हत्या.

उदाहरण :

२००५ मध्ये म्यासेचुसेत्स (USA), एका अल्पवयीन मुलास पीडित व्यक्तीचे अंदाजे १ मिलीयन डॉलर नुकसान करण्यासाठी दोषी ठरवण्यात आले. १५ महिने कालावधीच्या वर तो इंटरनेट आणि टेलीफोन सर्व्हिस प्रोव्हायडर यांना हॅककरून एकाची वैयक्तिक माहिती चोरून इंटरनेटवर पोस्ट केली , आणि अनेक शाळांना बॉम्ब हल्ल्याच्या धमक्या पाठवल्या होत्या.

14. *सायबर टेररीझम*

कॉम्प्युटर गुन्ह्यानी अविश्वसनीयरीत्या संपूर्ण मानवजातीला धक्का पोहचवला आहे. कॉम्प्युटर व्हायरस,वोर्म,ट्रोजन, ई फ्रोड इत्यदीमुळे जगात खळबळ माजली आहे. तथापि, या सर्वात जास्त धोका आहे तो सायबर टेररीझमचा

सायबर टेररीझम म्हणजे, सायबर स्पेस मध्ये पूर्वनियोजित खीळ घालण्यासाठीच्या किंवा घात करण्यासाठीची कृती जिचा उद्देश सामाजिक, वैचारिक धार्मिक हेतू साध्य करणे, किंवा इतर समान उद्देश,किंवा एखाद्या व्यक्तीस अशा कृती करण्यासाठी धमकावणे.

हि व्याख्या माद्रिद स्पेन २००२ मध्ये झालेल्या वर्ड कॉंग्रेस फोर इनफोरमेटीक्स अॅन्ड लॉ II , **सायबर टेररीझम इन ग्लोबल कॉनटेक्स्ट या लेखात रोहास नागपाल**, Asian School Of Cyber Laws **चे अध्यक्ष यांनी केलेली आहे**.

उदाहरण:

२६ नोव्हेंबर २०१० रोजी इंडियन सायबर आर्मी नावाच्या संघटनाने मुंबईवरील अतिरेकी हल्ल्याचा बदला म्हणून पाकिस्तान आर्मी, विदेश मंत्रालय,वित्त मंत्रालय, पाकिस्तान कॉम्प्युटर ब्युरो , इत्यादींच्या वेबसाईट हॅक केल्या.

उदाहरण:

१९९६ मध्ये एका कॉम्प्युटर हॅकर ने जो व्हाईट सुपरमासिस्त चळवळीशी संबंधित होता त्याने एक US **स्थित इंटरनेट सर्व्हिस प्रोव्हाडरची सेवा तात्पुरती बंद पाडली,आणि त्याच्या रेकॉर्ड यंत्रणेतील काही भागचे नुकसान केले**.

इंटरनेट सर्व्हिस प्रोव्हाइडरने त्यास सर्व जगाला ISP**च्या नावाने वर्णद्वेषाचे मेसेज पाठवण्यापासून रोखण्याचा प्रयत्न केला होता**. **हॅकर ने पुढील प्रमाणे एक धमकीचा मेसेज हि पाठवला** "you have yet to see true electronic terrorism. This is a promise." **होता**.

उदाहरण:

१९९८ मध्ये १२ वर्षीय मुलाने यशस्वीरीत्या USA **तील अरिझोना राज्यातील साल्ट नदीवरचे रूझवेल्ट धरच्या नियंत्रण यंत्रणेत हॅक केले होते**. **त्याने जर धरणाची दारे उघडली असती तर पुरामुळे कमीत कमी १ मिलियन लोकांचा जीव धोक्यात आला असता**.

उदाहरण :

२००५ मध्ये US **सुरक्षा सल्लागाराच्या मते हॅकर लोक** US **च्या पॉवर ग्रीडला लक्ष्य करत होते आणि ते इलेक्ट्रोनिक कंट्रोल यंत्रणेपर्यंत पोहचण्यात यशस्वी झाले होते**.

उदाहरण:

१९९७ मध्ये ३५ कॉम्प्युटर विशेषज्ञानी १९०० विविध वेबसाईट वरती असलेल्या हॅकिंग टूल्स वापरून US **पॉवर ग्रीडचा मोठा भाग बंद पडला होता. तसेच त्यांनी होनलुलु मधील पॅसिफिक कमांडची कंट्रोल यंत्रणा बंद पडलेली होती**.

उदाहरण:

२००० साली Asian School Of Cyber Laws **वर नेहमी एक हॅकटीविस्ट डिसट्रीब्युटेड डिनायाल ऑफ सर्व्हिसचा अटॅक करत होता जो राईट टु पोनोग्राफीचा प्रसार करत होता**. Asian School Of Cyber Laws **ने पोनोग्राफीच्या विरोधातील आंतरराष्ट्रीय मोहिमेचे नेतृत्व केले होते**.

उदाहरण :

२००१ मध्ये युस - चीन यांच्या खालावलेल्या संबंधामुळे, चीनी हॅकरनी कोड रेड व्हायरस रिलीज केला,या व्हायरसने जगातील लाखो कॉम्प्युटर इन्फेक्ट केले,आणि या कॉम्प्युटरचा वापर युस वेबसाईटवर डिनायाल ऑफ सर्व्हिसचा अटॅक करण्यासाठी वापर केला. यात मुख्यत्वे व्हाईट हाउसच्या वेबसाईटचा समावेश होता.

उदाहरण:

२००१ मध्ये हॅकरनी युस डिपार्टमेंट ऑफ जस्टीसमध्ये प्रवेश केला आणि डिपार्टमेंटचे चिन्ह स्वस्तिक या चिन्हाने बदलले, आणि युनायटेड डिपार्टमेंट ऑफ इनजस्टीस असा नावात बदल करून अनेक अश्लील छायाचित्रे वेबसाईटवरती पोस्ट केली.

15. सायबर वारफेअर

म्याकफी व्हरचुअल रिपोर्ट २००७ च्या मते, १२० देश इंटरनेटचा एक हत्यार म्हणून वापरून आर्थिक क्षेत्र, सरकारी कॉम्प्युटर सिस्टीम आणि साधने यांना लक्ष्य करण्यासाठी वेगवेगळे मार्ग शोधून काढत आहेत. सायबर वारफेअर म्हणजे कॉम्प्युटर आणि इंटरनेटचा वापर करून सायबर स्पेसमध्ये युद्ध करणे.

म्याकफी व्हरचुअल क्रिमीनोलोजी रिपोर्टच्या म्हणण्यानुसार आजकाल सरकार आणि सरकारशी सल्लग्न गट इंटरनेटचा वापर इतर देशाच्या महत्वाच्या राष्ट्रीय पायाभूत सुविधांवर हेरगिरी आणि सायबर अटॅक करण्यासाठी वापर करीत आहेत.

उदाहरण:

२००९ मध्ये GhostNet नावाच्या सायबर स्पाय नेटवर्कने १०० पेक्षा जास्त देशातील सरकारी आणि खाजगी संस्थाची गोपनीय माहिती मिळवली, GhostNet हि संस्था चीनची असल्याचे कळले होते,तरी चीनने हि जबाबदारी नाकारली.

GhostNet कसे काम करते हे Wikipedia ने खालील प्रकारे स्पष्ट केले आहे.

लक्ष्य असलेल्या संस्थाना त्यांच्या निगडीत विषयाशी संबंधित ईमेल्स पाठवले जातात,या ईमेलमध्ये मालीशीयस अटॅचमेंट असते, जी मेल ओपन केल्यावर एक ट्रोजन त्या कॉम्प्युटरमध्ये पसरवते. हा ट्रोजन तो कॉम्प्युटर चीन मधील कंट्रोल सर्व्हर कडून कमांड घेण्यासाठी त्यास जोडतो, जो कि बहुतकरून चीनमध्ये असेल. मग तो इन्फेक्ट झालेला कॉम्प्युटर त्या कंट्रोल सर्व्हर कडून आलेलली कमांड राबवेल. कंट्रोल सर्व्हर कडून आलेल्या कमांडनुसार GhOst Rat नावाचा ट्रोजन डाऊनलोड करेल,जो अटॅक करणाऱ्यास मायक्रोसोफ्ट विंडोज असलेल्या कॉम्प्युटरचा संपूर्ण ॲक्सेस मिळवून देईल.मग अशा प्रकारे कॉम्प्युटरचा संपूर्णपणे ताबा मिळवता येतो, त्यावरून कॅमेरा चालू करून हेरगिरी सुद्धा करता येते.

16. डाटा डिडलींग

कॉम्प्युटर गुन्ह्यातील सर्वात सामान्य प्रकारचा गुन्हा म्हणजे डाटा डिडलींग, म्हणजे अवैध किंवा अनधिकृत पणे डाटामध्ये बदल करणे. अशा प्रकारचे बदल डाटा इनपुट करताना किंवा आऊटपुट अगोदर होत असतो. डाटा डिडलींगचे बँक, पेरोल, इनव्हेनट्री, क्रेडीट रेकॉर्डस इ. वर परिणाम झालेले आहेत. डाटा डिडलींगमध्ये आपण डाटा इनपुट करण्याअगोदर किंवा नंतर त्यात मजा किंवा फायद्यासाठी बदल करतो. उदा: मार्काची अदलाबदल करणे, क्रेडीट रेटींग बदलणे, ऑडिट किंवा बँकेचे रेकॉर्ड बदलणे इ. गोष्टींचा यात समावेश होतो.

कॉम्प्युटर गुन्हा करण्याचा हा एक अतिशय सोपा मार्ग आहे, यासाठी आपणास काही विशेष येण्याची जरूर नसते, तरी पण तुम्ही आरामात हे करू शकता ज्याचे मोठे परिणाम होऊ शकतात.

उदाहरण:

१९९६ मध्ये NMDC **इलेकट्रीसीटी फ्रोड घडला होता. दिल्ली म्यनुसिपल कौन्सिल इलेकट्रीसीटी बिलच्या अकाऊटींग आणि पावतीसाठी कॉम्प्युटर नेटवर्कचा वापर करत होते. पैसे गोळा करण्याचे काम आणि सर्व बँकेचे व्यवहाराचे काम एका खाजगी कंत्राटदारास दिले**

होते, जो एक कॉम्प्युटर प्रोफेशनल होता. त्याने गैरमार्गाने डाटा डिडलींगचा वापर करून कमी पावत्या दाखवून खूप पैसे मिळवले.

उदाहरण:

ऑकलंड, USA तील डिपार्टमेंट स्ट्रोअर मधील किबोर्ड ओप्रेटरने काही सामानांचा डिलिव्हरी पत्ता बदलून हजारो डॉलर्सचे समान लंपास केले.

उदाहरण:

USA मधील अरिझोना वेटरनस मेमोरिअल कोलीझिंअमच्या तिकीट क्लार्कने बास्केट बॉल सामन्याची तिकीट पुर्ण किमतीस विकली पण, तिने कॉम्प्युटरवर

कोडचा वापर करून ह्या व्यवहाराची नोंद फक्त निम्म्या पैशाचीच केली.

उदाहरण:

साहिलच्या कॉम्प्युटरवर कंपनीच्या मिटिंगसाठीचे एक प्रेझेनटेशन होते. रोहन, साहिलवरती जळत होता व त्याला काहीतरी इजा करण्याच्या प्रयत्नात होता. त्यामुळे त्यानी साहिलच्या प्रेझेनटेशनमध्ये जंक डाटा वापरून बदल केले. ज्यामुळे साहीलला लाजीरवाण्या प्रसंगास सामोरे जावे लागेल आणि त्याची नोकरी धोक्यात आली.

उदाहरण:

हिंदी चित्रपट ३ इडीयटस मध्ये एका भाषणा मधील "चमत्कार" हा शब्द "बलात्कार" ने बदला होता.

17. *डाटा लिकेज*

डाटा लिकेज म्हणजे अनियंत्रित, अनाधिकृतपणे वर्गीकृत किंवा सुरक्षित माहिती अविश्वासर्ह माध्यमातून प्रसारित करणे. याप्रकारास सहेतुक माहिती उघड करणे, डेटा उल्लंघन(ब्रीच) आणि डाटा गळती अशा विविध नावाने हि ओळखले जाते. हा प्रकार संघटीत गुन्हेगारांकडून नियोजित हल्ला पासून राष्ट्रीय सरकार कडून कॉम्प्युटर आणि इतर मीडियाच्या हाताळणीमध्ये झालेला हलगर्जीपणा या साठी कारणीभूत असू शकतो.

डेटा उल्लंघन(ब्रीच) मध्ये आर्थिक माहिती,वैयक्तिक आरोग्य विषयक माहिती,किंवा इंटेलअॅकचुअल प्रोपर्टीचा समावेश असू शकतो.

iPAD साठी असलेल्या एक app नावाच्या application ने वैयक्तिक माहिती लिक केल्यामुळे दोन स्वतंत्र गट Apple विरोधात दावा करत आहेत.

18. डेफमेशन(अब्रुनुकसानी)

एखाद्या व्यक्तीची प्रतिष्ठा कधी कधी त्याच्या भौतिक मालमत्ते पेक्षा अधिक मौल्यवान असते. डेफमेशन म्हणजे एखद्या व्यक्तीच्या अब्रूस पोहचवलेली इजा होय. जर हि अबुनुकसानी कॉम्प्युटर किंवा इंटरनेटचा वापर करून झाली तर त्यास सायबर डेफमेशन असे म्हणतात. उदा: समीर पूजाबद्दल अब्रुनुकसानीकारक मजकूर वेबसाईटवर प्रकाशित करतो किंवा अब्रुनुकसानीकारक मजकूर असलेले ईमेल पूजाच्या मित्रांना पाठवतो.

डेफमेशनचे तीन महत्वाचे घटक आहेत:

१. ते वक्तव्य चुकीचे आणि बदनामीकारक असले पाहिजे,

२. ते वक्तव्य पीडित व्यक्तीशी संबंधित पाहिजे,

३. ते वक्तव्य प्रकाशित झाले पहिजे.

उदाहरण :

राहुल एक ब्लॉगमध्ये खोटा लेख लिहितो,ज्यात तो असे म्हणतो कि सोनियाच्या खुनासाठी सुमन जबाबदार आहे. ह्यामुळे सुमनची बदनामी झाली,इथे राहुलने सायबर डेफमेशन गुन्हा केला आहे.

उदाहरण:

Tuile **एक ऑनलाईन निनावी ग्रुप आपल्या वेबसाईट वरील मेसेज बोर्ड वरती** ROW & ROW **कंपनी बद्दल खोटी माहिती पोस्ट करतो,ज्यामुळे त्या कंपनीच्या शेअरची किंमत एकदम कमी होते आणि काही महत्वाचे करार रद्द होतात, हे सायबर डेफमेशन आहे.**

उदाहरण:

अभिषेक, या किशोरवयीन विद्यार्थ्यास सोशल नेटवर्कींग साईटवर एका मुलीची प्रतिमा डागाळल्यामुळे ठाणे पोलिसांनी त्यास अटक केली होती. अभिषेकने त्या मुलीचे नाव आणि फोन नंबर सहित प्रोफाईल तयार केले होते. ते प्रोफाईल अशा प्रकारे होते कि त्यावर अनेक जणांच्या असभ्य प्रतिक्रीया आल्या होत्या. ठाणे पोलिसांनी हा प्रोफाईल तयार करण्यासाठी वापरलेल्या खोटॅ ईमेल आयडीवरून अभिषेकला पकडले होते.

उदाहरण:

बॉम्बे हायकोर्टाच्या औरंगाबाद खंड पीठाने एका तरुण वकिलाने दाखल केलेल्या जनहित याचिके संदर्भात Google.com **ला नोटीस पाठवली. मिरोस्लाव स्तन्कोविक च्या** "We hate India " **या समुदाया विरोधात त्या वकिलाने आक्षेप घेतला होता. या समुदायाने इंडियाचा जळालेला ध्वज प्रदर्शित केला होता.**

उदाहरण:

एका अज्ञात व्यक्तीने दिल्लीतील शाळेतल्या मुलीचा फोन नंबर आणि अश्लील फोटो पोस्ट केले होते.'सेक्स शिक्षक' सारख्या नावाने काही नावे प्रोफाइल वर पोस्ट केली होती. मुलीच्या कुटुंबास या संदर्भात घाणेरडे फोन येऊ लागल्यावर हे प्रकरण उघडकीस आले. दोन अज्ञात व्यक्ती तर तिच्या घरी पोहोचल्या होत्या ,त्यांचे म्हणणे होते कि त्यांना मुलीने ओर्कुटवरून निमंत्रण दिले आहे.

19. DOS / DDOS

यामध्ये अस्तित्वात असलेल्या कॉम्प्युटर रिसोर्सेस पेक्षा जास्त मागणी करतात. ज्यामुळे रिसोर्सेस क्रॅश होऊन अधिकृत वापरकर्त्यांना सर्व्हिस नाकारण्यात येते. हे करण्यासाठीचा एक साधा मार्ग म्हणजे कॉम्प्युटरला बाह्य संवाद मागणी इतकी करयची कि तो अधिकृत मागणीस प्रतिसाद देण्यास असमर्थ ठरेल.

DoS हल्ले साधारणतः खालील प्रकारे अंमलात आणता येतात:

१. लक्ष्य असलेल्या कॉम्प्युटरला रिसेट करणे किंवा त्याच्या रिसोर्सेसचा अशा प्रकारे वापर करयचा कि तो त्याची नियोजित कामे करूच शकणार नाही.

२. संवाद माध्यमात अडथळा निर्माण करून संवाद बंद पाडणे.

DoS हल्ल्याचा अजून एक प्रकार म्हणजे डिसट्रीब्युटेड डिनायाल ऑफ सर्व्हिस हल्ला, ज्यात हल्लेखोर अनेक असतात आणि ती भौगोलिकदृष्टया खूप ठिकाणी पसरलेले असतात.

उदाहरण:

फेब्रुवारी २००० मध्ये एक डिसट्रीब्युटेड डिनायाल ऑफ सर्व्हिस हल्ला झाला होता ज्यामुळे बऱ्याच प्रसिद्ध वेबसाईट yahoo.com, amazon.com आणि cnn.com बंद पडल्या होत्या.

उदाहरण:

२००७ मध्ये १२५ पेक्षा जास्त वेगवेगळे पण समन्वित डिनायाल ऑफ सर्व्हिस हल्ले इस्टोनियाच्या सायबर इन्फ्रास्टकचर वरती झाले होते. हया हल्ल्याचा संबंध सरकारच्या सोविएत काळातील युद्ध मेमोरिअल शहरातून हटवण्याच्या निर्णयाशी होता. असा संशयित अंदाज होता कि हे हल्ले रशिअन हॅकरनि घडवून आणले आहेत, ज्याचा परिणाम बरेच दिवस राहिले होते.

20. DNS ***पॉयझनींग***

डोमेन नेम सिस्टीम (DNS) **पॉयझनींग हल्ला, यास** DNS **स्पुफींग असेही म्हणतात, यात हल्लेखोर पीडित व्यक्तीस त्याने टाइप केलेल्या वेबसाईट ऐवजी एका दुसऱ्याच साईटला रिडायरेक्ट करतो.** DNS **बद्दल अधिक माहितीसाठी ॲपेनडीक्समध्ये** IP **अड्रेस,**DNS **नावाचा भाग पहा.**

उदाहरणार्थ:

एखाद्याने आपल्या ब्राउझरमध्ये www.google.com **असे टाइप केले, पण तो गुगलवरती जाण्याऐवजी दुसऱ्याच एका गुगल सारख्या दिसणाऱ्या बनावट वेबसाईटला डायरेक्ट होतो ज्याचे नियंत्रण हल्लेखोर करत असतो. हे सर्व हल्लेखोर गुगलसाठी असलेला** IP **अड्रेस ऐवजी खोटा** IP **अड्रेस वापरून करतो. थोडक्यात** DNS **पॉयझनींग हल्ला म्हणजे** DNS **सर्व्हर बरोबर चलाखी करून चुकीच्या दिशेने ट्राफिक पाठवून चुकीचे** DNS **कंटेंट जोडणे.**

कॅशे पॉयझनींग वापरून हल्लेखोर DNS **मध्ये खोटा इंटरनेट डोमेन अड्रेस नोंद करतो, आणि जर हा खोटा अड्रेस स्वीकरला गेला तर कॅशे पॉयझनींग होते . मग त्या पुढील सर्व्हरसाठी आलेल्या रिक्वेस्ट ह्या हल्लेखोराकडून हाताळल्या जातील. जो पर्यंत खोटी नोंद सर्व्हर कडून स्वीकारली जाते तो पर्यंत ब्राउझर आणि ईमेल सर्व्हर आपोआप बनावट**

अड्रेसचा वापर करतील. ज्यामुळे वापरकर्त्याचा कॉम्प्युटरवर वॉर्म, स्पायवेअर, हॅकींग टुल इ. डाऊनलोड करता येईल.

उदाहरण:

Roar इंटरनेटवरील एक गुन्हेगारी टोळी,बँक ऑफ अनगुरियाच्या वेबसाईटचा IP अड्रेस बदलून DNS पॉयझनींग केले. बँकेचे ग्राहक त्यामुळे बँकेसारख्या दिसणाऱ्या वेबसाईट कडे वळवले गेले. आणि या बनावट वेबसाईट वरून बँकेच्या ग्राहकांच्या कॉम्प्युटरवर एक ट्रोजन डाऊनलोड करण्यात आला. अशाप्रकारे बँकेच्या ग्राहकांच्या सर्व गोपनीय डाटा Roarच्या हाताला लागला.

21. ***इस्टर एग्ज***

सॉफ्टवेअर टेस्टिंगचे अपयश आपण इस्टर एग्ज आरकाइव्ह (www.eeggs.com) **वर सहजपणे पाहू शकतो. आरकाव्हनुसार इस्टर एग्ज हे एक गुपित वैशिष्ठ किंवा एक नवलाई जी कि प्रोग्रामर आपल्या सॉफ्टवेअरमध्ये ठेवत असतो. थोडक्यात हि कुठलीही लपवलेली गोष्ट असू शकते जी निर्मात्या कडून त्याच्या वैयक्तिक कारणांसाठी ठेवलेली असते. ह्यामध्ये डेवलपरची लिस्ट, कमांडस,जोक,मजेशीर ॲनिमेशन यापैकी काहीही असू शकते.**

खऱ्या इस्टर एग्ज खालील निकष पूर्ण करणे आवश्यक आहे:

१. ते अलिखित, लपवलेले आणि अस्पष्ट असावे.

इस्टर एग्ज उत्पादनाच कायदेशीर वैशिष्ठ किंवा त्याचा सढळ भाग असू शकत नाही. इस्टर एग्ज त्यांच्या संदर्भामुळे गटात न बसणारे ठरतील,किंवा निर्मात्याला त्याचे विशेष महत्व वाटत असल्यामुळे ते करमणूक म्हणून त्यांचा वापर करतील.

२. त्याचं पुनरुत्पादन करता आले पाहिजे.

प्रत्येक वापरकर्त्याला सारख्या उत्पादना किंवा मिश्र उत्पादना बरोबर, त्याच प्रकारच्या सूचना देऊन सारखेच निकाल मिळाले पाहिजेत.

३. ते निर्मात्याकडून वैयक्तिक कारणांसाठी वापरले गेले पाहिजे.

कोणत्यातरी उद्देशासाठीच एग्ज वापरले गेले पाहिजे. आणि त्या मधून उत्पादन चांगले करण्याबरोबरच निर्मात्याचा वैयक्तिक फायदा झाला पाहिजे.

व्याख्येप्रमाणे इस्टर एग्ज हे करमणुकीसाठी आणि निरुपद्रवी असले पाहिजे. पण काही वेळेस इस्टर एग्ज हे उपद्रव करू शकतात. उदा: कदाचित प्रोग्रामरच्या इस्टर एग्ज कोडमध्ये बग असू शकतो.,आणि काही परिस्थिती मध्ये हा कोड प्रोग्राम किंवा पूर्ण कॉम्प्युटर क्रयाश करू शकतो.

काही इस्टर एग्ज:

१. विंडोज कॉम्प्युटरवरील सोलीटइर गेम जिंकण्यासाठी फक्त Alt + Shift + २ प्रेस करा.

२. मायक्रोसोफ्ट वर्ड मध्ये एक नवीन डोक्यूमेंट ओपन करा आणि खालील मजकूर टाइप करा:

=rand(200,99)

आणि इंटर प्रेस करा. काही क्षणातच आपल्याला शेकडो पेजेस "The quick brown fox jumps over the lazy dog" या वाक्याने भरलेले दिसतील.

इस्टर एग्ज हा एक ट्रोजन हॉर्सचा प्रकार आहे. सॉफ्टवेअर डेव्हलपर, सॉफ्टवेअर टेस्टिंग आणि क़्वालिटी इंटरनॅशनल टीमला

चकवून इस्टर एग्जचा वापर करू शकतात,त्याच प्रमाणे ते ट्रोजन हॉर्स किंवा बफर ओवरफ्लो हि घडवून आणू शकतात यात काही शंका नाही.

खरेतर, हल्लेखोर मेन प्रोग्राम मधील इस्टर एग्जमध्ये एक बॅकडोर एम्बेड करू शकतात. या प्रमाणे एखादा दुर्भावनायुक्त डेव्हलपर किंवा टेस्टर कुणाच्याही नकळत प्रोडक्ट कोड मध्ये अशी कार्यक्षमता लपवून ठेऊ शकेल आणि तो प्रोडक्ट रिलीज सुद्धा होईल.

22. *ईमेल स्पुफिंग*

स्पुफ्ड ईमेल हा ज्या स्रोतापासून आलेला आहे असे दिसत असते ,त्यापेक्षा वेगळ्या ठिकाणहून आलेला असतो. उदा: पूजाचा ईमेल अड्रेस pooja@asianlaws.org **आहे. तिचा माजी प्रियेकर समीर तिचा ईमेल अड्रेस स्पुफ करून तिच्या जवळच्या व्यक्तींना अश्लील मेसेज पाठवतो.जसे कि हा ईमेल स्पुफिंगमुळे पूजाने पाठवला आहे असे दिसत असल्याने, तिचे मित्र यावर आक्षेप घेऊ शकतात आणि तिचे त्यांच्या बरोबर कायमचे संबंध बिघडू शकतात.**

उदाहरण:

एका अमेरिकन केसमध्ये, अल्पवयीन मुलाने काही कंपन्या बद्दल खोटी माहिती पसरवली ज्यामुळे त्यांच्या शेअरचे भाव कोसळले, ज्यांचे शेअर त्यानी नुकतेच विकले होते, अशा प्रकारे त्याने लाखो रुपये कमावले.

उदाहरण:

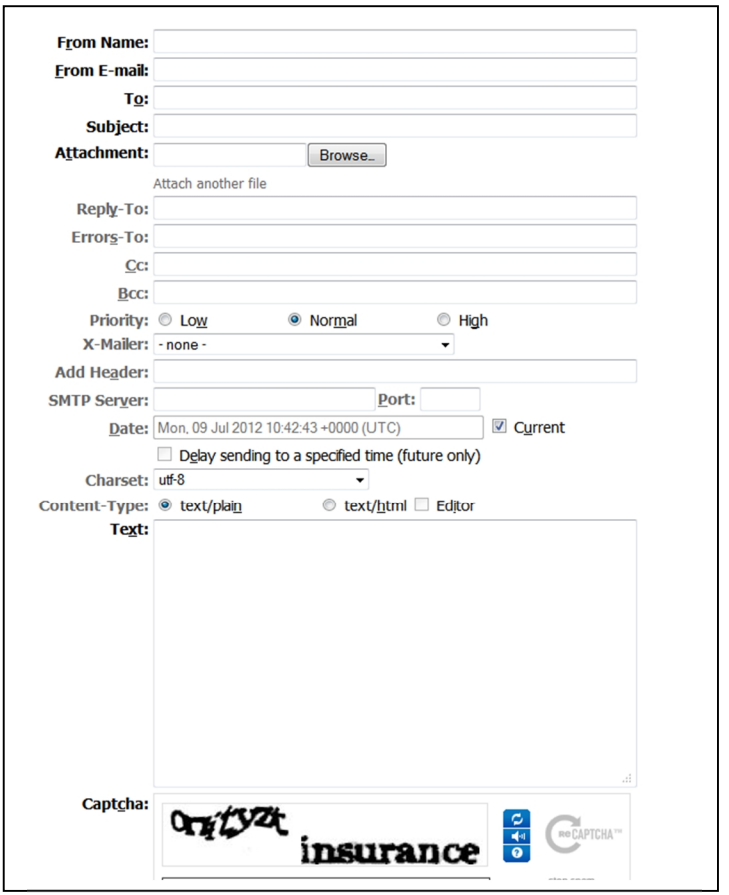
ग्लोबल ट्रस्ट बँकेच्या भारतातील शाखेतुन अनेक लोकांनी आपले पैसे काढयला सुरवात केली आणि आपले खाते बंद कारायला लागले.या गोष्टीचा तपास केल्यावर असे समजले कि कोणीतरी या खातेदारांना बँकेची आर्थिक स्थिती खुप वाईट आहे आणि ती कधीही बंद पडू शकते

असा एक स्पुफ मेसेज पाठवला होता आणि तो स्पुफ्ड ईमेल बँकेकडून आल्याचे भासवले गेले होते. स्पॅमचे वितरक स्पुफिंगचा वापर करतात, कधी कधी ईमेल प्राप्तकर्ता ते ईमेल्स ओपन हि करतो आणि क्लिक हि करतो ज्यामुळे संवेदनशील माहिती मिळवली जाऊ शकते.

http://emkei.cz **प्रसिद्ध ऑनलाईन स्पुफिंग वेबसाईट आहे.**

एक प्रसिद्ध ईमेल स्पुफिंग वेब साईट: http://emkei.cz

FAKE MAILER


From Name:
From E-mail:
To:
Subject:
Attachment:
Browse...
Attach another file
Reply-To:
Errors-To:
Cc:
Bcc:
Priority: Low Normal High
X-Mailer: - none -
Add Header:
SMTP Server:
Port:
Date: Mon, 09 Jul 2012 10:42:43 +0000 (UTC)
Current
Delay sending to a specified time (future only)
Charset: utf-8
Content-Type: text/plain text/html Editor
Text:
Captcha:
insurance

23. अतिरेक्यांकडून एनक्रिप्शनचा वापर

अतिरेक्यांकडून एनक्रिप्शनचा वापर:

एनक्रिप्शन, हाय फ्रिक़्वेनसी एनक्रिपटेड व्होइस/ डाटा लिंक्सचा वाढता वापर सध्या त्रासदायक प्रकार होऊन बसला आहे, यासाठी प्रिटी गुड प्रायव्हसी (PGP) एनक्रिप्शन सॉफ्टवेअरचा अतिरेकी आणि संघटीत गुन्हेगारीतील लोकांकडून याचा वापर केला जातो. स्ट्रॉंग एनक्रिप्शन गुन्हेगाराचा चांगला मित्र आणि पोलिसांचा हाडवैरी आहे.

जर गुन्हेगारांनी ५१२-बीटचे एनक्रिप्शन वापरले तर ते ब्रूट फोर्स हल्ला करून तोडायला किती वेळ लागेल?

समजा विश्वातील प्रत्येक अणु कॉम्प्युटर सारखे काम करण्यास सक्षम झाला आणि दर सेकंदाला २३०० किज तपासल्या तरी त्याला २१६२ हजारांवर वर्षे १% चे काम पूर्ण करण्यासाठी लागतील.

उदाहरण:

१९९५ मध्ये न्युयॉर्क मध्ये सबवे सिस्टममध्ये फायर बॉम्ब उडवल्या बद्दल ९४ वर्षाची कारावासाची शिक्षा झाली होती, त्यांनी एनक्रिप्शनसाठी कॉम्प्युटरवर स्वतःच एक अल्गोरिदम लिहिला होता.

उदाहरण:

काही नावाचे कारखानदार खालील गोष्टी वापरण्यासाठी प्रसिद्ध आहेत:

१. त्यांचे फोनवरील संभाषण लपवण्यासाठी अत्याधुनिक एनक्रिप्शनचा वापर करत होते.

२. चुकीचा आवाज काढणारे रेडिओ

३. व्हिडीओ फोन जे फोन करणाऱ्याचे व्हिज्युअल अथॉनटीकेशन करतात.

४. अशी साधने जी मोडेमचे ट्रान्समिशन ब्लोक करतात.

उदाहरण:

१९९७ मध्ये बोलिव्हियाच्या अतिरेकी संघटनेनी ४ अमेरिकी आर्मीतील लोकांचा खून केला होता. त्यांच्या लपण्याच्या एका जागेवरती छापा घातल्यावर सिमेट्रिक एनक्रिप्शननी एनक्रिप्ट केलेली माहिती अतिरेक्यांकडून सापडली. १२ तासाच्या ब्रुट फोर्स हल्ला केल्यानंतर ती माहिती डिक्रिप्ट झाली,हे बोलिव्हियाच्या इतिहासातील सगळ्यात मोठ्या अतिरेक्यास अटक सत्र घडले.

उदाहरण:

डच संघटीत गुन्हेगार टोळी PGP आणि PGPfone चा वापर त्यांचे संवाद एनक्रिप्ट करण्यासाठी करत होते.सुरक्षित उपकरण असलेला पाल्मटॉप कॉम्प्युटरचा हि ते वापर करत होते. इंटरनॅशनल डाटा एनक्रिप्शन अल्गोरीदम (IDEA) असलेल्या एका डच सॉफ्टवेअर कंपनीचे प्रोडक्ट एनक्रिप्शसाठी वापरत होते.

१९९५ मध्ये अमस्टरडॅम पोलिसांनी एका संघटीत गुन्हेगारा कडून एक कॉम्प्युटर जप्त केला होता, त्यात एनक्रिप्टेड पार्टीशन होते जे १९९७ मध्ये रिकव्हर झाले.

24. ई शॉपलिफ्टिंग:

दुकानामध्ये प्रदर्शनासाठी ठेवलेली वस्तु चोरण्याला शॉपलिफ्टिंग असे म्हणतात. ई शॉपलिफ्टिंग म्हणजे इलेक्ट्रोनिक स्टोरमध्ये प्रदर्शनासाठी ठेवलेली वस्तु चोरणे. एक इ-शॉप, बिजनेस लॉजिक आणि टेकनोलॉजी यांच्या मिश्रणातून तयार झालेले असते. टेकनोलॉजी मधील दुर्बलपणा शोधुन हॅकर लोक वस्तु किंवा सेवा कमी दरात पदरात पाडून घेतात किंवा फुकट हि मिळवतात.

इ-शॉप मध्ये असणाऱ्या काही प्रमुख दुर्बलता:

१. खालच्या दर्जाचे इनपुट प्रमाणिकरण(व्हयालिडेशन):

याचा अर्थ असा कि युझरकडून केलेले इनपुट व्यवस्थित पणे न तपासणे. युझर त्याचे युझर नेम टाइप न करता एखादा कोड इनपुट करून सिस्टीमचा चुकीचा वापर केला जाऊ शकतो.

२. कुकीजचा अनुचित वापर:

याचा अर्थ असा कि कुकीज हया दुर्बल असतात आणि त्याचा गैरवापर केला जाऊ शकतो. या प्रकारे हॅकर कुकीज मधल्या महत्वाच्या व्हयाल्यु बदलू शकतो.

३. अयोग्य प्रकारे सेशन किंवा स्टेट ट्र्याक करणे:

याचा अर्थ सेशन किंवा स्टेट ट्र्याक करण्यासाठी वापरण्यात येणारी पद्धत अपर्याप्त असते.

४. क्लायंट साइड स्क्रिप्ट मधील कमकुवत पणा:

क्लायंट साइड स्क्रिप्ट हे वेब वरील असे कॉम्प्युटर प्रोग्राम आहेत जे युझरचा वेब ब्राउझर एक्झिक्युट करत असतो. हॅकर क्लायंट साइड स्क्रिप्ट हाताळून ई शॉपला कोड पाठवू शकतो.

५. खालच्या दर्जाचे डेटाबेस इनर्टीग्रेशन:

याचा अर्थ असा कि डेटाबेस स्टोर करणारी सर्व माहितीचे फ्रंटएंड बरोबर किंवा इतर ई शॉपच्या भागांन बरोबर सुरक्षित पद्धतीने इनर्टीग्रेट केलेले नसते. यामुळे माहितीची देवाणघेवाण होताना माहिती चोरली जाऊ शकते आणि युझर डेटाबेसमध्ये म्यालीशियस कोड इनपुट करू शकतो.

६. थर्ड पार्टी प्रोडक्टमधिल सेक्युरिटी दोष:

थर्ड पार्टी प्रोडक्टमधिल पेमेंट गेटवे सदोष असतील तर ते ई शॉपच्या सुरक्षेशी तडजोड करू शकतात.

25. फायनानशीअल (आर्थिक) गुन्हे

मुख्यत्वे करून पैसा हा जास्तीजास्त गुन्ह्यान मध्ये महत्वाचा हेतू असतो. सायबर गुन्ह्यानच्या बाबतीत हि हीच गोष्ट खरी आहे. जगभरात असे निदर्शनास आले आहे कि जास्ती जास्त सायबर गुन्हे बदला किंवा मजेपेक्षा आर्थिक फायद्याच्या हेतूने होत आहेत. इंटरनेट, मोबाईल बँकिंग, ऑनलाईन शेअर ट्रेडिंगच्या वाढत्या वापरामुळे असे प्रकार वरचेवर घडतच राहतील. आर्थिक गुन्ह्यांमध्ये सायबर फसवणूक, क्रेडिट कार्ड चोरी, मनी लाऊनडरिंग,बँक सर्व्हर व संगणक हाताळणी करताना हॅकिंग, अकौंन्टींग स्कॅम इ. चा समावेश होतो.

उदाहरण:

कॉम्पुटराइसड अकाउंटमध्ये खोटे डेबिट आणि क्रेडीट व्यवहार करून भारतातील पंजाब नॅशनल बँकमध्ये १३.९ मिलियन रुपयाचा घोटाळा झाला होता.

उदाहरण:

बनावट कॉम्पुटराइसड अकाउंटचा वापर करून भारतातील बँक ऑफ बडोदामध्ये २,५०,००० रुपयाचा घोटाळा झाला होता.

उदाहरण:

भारतात हैदराबाद पोलिसांनी एक बेरोजगार कॉम्प्युटर ओप्रेटर तरुणास आणि त्याचा मित्र जो एका पंच तारांकित हॉटेलमध्ये काम करत होता, यांना हॉटेलच्या ग्राहकांच्या क्रेडीट कार्ड नंबरचा गैरवापर केल्यामुळे अटक केली होती. हॉटेलमध्ये काम करणाऱ्या मित्राने क्रेडीट कार्ड नंबर नोंद करून ठवले आणि आपल्या कॉम्प्युटर ओप्रेटर मित्रास देऊन हा घोटाळा केला.

उदाहरण :

२००४ मध्ये US **गुप्तहेर खात्याने एका तपासात एक ओनलाईन चालणारी संस्था बंद केली कारण कि या संस्थेने १.७ मिलियन क्रेडीट कार्ड आणि त्याच्या माहितीची कागदपत्रे यांची अनैतिक देवाणघेवाण केली होती.**

ऑपरेशन फायरवॉल नावाची एक उच्चभ्रु केसच लक्ष्य ४००० सभासद असणाऱ्या गुन्हेगारी संघटनानवरती होत, ज्यांची वेबसाईट ओळख चोरीसाठी हब म्हणून काम करत होती.

26. फायर सेल

देशाच कॉम्प्युटर कंट्रोलवरती असलेल्या अवलंबित्वावर हल्ला करण्यासाठी फायर सेलची रचना केलेली असते. फायर सेल हा देशाच्या दळणवळण, दूरसंचार, आर्थिक यंत्रणावर केलेला त्रिस्तरीय समन्वित असा हल्ला असतो. या हल्ल्याची रचना सर्वत्र अनागोंदी आणि नेतृत्वहीन वातावरण निर्मितीसाठी करण्यात आलेली असते. या हल्ल्यातील पहिला टप्पा दळणवळण, रस्ते, हवाई वाहतूक, रेल्वे, रस्त्यावरील सिग्नल यांना लक्ष्य करतो. पहिल्या टप्प्याचा उद्देश लोकांत अनागोंदी माजवणे आणि दळणवळण, अत्यावशक सुविधा ठप्प पाडणे हा असतो. दुसऱ्या टप्प्यात देशाची आर्थिक यंत्रणा जसे की शेअर बाजार, सरकारी संस्था ह्या बंद पाडणे असा असतो. शेवटचा टप्पा देशभरतील सर्व दूरसंचार यंत्रणा जसे फोन, सॅटेलाईट संवाद इ . बंद पडण्यासाठी असतो. या हल्ल्या नंतर सर्व परिस्थिती हाताबाहेर गेलेली असते.

डाय हार्ड ४.० चित्रपट याच संकल्पनेवर आधारित आहे.

27. फायर वाकिंग

फायरवॉल एक सेक्युरिटी टुल आहे (सॉफ्टवेअर किंवा हार्डवेअर) जे सुरक्षित कॉम्प्युटर व नेटवर्क वरून येणारा जाणाऱ्या डेटाचे नियंत्रण करते. फायरवॉल सुरक्षित कॉम्प्युटर व नेटवर्कची माहिती बाहेरील जगा पासून लपवून ठेवते.फायर वाकिंगमुळे हॅकर फायरवॉल मधून चालणाऱ्या सर्विसेस ची माहिती मिळवू शकतो.

28. फुटप्रिंटींग

लक्ष्य असलेल्या ठिकाणच्या वातावरणात शिरण्यासाठीचा मार्ग शोधण्यासाठी फुटप्रिंटींगचा वापर केला जातो. फुटप्रिंटींग यंत्रणेतील कमकुवतपणा निदर्शनास आणून देतात आणि त्याचा गैरवापर करण्यासाठीचा आपला मार्ग अधिक सुकर करतात. या मागील प्रमुख उद्देश जास्ती जास्त माहित जाणून घेणे हा असतो.लक्ष्य असलेल्या संस्थेवर हल्ला करण्याअगोदर त्या संस्थेचे टेकक्नोलॉजी फ्रेमवर्क बद्दलची माहिती गोळा करण्यासाठी फुटप्रिंटींगचा वापर केला जातो.फुटप्रिंटींग मध्ये कोणताही सक्रिय हल्ला केला जात नाही, फक्त हल्ल्याची योजना करण्यासाठी जरुरी असलेली सलग्न माहिती गोळा करणे इतकेच केले जाते.

१.१ प्रत्यक्ष स्थान आणि संपर्क माहिती:

माहितीचा स्त्रोत:

१. कॉर्पोरेट वेबसाईट

२. बिझनेस डिरेक्ट्रीज

३. ऑनलाईन डिरेक्ट्रीज

४. वार्षिक अहवाल

५. प्रकाशने इ .

भावी वापर किंवा गैरवापर:

हि सर्व माहिती सोशल इंजीनिअरिंग हल्ला योजण्यासाठी वापरली जाऊ शकते.

उदाहरण:

ग्लोबल सॉफ्टवेअर कंपनी मधील नेटवर्क ॲडमिनीस्ट्रेटरला एक CDs **असलेल छानस पॅकिंग केलेल कुरिअर आले होते. ह्या** CDs **मध्ये त्यांची कंपनी वापरत असलेल्या सर्व्हर कॉम्प्युटरच्या महत्वाच्या सेक्युरिटी अपडेटस होत्या, ज्या त्याने इनस्तॉल केल्या ज्यात खर तर ट्रोजोनाइजड सॉफ्टवेअर होते. त्यानंतरच्या झालेल्या हॅकिंगच्या हल्ल्यात लाखो रुपयाचा सोर्स कोड चोरी झाला होता.**

१.२ IT **इन्फ्रास्ट्रकचरची साधारण माहिती:**

माहितीचा स्त्रोत:

१. रेड हेरिंग प्रोसपेक्टस इनिशीअल पब्लिक ऑफरिंगच्या वेळी कंपनीकडून प्रकाशित होते.

जे आपण खालील संकेतस्थळावरून डाऊनलोड करू शकता:

www.sebi.gov.in

संभाव्य वापर किंवा गैरवापर:

डेक्कन एव्हीएशनचे रेड हेरिंग प्रोसपेक्टस कंपनीच्या IT **इन्फ्रास्ट्रकचरची सविस्तर माहिती देत. या वरून हे कळले कि एअर डेक्कनचे सेंट्रलाइज्ड** IT **रिसोर्सेस आहेत जे** IT **टीमच्या अखत्यारीत येते ज्यात ३१ मार्च २००६ पर्यन्त ३५ लोकांचा स्टाफ आहे. तसेच डोक्यूमेंट असेही उघड करते कि** CRS **सर्व्हर वरती आहे जे भारतातील गुरगाव येथे इंटरग्लोबच्या डाटा सेंटर मध्ये स्थित आहे.**

प्रोसपेक्टस मधील काही मनोरंजक माहिती:

"BSNL **आणि** Bharti **च्या लीज वरती असलेल्या रिडनडंट इंटरनेट कनेक्शननी सर्व्हर्स जोडले गेले आहेत.** Bharti **आणि** HCL **चे वायरलेस लुप नेटवर्कची उपलब्धता वाढवण्यासाठी मदत करतात.** Bharti **चे कनेक्शन जर फेल झाले तर प्रायमरी** BSNL **कनेक्शनचे आटोमेटेड राउटर वापरून कनेक्टीव्हीटी चालू ठेवली जाते. आणि जर दोन्ही लीज्ड कनेक्शन बंद पडले तर** HCL **ची वायरलेस लुप वापरण्यात येईल. एअर डेक्कनचे सर्वर्स इतर नेटवर्क पासून वेगळे ठेवले आहेत आणि नेटवर्क सेक्युरिटी वाढवण्यासाठी सिस्को पिक्स ५१५**e **फायरवॉल आणि** LINUX **फायरवॉल वापरण्यात आलेले आहे."**

१.३ सर्व्हरचे IP **अड्रेसेस**:

माहितीचा सोर्स:

१. सर्व्हरचा IP **अड्रेस आपण** www.who.is **चा वापर करून मिळवू शकतो**.

२. नेम सर्व्हर आणि मेल सर्व्हरचे IP **अड्रेस** www.iptools.com **वर** DNS **लुकअप वापरून आपण मिळवू शकतो**.

संभाव्य वापर किंवा गैरवापर:

ह्या माहितीचा उपयोग पोर्ट स्क्यानिंगसाठी केला जाऊ शकतो ज्याद्वारे आपल्याला कोणते पोर्ट चालू आहे हे कळू शकते,आणि त्यातील दुर्बलता देखील समजू शकतात.

आटोमेटेड हॅक आणि पेनीट्रेशन टेस्टिंग सॉफ्टवेअरचा वापर करून आपण हल्लाही करू शकतो.

१.४ वैयक्तिक कॉम्प्युटरचे IP **अड्रेस**:

माहितीचा सोर्स:

१. इम्प्लोयीनी पाठवलेल्या ईमेलच्या हेडरचे ॲनालीसीस.

२. Readnotify.com चा वापर करून पाठवलेल्या ईमेलस ट्र्याक करणे.

संभाव्य वापर किंवा गैरवापर:

या माहितीचा उपयोग पोर्ट स्क्यानिंग साठी केला जाऊ शकतो ज्याद्वारे आपण कोणते पोर्ट चालू आहे हे कळू शकते,दुर्बलता देखील समजू शकतात.

आटोमेटेड हॅकिंग आणि पेनीट्रेशन टेस्टिंग सॉफ्टवेअरचा वापर करून आपण हल्लाही करू शकतो.

१.५ नजीकच्या काळातील मर्जर, ॲक्वीजीएशन, टेकओवर:

माहितीचा सोर्स:

संस्थेच्या नजीकच्या काळातील मर्जर, ॲक्वीजीएशन, टेकओवर बद्दलची माहिती त्या संस्थेच्या वेबसाईट वरून मिळू शकते,तसेच हि माहिती नियामक संस्थानच्या वेबसाईट वरून हि मिळू शकते. उदा: www.sebi.gov.in,, www.bseindia.com, www.nseindia.com इ .

संभाव्य वापर किंवा गैरवापर:

हि माहिती महत्वाची आहे कारण मर्जर, ॲक्वीजीएशन, टेकओवर नंतर संस्थांचे नेटवर्क एकत्र येण्यासाठी बरेच महिने लागतात ज्याकाळात त्यावर हल्ला करता येऊ शकतो कारण त्यावेळी नेटवर्क फारच दुर्बल स्थितीत असतात.

१.६ वेबसाईटस:

माहितीचा सोर्स:

वेब डेव्हलपर कडून वेबसाईटच्या HTML **आणि** Javascript **कोड मधील कमेंटस आपण लक्ष्य केलेल्या वेबसाईटवरून मिळवू शकतो.** robotos.txt **नावाची फाईल वेबसाईटवरून आपल्याला मिळू शकते.** www.google.com **वरील अडव्हांन्स पर्याय वापरून लक्ष्य असलेल्या वेबसाईटवरील वर्ड, एक्सेल फाईल डाऊनलोड करू शकतो. या फाईलमध्ये महत्वाची माहिती बरोबरच डिलीट केलेला डाटा असतो जो कि परत मिळवला जाऊ शकतो.** 'websleuth' **वापरून वेबसाईट डाऊनलोड करता येऊ शकते.**

संभाव्य वापर / गैरवापर:

मिळालेली माहिती असलेल्या त्रुटी आणि दुर्बलता दर्शवते ज्याचा गैरवापर केला जाऊ शकतो.

१.७ वायरलेस नेटवर्क:

माहितीचा सोर्स:

GPS **सुविधा असलेला फोन वापरून** Airomap **सारख्या सॉफ्टवेअरचा वापर करून वॉर ड्रायव्हिंग केले तर ते ओपन आणि कमी प्रमाणात सुरक्षित आहेत असे वायरलेस नेटवर्कची माहिती उघड करते**.

संभाव्य वापर / गैरवापर:

मिळालेली माहिती असलेल्या त्रुटी आणि दुर्बलता दर्शवते ज्याचा गैरवापर केला जाऊ शकतो.

१.८ इतर माहिती:

एखाद्या संस्थेमधील सुरक्षा धोक्या बद्दलची माहिती आपणास न्युज वेबसाईट किंवा विशेष सर्च इंजिन जसे कि www.data64.cc **आणि** www.bugs.ms **वरून मिळू शकते. कंपनी रजिस्ट्रार, स्टॉक एक्स्चेंज, सेबीकडे केलेल्या वैधानिक घोषणा त्यांच्या वेबसाईट वरून मिळू शकतात किंवा संबंधित प्राधिकरणाकडून थेट माहिती मिळवू शकता. किंवा ट्रेसराऊटचा हि वापर करू शकतो.**

संभाव्य वापर / गैरवापर:

मिळालेली माहिती असलेल्या त्रुटी आणि दुर्बलता दर्शवते ज्याचा गैरवापर केला जाऊ शकतो. ट्रेसराऊटचा वापर करून नेटवर्क इन्फ्रास्ट्रकचर आणि होस्टसाठी दिले गेलेले IP अड्रेसची माहिती करू शकतो.या माहितीचा वापर करून दुर्बल नोडस किंवा कॉम्प्युटर बद्दलची माहिती मिळवू शकतो.

29. फ्रौड

प्रिय, श्री. जस्टीन विलिअम्स माझे नाव विकास मनजित सिंग आहे मी पंजाब (इंडिया) मध्ये राहतो. माझ्या शहाराचे नाव लुधियाना आहे. माझा एक भाऊ कॅनडामध्ये राहतो ज्याचे नाव जस्टीन विलिअम्सच आहे. त्यास वेलंडचे श्री. विलिअम राम यांनी माझ्या पालकांकडून दत्तक घेतले आहे. मी आणि माझी आई जस्टीनला त्यांच्याकडे सोपवण्यासाठी कॅनडात आलो आहोत. तर मग श्री. जस्टीन विलिअम्स मी ज्यांच्या बद्दल बोलत आहे ते जर आपणच असाल तर मी आपणास भेटून सत्य परिस्थिती सांगू इच्छितो.

विचार करा हे पत्र वाचल्यावर श्री. जस्टीन विलिअम्स यांच्या डोक्यात काय विचार चालू असतील, का ते खरच दत्तक घेतलेले असतील ? मग त्यांचे खरे पालक कुठे असतील? हा मेल त्यांच्या सख्या भावाचा तर नाही?

खरे तर हा एक घोटाळा आहे, हा मेल भारतातील संगरुर मधील एका कॉलेज मधून पाठवलेला असतो. कॅनडाच्या नागरिकांना अशा प्रकारच्या मेलनी लक्ष्य केले जाते. जर एखाद्याला वाटले कि हा मेसेज खरच त्यांच्या भावाकडून आला असेल,मग त्यांच्या कडे पैशाची मागणी

केली जाते जेणेकरून त्यांचा तो भाऊ कॅनडात येउन ते दत्तक असल्याची खात्री पटवून देईल!

इंटरनेट वरील शेकडो ईमेल घोटाळ्यान पैकी हा एक घोटाळा आहे. या प्रकारच्या घोटाळ्यांना "नायझेरियन ४१९" या नावाने ओळखले जाते, असे घोटाळ्याचे ईमेल नायझेरियातून पाठवलेले असतात आणि नायझेरियन दंड संहिता कलम ४१९ हा फसवणुकीशी संबंधित आहे. (जसा भारतात कलम ४२० प्रसिद्ध आहे). ४१९ पत्र घोटाळ्याची सुरवात १९८० च्या सुरवातीच्या काळात सुरु झाली. १९९० मध्ये ईमेल घोटाळ्याची सुरवात झाली. २००७ मध्ये एशियन स्कूल ऑफ सायबर लॉने ३ महिन्यासाठी अशा प्रकारच्या शेकडो ईमेल घोटाळ्याच्या तपासावर लक्ष्य केंद्रित केले होत, आश्चर्याची गोष्ट अशी कि सर्व ईमेल पैकी फक्त १०% मेल नायजेरिया मधून आलेले होते. यातील बहुत करून मेल इस्राईल, नेदरलॅड, UK आणि इतर युरोपीअन देशातुन आलेले होते. "बर्थ ब्रदर " नावाचा फक्त एक मेल भारतातून आला होता. यातील बहुतकरून मेल हे रिसिव्हरला लाखो किंवा करोडो रुपये देण्याचे वचन देत होते, तेही त्याचा बँक अकाउंट वर ट्रान्स्फर करून, यासाठी मेल रिसीव्ह करणाऱ्याला त्याचे बँक खात्याची सविस्तर माहिती द्यावी लागेल , आणि तो लखपती बनेल! आणि जर कोणी या जाळ्यात फसूवून आपल्या बँकची माहिती किंवा खरी कागदप्रते दिली तर तो व्यक्ती फसेल. कारण परत त्यांच्याकडून बँकेत पैसे ट्रान्स्फर करण्यासाठी, किंवा इतर कामांसाठी १०० ते २५०० डॉलरची मागणी केली जाईल, हे पैसे मिळवणे ह्या घोटाळ्या मागील खरा उद्देश

असतो , एकदा का पीडित व्यक्तीने पैसे दिले कि समोरची व्यक्ती गायबच होऊन जाते.

लॉटरी इमेल घोटाळ्यामध्ये आपण मायक्रोसोफ्ट, याहु किंवा इतर प्रसिद्ध कंपनीची लॉटरी जिंकला आहात असे सांगण्यात येते, आणि विजेत्या व्यक्तीस त्याचे बँक खाते माहिती आणि काही रक्कम प्रोसेसिंग फी म्हणून मागण्यात येते.अजून एक ईमेल घोटाळा ज्यात असे म्हटले असते कि "आमच्याकडे ब्रिटीश नॅशनल लॉटरीकडून आपल्यासाठी एक कुरिअर आहे जे आपणास पाठवायचे आहे त्यासाठी आपल्याला ४७० पौंड रक्कम अगोदर पाठवावी लागेल जेणेकरून आम्ही आपणस लॉटरीचा चेक पाठवू शकू." अशा प्रकारचा मजकूर असतो.अजून एक ईमेल घोटाळा ज्यात असे म्हंटलेले असते कि एक विधवा स्त्री जी मरणाच्या दारात उभी आहे, ती तिची संपती तिच्यासाठी प्रार्थना करणाऱ्याला दान करेल.अजून एक ईमेल घोटाळा, इम्प्लोयी ऑफ द युरो लॉटरीचा आहे, यात तो व्यक्ती असे म्हणत असतो कि तो घोटाळा करणार आहे आणि मिळालेली रक्कम आपल्या बरोबर वाटून घेण्यास तयार आहे.या सर्व घोटाळ्यान मधील समान धागा असा आहे कि पीडित व्यक्तीला काही कागदपत्रे स्कॅन करून मेल केली जातात, आणि एकदा का त्यांची खात्री पटली कि हे सर्व खरे आहे मग त्यांच्या कडून विविध कारणांसाठी काही पैशाची मागणी केली जाते. आणि हे पैसे मिळवणे हाच ह्या घोटाळ्या मागील उद्देश असतो. अशा प्रकारे हजारो लोकांना लुटून खूप पैसे कमावले जातात.

उदाहरण:

२००५ मध्ये एका भारतीय उद्योजकाला आफ्रिकेतील एक मोठया बँकेच्या उपाध्यक्षाकडून ई मेल आला त्यात त्याने १ मिलिअन डॉलरसाठीचा एक फायदेशीर करारासाठीची विचारणा केली. भारतीय उद्योजकाचे त्या ईमेल पाठवणारयां व्यक्ती बरोबर फोनवर अनेकदा बोलणे झाले.भारतीय उद्योजकाने त्या व्यक्तीचा ईमेल वेबसाईट वरून पडताळून पहिला, आणि त्यांनी इमेल मध्ये दिलेल्या बँक अकाउंटवर पैसे पाठवले. नंतर उद्योजकाला समजले कि तो ईमेल एका नायजेरिया स्थित भारतीया कडून स्पुफ करून पाठवला होता.

उदाहरण:

एक नवीन प्रकारचा ईमेल घोटाळा ज्यात म्हणलेले असते कि जर आपण ईमेल पाठवणाऱ्या व्यक्तीस पैसे दिले नाही तर तुम्हाला ठार करण्यात येईल, आणि तो स्वतःची ओळख कॉंट्रक्ट किलर आहे अशी सांगतो. या उत्तर दिल्यास त्यास समजते कि त्याने चालू अकाउंटशी संपर्क साधला आहे, आणि अजून धमक्या दिल्या जातील.

एका केस मध्ये पीडित व्यक्तीने रिप्लाय केला होता कि जर त्यास परत त्रास दिला तर तो पोलिसांना फोन करेल. त्या व्यक्तीस २०००० डॉलर्सची मागणी करणाऱ्याने त्याच्या वैयक्तिक जीवना विषयीची

माहिती पाठवून परत धमकावण्याचा प्रयत्न केला. आणि निर्वाणीचा इशारा दिला, "मला तू सांग कि मी सांगितल्या प्रमाणे तू वागणार आहेस कि नाही का मी मग माझ्या पद्धतीने काम करू? फक्त हो किंवा नाही संग बाकीचे प्रश्न विचारू नकोस !!" काही ठिकाणी FBI च्या नावानी खोटे मेल पाठवले गेले, ज्यात असे म्हंटले होते कि "आम्ही एका व्यक्तीस अटक केली आहे आणि त्याच्या जवळ तुमची माहिती सापडली आहे तेव्हा त्वरित आम्हाला संपर्क साधा." हा हि एक घोटाळाच आहे.

30. ऑनलाईन गॅमब्लिंग

अशा हजारो वेबसाईटस आहेत ज्या ऑनलाईन गॅमब्लिंग सुविधा पुरवतात. या बाबत विशेष मुद्दा म्हणजे काही देशात ऑनलाईन गॅमब्लिंग कायदेशीर आहे. म्हणजे कायदेशीरदृष्ट्या हया वेबसाईटसचे मालक सुरक्षित आहेत. कायदेशीर बाब तेव्हा समोर येते जेव्हा ऑनलाईन गॅमब्लिंग बेकायदेशीर असलेल्या देशातील (उदा : भारत) व्यक्ती जेव्हा ऑनलाईन गॅमब्लिंगचा वापर करतो.

उदाहरण:

www.ladbrokes.com **हि वेबसाईट क्रिकेट, फुटबॉल, टेनिस, गोल्फ, मोटर रेस, आइस हॉकी, बास्केटबॉल, बेसबॉल, एक स्पर्धात्मक खेळ, स्नूकर, बॉक्सिंग, ॲथलेटिक्स,, रग्बी, व्हॉलीबॉल, मोटर सायकलिंग इत्यादी खेळानसाठी ऑनलाईन गॅमब्लिंग सुविधा पुरवते. तसेच ऑनलाईन क्यासिनो देखील इथे आहे, ज्या देशात ऑनलाईन गॅमब्लिंग बेकायदेशीर आहे अशा देशातील लोकांनी या साईटचा वापर करण्यापासून रोखणारी कोणतीही तरतूद इथे केलेली नाही.**

31. गुगल आधारित हॅकिंग

गुगल हे जगातील सगळ्यात प्रसिद्ध आणि शक्तिशाली सर्च इंजिन आहे, ज्याचा हॅकर कडून सहज पणे गैरवापर केला जाऊ शकतो. सहजपणे न दिसणारी संवेदनशील आणि गोपनीय माहिती हॅकरस गुगल सर्च इंजिनचा व्यापक प्रमाणावर वापर करून मिळवू शकतात.काही विशेष कमांडसचा वापर महत्वपूर्ण माहिती शोधण्यासाठी केला जातो.

intitle:

"intitle" **हा सिनटॅक्स वापरून गुगल त्यातील शब्द असलेली पेजेस निषिद्ध करतो.**

उदाहरणार्थ:

intitle : login password **हया मुळे ज्या ज्या पेज मध्ये हे दोन शब्द आढळतील त्याची लिंक शोधेल, जर एखाद्या पेज वरील एका पेक्षा जास्त शब्द शोधायचे असतील तर** "allintitle:" **चा वापर करतात.**

उदाहरणार्थ :

intitle: login intitle: password **हे** allintitle: login password **सारखेच आहे.**

दुर्बल साईटस शोधण्यासाठी सिनटॅक्स:

allintitle: “index of /root”

यामुळे आपल्याला अशा वेब सर्व्हरची यादी मिळेल जे निषिद्ध असलेल्या रूट डिरेकट्रीजला ॲक्सेस देतात. काही वेळेस अशा डिरेकट्रीमध्ये संवेदनशील माहिती असते जी सध्या वेब रिक्वेस्टने मिळवता येते.

allintitle: "index of /admin” :

यामुळे आपल्याला अशा वेबसाईट लिंक्सची यादी मिळेल ज्यांच्या निषिद्ध डिरेकट्रीच वेब मधून इंडेक्स ब्राउझिंग सुरु आहे. बरेच वेब ॲप्लिकेशन एडमीनचे तपशील "admin' **हे नाव वापरून सेव्ह करतात. काही वेळेस अशा डिरेकट्रीमध्ये संवेदनशील माहिती असते जी सध्या वेब रिक्वेस्टने मिळवता येते.**

काही इतर उदाहरणे :

- intitle:"Index of" .sh_history
- intitle:"Index of" .bash_history
- intitle:"index of" passwd
- intitle:"index of" people.lst
- intitle:"index of" pwd.db

- intitle:"index of" etc/shadow
- intitle:"index of" spwd
- intitle:"index of" master.passwd
- intitle:"index of" htpasswd
- intitle:"index of" members OR accounts
- intitle:"index of" user_carts OR user_cart
- allintitle: sensitive filetype:doc
- allintitle: restricted filetype :mail
- allintitle: restricted filetype:doc site:gov

site:

" site:" **हा सिनटॅक्स गुगलला ठराविक माहिती शोधण्यापासून रोखतो**.

उदाहरणार्थ:

Courses site:asianlaws.org: **मुळे** asianlaws.org **डोमेन मधील** "courses" **हा शब्द असलेली सर्व पेजेस शोधली जातील**. "site:" **आणि** "domain name" **मध्ये स्पेस असता कामा नये**.

inurl:

" inurl:" **हा सिनटॅक्स सर्च रिझल्ट, सर्च कीवर्ड असलेल्या** URL **पुरताच निर्धारित करेल**.

उदाहरणार्थ :

inurl: passwd: **हा सिनटॅक्स** password **हा शब्द असेल्याच** URL **दाखवेल**. **जर एका पेक्षा जास्त शब्द शोधायाचे असतील तर** "allinurl:" **चा वापर केला जातो**.

allinurl: etc/passwd: **हा सिनटॅक्स** "etc" **आणि** "passwd" **हे दोन शब्द असलेल्या** URL **शोधेल, दोन शब्दांमधील** "/" **हे चिन्ह गुगल दुर्लक्षित करेल**.

दुर्बल साईट शोधण्यासाठी खालील सिनटॅक्स वापरतात:

allinurl:winnt/system32/: **हा सिनटॅक्स वेब मधून** "system32" **सारख्या निषिद्ध असणाऱ्या डिरेकट्रीज ॲक्सेस देणाऱ्या वेबसाईटस शोधतो. जर** "system32" **मधील** cmd.exe **ला ॲक्सेस मिळत असेल तर सर्व्हरच्या सुरक्षेशी तडजोड झाली आहे**.

allinurl: wwwboard/passwd.txt: **हा सिनटॅक्स** "WWWBoard Password vulnerability" **ला व्हलनरेबल असलेल्या सगळ्या सर्व्हरच्या लिंक दाखवेल. या व्हलनरेब्लीटी बाबत अधिक माहितीसाठी**

http://www.securiteam.com/exploits/2BUQ4S0SAW.html **ला भेट द्या**.

inurl:.bash_history: **हा सिनटॅक्स वेब मधून** ".bash_history" **या फाईलला ॲक्सेस देणाऱ्या सगळ्या सर्व्हरची लिस्ट दाखवेल, हि कमांड हिस्ट्री फाईल आहे. ॲडमिनीस्ट्रेटरने वापरलेल्या सर्व कमांडस आणि पासवर्ड ह्यात सेव्ह असतात. ह्या फाईल मध्ये एक एनक्रिपटेड पासवर्ड असतो जो** "JohnThe Ripper" **सारखे टुल वापरून सहज क्र्याक करता येतो**.

inurl: config.txt: **हा सिनटॅक्स वेब मधून** "config.txt" **या फाईलला ॲक्सेस देणाऱ्या सगळ्या सर्व्हरची लिस्ट दाखवेल, या मध्ये संवेदनशील माहितीचे हॅश मुल्य असते**.

इतर काही उदाहरण:

- inurl:admin filetype:txt
- inurl:admin filetype:db
- inurl:admin filetype:cfg
- inurl:mysql filetype:cfg
- inurl:passwd filetype:txt

- inurl:iisadmin
- inurl:orders.txt
- inurl:"wwwroot/*."
- inurl:adpassword.txt
- inurl:webeditor.php
- inurl:file_upload.php
- inurl:gov filetype:xls "restricted"
- index of ftp +.mdb allinurl:/cgi-bin/ +mailto
- inurl:auth_user_file.txt

link:

हा सिनटॅक्स निर्देशित केलेल्या वेबपेजेसच्या लिंक असलेल्या सर्व साईटसची लिस्ट दाखवतो.

उदाहरणार्थ:

link:www.asianlaws.org : **हा सिनटॅक्स** asianlaws.org **च्या होमपेज च्या लिंक असणाऱ्या सर्व साईटसची लिस्ट दाखवेल**. "Link " **आणि** URL **मध्ये स्पेस देऊ नका**.

filetype:

filetype **सिनटॅक्स विशिष्ट एक्स्टेनशन असलेल्या फाइल्स**(**उदा**: . doc, pdf or ppt **इ**) **शोधण्यापासून गुगलला रोखते**,

उदाहरणार्थ :

filetype:doc site:gov confidential **हा सिनटॅक्स सर्व सरकारी डोमेन जे** ".gov" **आहेत त्यावरील** ".doc" **एक्स्टेनशन असलेल्या आणि ज्या पेजेस मध्ये किंवा** .doc **फाईलमध्ये** "confidential" **असा शब्द असेल त्याचा शोध घेईल**, **म्हणजे सर्व** "confidential" **शब्द असलेल्या सरकारी साईट वरील डॉक्युमेंट फाईल्स शोधल्या जातील**.

related:

हा सिनटॅक्स निर्दिष्ट केलेल्या वेबसाईटशी संबंधित सारखी वेबपेज शोधेल.

उदाहरणार्थ :

related:www.asianlaws.org **हा सिनटॅक्स** www.asianlaws.org **या साईशी संबंधित सारखे वेबपेजेसची लिस्ट दाखवेल**, related: **आणि** www.asianlaws.org **मध्ये कोणतीही स्पेस नसेल**.

cache:

हि क़्वेरि आपल्याला गुगल cache **मध्ये असलेले वेबपेजचे व्हर्जन दाखवेल**.

उदाहरणार्थ:

cache:www.asianlaws.org **हा सिनटॅक्स गुगलच्या क्याश मधील** asianlaws.org **मधील होमपेज दाखवेल**.cache: **आणि** www.asianlaws.org **मध्ये कोणतीही स्पेस नसेल**. **जर तुम्ही या क़्वेरिमध्ये इतर शब्दांचा समावेश केला तर**, **गुगल क्याशड डॉक्युमेंट मध्ये ते शब्द हायलाईट करेल**.

उदाहरणार्थ:

cache:www.asianlaws.org courses **हा सिनटॅक्स क्याशड कनटेंट दाखवेल ज्यात** "courses" **शब्द हायलाईट केलेला असेल**.

intext:

हा सिनटॅक्स विशिष्ट वेबसाईट मधील शब्द शोधण्यासाठी वापरला जातो, **तो लिंक्स किंवा** URL, **आणि पेज टायटलकडे दुर्लक्ष करतो**.

उदाहरणार्थ:

intext:exploits **हा सिनटॅक्स** "exploits" **हा शब्द असलेल्या वेबसाईटसची यादी दाखवेल**.

phonebook:

हा सिनटॅक्स US **मधील पत्ते आणि फोन नंबरचा शोध घेतो**.

उदाहरणार्थ:

phonebook:Lisa+CA **हा सिनटॅक्स क्यालीफोर्नियात** (CA) **राहणाऱ्या आणि** Lisa **नाव असलेल्या सर्वांची लिस्ट दाखवेल, सोशल इंजिनीअरिंगसाठी वैयक्तिक माहित मिळवण्यासाठी याचा वापर केला जाऊ शकतो**.

32. ग्रीफरस

ग्रीफर हा असा खेळाडू आहे जो खेळामध्ये मुद्दामहून इतरांना त्रास किंवा दुख होईल असे वागतो. बरेच वर्गणी आधारित खेळ ग्रीफरला सक्रिय पणे विरोध करतात, कारण त्याचा व्यवसायावर दुष्परिणाम होत असतो. अशा ग्रीफरला हद्दपार करण्यासाठी सर्व्हर साइड अपग्रेड आणि प्याचेस देण अगदी सामान्य गोष्ट आहे. अनेक ऑनलाइन गेम अशा प्रकारच्या दोषी लोकांना तंबी देण्यासाठी गेम मास्टर्सची नेमणूक करतात. आणि बाकीचे काही क्राउड सोर्सिंग दृष्टीकोन स्वीकारतात जेथे खेळाडू स्वतःच अशा घटनांची माहिती देतात. मग अशा लोकांना समन्स बजावण्यात येतो , आणि गेम मास्टर्स निर्णयानुसार पुढील कारवाई करतात. ग्राहक तक्रार निवारण केंद्रात येणारे २५ % फोन याच्याशी निगडीत असतात.

त्रास देण्याचे विविध मार्ग:

१. खेळाडू विरुद्ध खेळाडूचा छळ:

ऑनलाईन खेळामध्ये एखाद्या विशिष्ट खेळाडूला लक्ष्य करून निराधार अवस्थेत असताना खेळामध्ये सारखा सारखा हल्ला करून मारणे आणि खेळातून बाहेर पडण्यास भाग पाडणे.

२. किल स्टीलिंग:

वारंवार खेळामध्ये दुसऱ्याचे किल्स चोरून त्यांचा वेळ वाया घालवणे.

३. शाब्दिक छळ:

एखाद्या व्यक्तीस अश्लील, तिरस्करणीय, किंवा आक्षेपार्ह संदेशाचा वापर करून त्रास देणे.

४. ब्लोकिंग(अडवणूक) :

दुसऱ्याच्या मध्ये मध्ये करणे ज्यामुळे त्यांना कोणतीही हालचाल करता येऊ नये किंवा त्या ठिकाणाहून बाहेर पडता येऊ नये.

५. ट्रिगरिंग:

ऑन लाईन गेममध्ये खुप मॉनस्टर पाठवून ज्यामुळे खेळाडूला खेळ खेळणे अवघड जाईल आणि एक तर तो खेळ तर सोडून जाईल किंवा त्यात मारला जाईल.

उदाहरण:

सेकंड लाईफ नावाच्या गेमने छळ (ज्या मध्ये रुक्षपणे वागणे, धमकावणे, त्रास देणे इ.) किंवा हल्ला(गोळ्या चालवणे, धक्का देणे, स्क्रीप्टचा वापर करून खेळाडूस खेळाचा आनंद घेण्यापासून रोखणे)

त्यांच्या कम्युनिटीच्या नियमांनुसार बंदी घातलेली आहे. यामध्ये इशारा, निलंबन आणि पूर्णपणे बंदी यांचा समावेश होतो.

33. हॅकटीविझम

हॅकटीविस्ट हा एक हॅकर आहे जो तंत्रज्ञानाचा वापर सामाजिक, वैचारिक, धार्मिक किंवा राजकीय संदेश देण्यासाठी करत असतो. राजकीय हेतूसाठी वैध किंवा अवैध पणे डिजिटल टूल्स चा वापर करणे अशी याची व्याख्या करता येईल म्हणून हा राजकीय किंवा वैचारिक प्रेरणेतून केलेला विध्वंस आहे. हॅकटीविस्ट हा हॅकर प्रमाणेच टूल्सचा वापर करून एखादी सेवा बंद पपाडून, सामाजिक किंवा राजकीय मुद्यांकडे लक्ष वेधण्याचा प्रयत्न करतो. उदाहरणार्थ : एखाद्या प्रसिद्ध वेबसाईट वरती ठळकपणे दिसेल असा मेसेज पोस्ट करून त्याद्वारे आपला मुद्दा मांडण्याचा प्रयत्न करतो. किंवा हॅकटीविस्ट एखाद्या वेब साईटवर डिनायल ऑफ सर्व्हिसचा हल्ला करून ती बंद पाडतात.

हॅकटीविझम मागील प्रमुख उद्देश पैसा नसतो पण विशिष्ठ मुद्दा लावून धरणे हा असतो. हॅकटीविस्ट बदल, राजकारण, विचार, विरोध, आणि कुणाला तरी त्रास द्यायच्या इच्छेने प्रेरित असतात, पण मुद्दा असा आहे कि जर हल्ला करणार्याची जर ओळखच कळत नसेल तर एवढा खटाटोप कशासाठी करायचा?

उदाहरण:

मायक्रोसोफ्टचा UK च्या कार्यक्रमाची वेबसाईट हटवून सौदी अरेबियाच्या ध्वज त्याच्या जागी पोस्ट होता. इराणच्या निवडणुकीचा निषेध करणाऱ्या हॅकटीविस्टनी इराण बाहेरून इराण सरकारकडून चालवण्यात येणाऱ्या वेबसाईटसवर DDOS चा हल्ला केला. ज्यामुळे इराण सरकारच्या वेबसाईटचा जगाशी संपर्क तुटला त्यामुळे इराण मधील चालु परिस्थिती बद्दलची माहिती नेट वापरकर्त्यांना मिळणे अशक्य झाले होते.

जॉर्जिअन लेखकाचे लेख प्रसिद्ध केल्याबद्दल त्या सोशल नेटवर्किंग साईटला रशिअन हॅकटीविस्टने लक्ष्य केले. आणि DDOS हल्ल्याचा वापर करून फेसबुक आणि ट्वीटर सारख्या सोशल नेटवर्किंग साईट बंद पडल्या होत्या. त्या जॉर्जिअन लेखकाच्या विरोधात केलेली हि कृती होती कारण त्याचे या दोन वेबसाईट वर अकाउंट होते.

२००१ मधे US च्या विमानाशी जेट फायटर धडकून चायनीज वैमानिकाच्या झालेल्या मृत्यू नंतर एक हॅकटीविझमचे प्रात्येक्षिक झाले होते. चायनीज आणि अमेरिकन हॅकटीविस्टनी एकमेकांवर हल्ले केले होते.

34. हायज्याकिंग

ज्या प्रमाणे पारंपारिक पद्धतीने विमानाचे हायज्याकिंग बळाचा वापर करून करण्यात येते त्याच प्रमाणे वेबज्याकिंग म्हणजे बळाचा वापरकरून वेबसाईटचा ताबा मिळवणे. यामागील उद्देश पारंपारिक अपहरणासारखाच असतो, पैसा. हे करणाऱ्या लोकांचा राजकीय किंवा आर्थिक उद्देश असतो जो साध्य करण्यासाठी ते जबरदस्तीने वेबसाईटचा ताबा मिळवतात आणि आपल्या मागण्या पूर्ण करून घेतात.

वेबसाईटचा जबरदस्तीने ताबा मिळवल्यावर, त्यावर काय पोस्ट होईल याच्यावर वेबसाईट मालकाचा ताबा राहत नाही.

वेब जॅकिंग कशा पद्धतीने होते?

वेबसाईटच्या ॲडमिनीस्ट्रेटर कडे एक युझरनेम आणि पासवर्ड असतो जो फक्त त्यालाच माहित असतो, ज्याचा उपयोग वेबसाईट वर फाइल्स उपलोड करण्यासाठी केला जातो . आणि जर हा पासवर्डच हॅकरच्या हाती लागला तर तो ॲडमिनीस्ट्रेटर म्हणून वागेल आणि वाटटेल ते उपलोड करेल. कॉम्प्युटर माणसे ओळखत नाही त्यास फक्त युझरनेम आणि पासवर्ड समजतात.

अशा वेळी हॅकर क्र्याकिंग सॉफ्टवेअर वरून पासवर्ड मिळवू शकतो . पासवर्ड दोन प्रकारे करता येते, डिक्सनरी हल्ला आणि ब्रूट फोर्स हल्ला.

डिक्सनरी हल्ल्या मध्ये पूर्व निर्धारित डिक्सनरी शब्दांचा वापर केला जातो. ब्रूट फोर्स हल्ला विविध प्रकारचे शब्द संग्रह वापरून केला जातो ज्यात नंबर, अक्षर आणि चिन्हांचा समावेश होतो. डिक्सनरी हल्ल्या पेक्षा ब्रूट फोर्स हल्ला जाता वेळ घेतो.

उदाहरण:

USA मध्ये एक घटना घडली होती,एक लहान मुलांसाठी असलेल्या वेबसाईटच्या मालकाला एका हॅकर गटा कडून मेल आला होता, कि आम्ही तुमची वेबसाईट हॅक केली आहे आणि त्यांनी १ मिलियन डॉलरची मागणी केली होती. पण वेबसाईटच्या मालकिणीने हॅ धमकीला विशेष महत्व दिले नाही ,परंतु ३ दिवसांनी तिला सगळीकडून फोन येऊ लागले कि तुमची वेबसाईट हायजॅक झालेली आहे. कालांतराने वेब जॅकरनी वेबसाईटचा मजकूर बदलला आणि 'How to have fun with goldfish' ऐवजी 'How to have fun with piranhas' असा सगळीकडे बदल करून टाकला. Piranhas एक मासाहारी अतिशय खतरनाक मासा आहे, पण काही मुलांनी हि माहिती खरी आहे असे समजून तसा प्रयत्न केला आणि जखमी झाले.

35. आयडेनटीटी फ्रौड (ओळख फसवणूक)

ओळख फसवणूकी मध्ये एखादी व्यक्ती दुसऱ्याची ओळख चोरते आणि तो स्वतःच ती व्यक्ती आहे असे सगळ्यांना भासवण्याचा प्रयत्न करतो, या मागील उद्देश दुसऱ्याच्या नावचे फायदे लाटण्याचा असतो. अशा प्रकारे ओळख चोरणाऱ्याच्या कृत्याचा परिणाम खऱ्या व्यक्तीस भोगावा लागतो. ओळख फसवणूक करून एकदी व्यक्ती तुमची वैयक्तिक माहिती जसे फोन नंबर, बँक खाते, क्रेडीट कार्ड नंबर वापरून गुन्हा करू शकते. या मध्ये ती आपले पैसे चोरू शकतो किंवा इतर लाभ घेऊ शकतो या चे आपल्यावर आर्थिक आणि मानसिक परिणाम होऊ शकतात.

उदाहरण:

हेलननी एका व्यक्तीची अधिकृत रजिस्टर मध्ये असलेली माहित मिळवली, त्या व्यक्तीचे नाव हरक्युलस होते. आणि हि माहिती वापरून हेलनने एक फोनचे कनेक्शन घेतले, जो कि यडेनटीटी फ्रौड आहे.

उदाहरण:

कै कै ने पाकीटमारी करून क्रेडीट कार्ड चोरले होते, आणि त्याचा वापर करून महागडे दागिने खरेदी केले, जो कि आयडेनटीटी फ्रौड आहे.

उदाहरण:

बोरा बोरा बँक गोपनीय माहिती फेकून द्यायच्या अगोदर नष्ट करायचे विसरून गेली. हि माहिती चोरून मोकॅम्बोनी इतर कंपनीला बँकेचा डायरेक्टर म्हणून पत्र लिहिली,जो कि आयडेनटीटी फ्रौड आहे.

36. *इमपेर्सोनेशन*

ऑनलाईन इमपेर्सोनेशन हा एक सगळ्यात खतरनाक असा ऑनलाईन अब्रुनुकसानीचा प्रकार आहे. हा प्रकार तेव्हा घडतो जेव्हा एखादा व्यक्ती दुसऱ्याची ओळख वापरून (नाव अथवा फोटो) इतरांशी संपर्क करते. इमपेर्सोनेटर अकाउंट हॅक करू शकतो किंवा बनावट अकाउंट तयार करू शकते

. या मागील उद्देश बदला,खंडणी, नैराश्य किंवा करमणूक असा असू शकतो. ऑनलाईन झालेली अब्रुनुकसानी खुप मोठी असू शकते ज्यातून सावरणे खूप कठीण असते.

उदाहरण:

आर्यन पोलिसाचा गणवेश घालून श्रीमती फर्नांडीस यांच्या घरी जातो ज्या वयोवृद्ध असतात आणि एकत्याच राहत असतात. आर्यन ने त्यांना असे सांगितले कि तो त्यांच्या सुरक्षेसाठी आला आहे आणि त्यांनी त्यांची सर्व मौल्यवान वस्तु त्याच्याकडे सांभाळण्यासाठी द्याव्यात. आणि मग आर्यन त्या सर्व मौल्यवान वस्तु घेऊन पळून जातो, हि पोलिसांच इमपेर्सोनेशन केल्याची घटना आहे. इमपेर्सोनेशन हे ट्विटरच्या नियमांचे उल्लंघन आहे. ट्विटरवरती जर आपण बनावट खाते उघडले तर ट्विटर इमपेर्सोनेशन धोरणानुसार आपल्याला कायमचे निलंबित केले जाऊ शकते.

37. जो-जॉब

जो-जोब हा ईमेल स्पुफिंग चा प्रकार आहे, ज्यात एखादा व्यक्ती खुप स्पॅम ईमेल पाठवते जे ईमेलचा खरा सोर्स दाखवत नाहीत. काही वेळेस इंटरनेट सर्व्हिस प्रोव्ह्यडर कडे तक्रार केली म्हणून त्याचा बदला घेण्यासाठी असे मेलं पाठवण्यात येतात. हे कृत्य करणारया ईमेलच्या कायदेशीर मालकला जोइंग करतोय असे म्हणण्यात येते. स्प्यामरला जास्त काही नाहीतर ईमेल मधील "Reply To" चा अड्रेस बदलावा लागतो.

खरेतर जो-जोब आयडेनटीटी थेफ्टचा खूप रुक्ष प्रकार आहे. बऱ्याच वेळेस तुमचा ईमेल अड्रेस "sender's address" म्हणून वापरला जाईल. आणि लाखो ईमेल्स फक्त एकदाच नाही तर हा हल्ला संपण्या अगोदर परत परत पाठवण्याची साखळी असते. म्हणून हा सेंडरचा डाटा स्पूफ करून केलेला स्पॅम हल्ला आहे. यामुळे कथित सेंडरची प्रतिमा डागाळेल आणि ईमेल रेसिपीअन्ट कारवाई करण्यास भाग पडेल.

जो-जॉबर हे व्यवसाईक असू शकतात जे आपल्या प्रतिस्पर्ध्याला नुकसान पोहचवण्याच्या दृष्टीने हे करत असतात,किंवा त्यांचा राजकीय हेतू हि असू शकतो.

38. *किस्ट्रोक लॉगिंग*

किस्ट्रोक लॉगिंग (किलॉगिंग किंवा किलॉगर्स) म्हणजे गुप्तपणे वापर कर्त्याच्या नकळत किबोर्डच्या वापरल्या जाणाऱ्या प्रत्येक किची नोंद ठेवली जाते. किबोर्ड वापरणाऱ्या व्यक्तीस माहित नसते कि त्याच्या हालचालींवर देखरेख ठेवली जात आहे. किस्ट्रोक लॉगिंग करण्याच्या बऱ्याच पद्धती आहेत ज्यात, हार्डवेअर, सॉफ्टवेअर आधारित किलॉगिंग ते इलेक्ट्रोमॅग्नेटिक, अकाऊस्टिक्सवर आधारित किलॉगिंगचा समावेश होतो.

किलॉगर हे एक हार्डवेअर उपकरण किंवा छोटा प्रोग्राम असू शकतो, जो कि किबोर्डवरती घडणाऱ्या प्रत्येक कृतीची नोंद करून ठेवत असतो. हार्डवेअर किलॉगर हे छोटॅ बॅटरी सारखे असते जे युझरचा किबोर्ड आणि कॉम्प्युटरमध्ये कनेक्टरचे काम करतो, हे उपकरण एका छोटॅ प्लग सारखे दिसत असल्यामुळे देखरेख ठेवणे सोपे जाते आणि कुणाच्याही लक्षात येत नाही. जसे युझर किबोर्ड वरती काही टाईप करतो तेव्हा हे उपकरण सर्व किस्ट्रोकस सेव्ह करून ठेवते. आणि नंतर हा सेव्ह केलेला डाटा आपल्याला पाहता येऊ शकतो, अशा प्रकारे आपण हि माहिती गोळा करू शकतो. किलॉगर प्रोग्रामला कॉम्प्युटरला फिजीकल ॲक्सेस असण्याची जरुरी नसते, ज्याला याचा वापर करायचा आहे तो हा प्रोग्राम युझरच्या कॉम्प्युटरवर डाऊनलोड करून ठेवू शकतो.

39. *लॉजिक बॉम्ब*

लॉजिक बॉम्ब हा एक प्रकारचा कोड असतो जो मुद्दामहून सॉफ्टवेअर प्रोग्राममध्ये ठेवलेला असतो, जो कि योग्य वेळी कॉम्प्युटर हार्डड्राइव्ह वरील डाटा अल्टर, डिलीट, किंवा करप्ट करू शकतो. लॉजिक बॉम्ब सॉफ्टवेअर प्रोग्राममध्ये गुप्तपणे ठेवलेला असतो जो विशिष्ट गोष्टी घडे पर्यंत सुप्त अवस्थेत राहतो.

एखाद्या प्रोग्राम मध्ये हा कोड असेल तर तो एखादी लॉजिकल कंडीशन पूर्ण नाही झाली तर तो कोड एक्झीक्युट होईल, उदा: पेरोल फाईलमध्ये जर एखादयाचे नाव दिले नसेल तर. लॉजिक बॉम्ब हा एक ट्रोजन हॉर्सचा प्रकार आहे,आणि अनेक व्हायरस हे लॉजिक बॉम्ब असतात.

उदाहरण:

TSA च्या कोलोराडो स्प्रिंग ओपरेशन सेंटर मधून ऑक्टोबर २००९ साली डाटा अनालिस्ट डग्लस डुचक यांची नोकरीवरून हकालपट्टी झाली. कारण देखरेख ठेवण्यासाठी असलेल्या कॅमेऱ्यातून असे दिसून आले कि त्याने CSCO सर्व्हर ज्यावर U.S. मार्शलचा डाटा होता त्यामध्ये लॉजिक बॉम्ब लोड केला. जानेवारी २०११ मध्ये डग्लसला दोन वर्ष कारावास आणि ६०,५८७ डॉलर्स दंड आणि तीन वर्ष प्रोबेशन अशी शिक्षा झाली होती.

जून २००६ मध्ये UBS Paine Webber मधील या आर्थिक कंपनीतील असंतुष्ट सिस्टम ॲडमिनीस्ट्रेतर रॉजर दुरोनिओ याने लॉजिक बॉम्ब वापरून कंपनीच्या नेटवर्कचे नुकसान केले. लॉजिक बॉम्बचा वापर करून कंपनीच्या स्टोकची किमंत पाडण्याचा प्रयत्न केल्यामुळे त्याच्यावर सेक्युरिटी घोटाळ्याचा ठपका ठेवण्यात आला. दुरोनिओ नंतर दोषी ठरवण्यात आला आणि त्यास ८ वर्ष आणि १ महिन्याचा कारावास आणि ३. १ मिलियन डॉलरचा दंड झाला.

40. लॉटरी स्क्याम

लॉटरी स्क्याम हा ॲडव्हान्स फी स्क्यामचा प्रकार आहे ज्याची सुरवात एका ईमेल पासून होते ज्याचा विषय "You have won!" **असा असतो आणि ज्यात म्हंटले असते कि आपण एका लॉटरीमध्ये खूप पैसे जिंकला आहात. आपणास ह्या बाबत गुप्तता पाळण्यास सांगितली जाते, आणि पुढील माहिती साठी क्लेम एजंटशी संपर्क करण्यास सांगण्यात येते, क्लेम एजंटशी संपर्क केल्यानंतर आपणास प्रोसेसिंग फी किंवा ट्रान्स्फर फी मागण्यात येते, तुम्ही जर हि फी भरली तरी लॉटरीची रक्कम आपणास मिळत नाही कारण हा सर्व आपल्याला फसवण्यासाठी बनाव रचलेला असतो. आणि जर आपण हि फी भरली नाही तर या संदर्भातले ईमेल आपल्याला सतत येत राहतील. काही वेळेस आपल्याला एका बँकेत खाते उघडून त्यात पैसे भरण्यास सांगण्यात येईल, पण हि बँक बोगस असते,ह्या प्रकारचे घोटाळे करण्यासाठी मोठमोठया कंपनींच्या नावाचा वापर केला जातो.**

उदाहरण:

३५ वर्षीय नायजेरिअन तरुण जो ओझोया इसैन नावाने ओळखला जातो त्यास ऑनलाईन लॉटरी स्क्याम मध्ये लोकांना करोडो रुपयास लुटल्याच्या आरोपावरून दिल्लीत अटक करण्यात आली. पुण्यातील एका रहिवासाच्या तक्रारीचा तपास करताना पोलिसांनी त्याला

पकडले होते, त्या माणसाला त्याने २२ लाख रुपयाला फसवले होते, त्याचे असे म्हणणे होते की त्याला लॉटरी जिंकल्याचा एक मेसेज आला होता त्याला उत्तर दिल्या नंतर पुढील प्रकार घडला होता.

२००८ मध्ये याहूने नायजेरिअन आणि थाय गटाच्या विरोधात खटला दाखल केला होता कारण कि हे गट ऑनलाईन लॉटरी स्क्याम करत होते, ज्यात ते लोकांना असे सांगत होते कि ते याहू कडून चालवल्या जाणारी लॉटरी जिंकले आहेत. याहूला या खटल्याच्या निकालात ६१० मिलियन डॉलर मिळाले.

हिल्सबर्ग, क्यालिफोर्नियातील ८९ वर्षाच्या एका वृद्ध स्त्रीला असे वाटत होते कि ऑस्ट्रेलिअन सरकारी लॉटरी मध्ये ७.५ मिलिअन डॉलर जिंकले आहेत आणि हि रक्कम मिळवण्यासाठी ७०,००० डॉलर व्हयानकोव्हानेर नावाच्या गुप्त अशा स्वीत्झ बँकेत भरले, पण नंतर त्यांच्या लक्षात आले कि हा सर्व एक घोटाळा आहे.

41. *ईमेल बॉम्बिंग*

ईमेल बॉम्बिंग मध्ये पिडीत व्यक्तीस खूप मोठया प्रमाणावर ईमेल पाठवले जातात ज्यामुळे त्याचे ईमेल अकाउंट किंवा मेलसर्व्हर क्र्याश होतो. ईमेल बॉम्बिंग हे ठराविक डीनायल ऑफ सर्व्हिसचे ठराविक उदाहरण आहे ज्यात सर्व्हरला ईमेलचा पूर पाठवण्यात येतो ज्यामुळे सर्व्हर काम करण्यास अक्षम बनून बंद पडतो ज्यामुळे त्याचे इतर ॲक्सेस बंद होतात.

उदाहरण:

एका ब्रिटीश तरुणाने त्याच्या माजी मालकाच्या विरोधात डीनायल ऑफ सर्व्हिसचा हल्ला करून त्याचा सर्व्हर बंद पाडला होता. पण UK कॉम्प्युटर गैरवापर कायद्या अंतर्गत डीनायल ऑफ सर्व्हिसचा हल्ला गुन्हा नसल्याने कोर्टाने त्याची निर्दोष म्हणून मुक्तता केली.

उदाहरण:

भारतात सिमल्यामध्ये ३० वर्ष पासून राहत असलेल्या एक परकीय व्यक्तीस सिमला हौसिंग बोर्डच्या योजनेचा लाभ घ्यायचा होता, पण हि योजना फक्त भारतीय नागरिकांसाठी असल्यामुळे त्याचा अर्ज नाकारण्यात आला, हॅ गोष्टी वर चिडून सिमला हौसिंग बोर्डला खूप ईमेल्स पाठवून सर्व्हर क्र्याश केला.

42. मालवेअर

मालवेअर हे मालीशियस सॉफ्टवेअरचे संक्षिप्त रूप आहे, हे सॉफ्टवेअर हॅकरकडून घुसखोरी, नुकसान, कॉम्प्युटर सिस्टीम बंद पडण्यासाठी, संवेदनशील माहिती मिळवण्यासाठी, खाजगी कॉम्प्युटर सिस्टमला ॲक्सेस मिळवण्यासाठी वापरले किंवा तयार केले जाते. हे सॉफ्टवेअर असल्या कारणाने स्क्रिप्ट किंवा कोडच्या स्वरुपात असते.

मालवेअर मध्ये कॉम्प्युटर व्हायरस, वोर्म, ट्रोजनहॉर्स, स्पायवेअर, आणि इतर मलिशिअस प्रोग्रामचा समावेश होतो. US मधील बऱ्याच राज्यांच्या कायद्यामध्ये मालवेअरला कॉम्प्युटर कन्टेनमेंट असे म्हणतात. काही मालवेअर छुप्या पद्धतीने अस्सल सॉफ्टवेअर म्हणून कंपनीच्या वेबसाईट कडून बाजारात येतात. मालवेअर मुख्यत्वे करून गैर वापरासाठीच अंमलात आणले जाते. मालवेअर आपले ब्राउझर हायजॅक करून आपल्या सर्च रीडायरेक्ट करू शकते. बरेच मालवेअर तुम्ही त्यांना अनइनस्टोल केल्यावर परत रिइनस्टोल होतात. जर योग्य खबर घेतली नाही तर वैयक्तिक आणि नेटवर्कड कॉम्प्युटर मालवेअर धोक्यान पछाडू शकतात.

43. नायजेरीअन ४१९ फ्रौड स्कीम

नायजेरीअन ४१९ फ्रौड स्कीम हि एक चलाखी आहे ज्यात लक्ष्य असलेल्या व्यक्तीला हे पटवून सांगण्यात येते, की जर त्याने आत्ता थोडे पैसे देऊ केले तर नंतर त्याला खूप पैसे मिळतील. ४१९ हा आकडा, नायजेरीअन दंड संहिता कलम ४१९ मधून आलाय ज्या अंतर्गत फसवणूक केल्यास त्या व्यक्तीस शिक्षा होते. हा घोटाळा नायजेरीया पुरता सिमित नाही, पण नायजेरीअन लोक या घोटाळ्याशी संलग्न झाल्यामुळे यास नायजेरीअन ४१९ फ्रौड स्कीम म्हणून ओळखण्यात येते. २००५ मध्ये नायजेरीयातील लागोस घोटाळ्यासाठी जगभरात अग्रणी होते.

काही उदाहरण :

नवीन एक फ्रौड स्कीम आहे ज्यात नौकरीच्या वेबसाईटवर आपला बायोडाटा पोस्ट करणार्यांना लक्ष्य करण्यात येते. यात खोटा कंपनीचा लोगो वापरून पत्र पाठवण्यात येते,ज्यात उत्तम पगार आणि बाकीचे फायदे दाखवलेले असतात, पण त्या ठिकाणी काम करण्यासाठी परवानगी लागते असे लिहिलेले असते.आणि सरकारी अधिकारी म्हणून एक खोटा संपर्क दिलेला असतो, ज्याच्या वर संपर्क केल्यावर तो या परवानगीसाठी काही रक्कम मागतो, अमी हि रक्कम मिळवण्यासाठीच हा घोटाळा केलेला असतो. काही वेळेस ऑनलाईन कमी किमती मध्ये कार विकण्यास आहे अशी जाहितात करून लोकांना लुबाडण्यात येते. ह्या

ठिकाणी घोटाळा करणारा सांगतो कि मी देशाच्या बाहेर असतो पण तुम्ही माझ्या खात्यावर जर पैसे टाकलेत तर माझा मित्र आपणास गाडी आणून देईल. अशाच प्रकारे ऑनलाईन डेटिंग साईटवरती आकर्षक फोटो पोस्ट करून बऱ्याच जणांची फसवणूक केली जाते.

उदाहरण :

जानेवारी ५, २०१२ रोजी एक साउथ कोरिअन ६५ वर्षाच्या माणसास आणि ३० वर्षीय त्याच्या मुलीस फसवून साउथ आफ्रिकेला बोलावण्यात आले आणि तिथे त्यांचे अपहरण झाले, त्यानंतर अपहरणकर्त्यांनी साउथ कोरिआतील त्यांच्या कुटुंबाकडून पैशाची मागणी केली. त्यांच्या कुटुंबाने लगेच साउथ आफ्रिकेतील वाकालतीत संपर्क साधला. अपहरणकर्त्यांच्या तावडीतून त्यांचा ड्राइव्हर निसटून गेला, ज्यांनी स्थानिक पोलिसांना याची माहिती दिली, नंतर पोलिसांनी त्यांची सुटका केली.

उदाहरण:

फेब्रुवारी २००३ मध्ये जिरी पासोवास्की, या ७२ वर्षीय पिडीत व्यक्तीने एका घोटाळ्यात ६ लाख डॉलर घालवले होते, नायजेरीअन कौन्सेल जनरल ने हे पैसे परत करता येऊ शकत नाही असे सांगितल्यामुळे त्या पीडिताने प्राग मधील नायजेरीअन वकलतीत काम

करणाऱ्या मायकल लेकारा वाहिद याचा खुन केला आणि अजून एका व्यक्तीला दुखापत केली.

44. पॅकेट स्निफिंग

इंटरनेट वरील सर्व डाटा वेग वेगळ्या डाटा पॅकेटस मध्ये फिरत असतो. सामान्य कॉम्प्युटर हे काही पाहू शकत नाही पण बरेच स्पायवेअर गुप्तपणे युझरच्या कॉम्प्युटर मधील संवेदनशील माहिती बाहेर पाठवत असतात. पॅकेट स्निफिंग म्हणजे नेटवर्क मध्ये फिरणारे पॅकेटस कॅपचर करणे, म्हणजेच हे एक अस तंत्र आहे ज्यात आपण दुसऱ्या व्यक्तीचा डाटा चोरून घेऊ शकतो (स्निफ करू शकतो). पॅकेट स्निफरचा प्रशासकीय कामासाठी किंवा हॅकिंग टूल म्हणून वापर करता येतो, जे कि युझरवरती अवलंबुन आहे. नेटवर्क स्निफर नेटवर्क मधील पासवर्ड किंवा इतर संवेदनशील माहिती क्यापचर करू शकतात.

45. फिशिंग आणि स्पुफिंग हल्ले:

एक जुनी मराठी म्हण आहे "दिसत तस नसत म्हणून जग फसत . "

१९ व्या शतकात ब्रिटीश कलाकार आर्थर रॉबर्ट्स यांनी एक खेळाचा शोध लावला ज्याचे नाव स्पुफ होते, ज्याच्या मध्ये चलाखी आणि मुर्खपणाचा समावेश होता. ह्यामुळे इंग्रजी बोलणाऱ्या जगाला एक नवीन शब्द मिळाला जो हॅकिंग तंत्रज्ञानाचे प्रतिनिधित्व करतो. स्पुफिंग हल्ल्या मध्ये मुख्यत्वे करून ईमेल स्पुफिंगचा, SMS स्पुफिंग, IP स्पुफिंग, आणि वेब स्पुफिंगचा समावेश होतो. स्पुफिंग हल्ल्याचा उपयोग लोकांना फसवून त्यांच्या कडून माहिती काढून घेण्यासाठी किंवा त्यांच्या कडून असे कृत्य करून घेण्यासाठी केला जातो जे सहसा त्यांनी केले नसते.

अशा प्रकारच्या स्पुफिंग हल्ल्याला सामान्यतः फिशिंग असे हि म्हणतात. दुसऱ्याच्या ईमेल आयडी वापरून मेल पाठवणे हे सगळ्यात सध्या प्रकारचे ईमेल स्पुफिंग आहे.

उदाहरण:

बऱ्याच बँकेच्या ग्राहकांना त्यांचा युझरनेम आणि पासवर्ड तपासण्यासाठी ईमेल आला. हा ईमेल स्पुफ्ड होता तरी हजारो लोकांनी यातील लिंकवरती क्लिक केले,आणि नंतर ओपन झालेल्या वेबपेजवरती

आपली माहिती देऊन टाकली. याचा तपास केल्यावर असे लक्षात आले कि हा ईमेल एका असंतुष्ट कर्मचार्याने पाठवला होता.

उदाहरण :

एका ग्लोबल IT कंपनीच्या हजारो कर्मचार्यांनी आलेला ईमेल आपल्या बॉस कडून आल्याचे समजून उघडल्यामुळे सगळ्यांच्या कॉम्प्युटरवर व्हायरस इनस्टोल झाला होता. ईमेल मध्ये सांगितल्या प्रमाणे सगळ्यांनी अन्टी व्हायरस सॉफ्टवेअर डिसेबल करून ठेवले होते. तपासातून असे निष्पन्न झाले कि तो ईमेल एका प्रतिस्पर्धी कंपनीने पाठवला होता.

SMS स्पुफिंग हे ईमेल स्पुफिंग सारखेच असते, पण सगळ्यात मोठा हा फरक असतो कि ईमेल आयडीच्या ऐवजी फोन नंबरचा वापर केला जातो.

उदाहरण:

एका तरुण मुलीस तिच्या नवऱ्याच्या मोबाईल नंबर वरून मेसेज आला कि त्याचा अपघात झाला आहे आणि तो हॉस्पिटल मध्ये आहे, आणि त्याला त्वरित पैशाची गरज आहे. असा मेसेज पाहिल्यावर ती त्वरित घरी जाऊन पैसे घेते आणि हॉस्पिटलकडे जाण्यास निघते तेव्हा स्पुफ मेसेज पाठवणारा तिच्यावर हल्ला करून पैसे घेऊन पळून जातो.

इंटरनेटशी जोडलेल्या कॉम्प्युटरची मुख्य ओळख हा त्याचा IP अड्रेस असतो. म्हणून गुन्हेगार लोकांना फसवण्यासाठी IP स्पुफिंगचा वापर करतो. IP स्पुफिंग प्रोक्झी सर्व्हर वापरून किंवा एक साधी php स्क्रिप्ट वापरून देखील करता येते.

उदाहरण:

सरकारने घातलेल्या बंधना पासून(सेन्सॉरशिप) वाचण्यासाठी बरेच इंटरनेट वापरणारे प्रोक्झी सर्व्हरचा उपयोग करतात.(हि गोष्ट योग्य आहे कि अयोग्य यावर आम्ही कोणतेही भाष्य करत नाही.)

उदाहरण:

एका गुन्हेगाराने सरकारी कॉम्प्युटर हॅककरून संवेदनशील माहिती चोरली, पण त्याचा तपास केल्यावर पुरावा एका वरिष्ट सरकारी अधिकार्याकडे खुणावत होता, पण तो अधिकारी स्वच्छ चारित्र्याचा असल्यामुळे त्यास अटक झाली नाही, नंतर अधिक तपासात असे आढळून आले कि यात स्पुफिंगचा वापर करण्यात आला होता.

DNS **स्पुफिंग**:

यात डोमेन नेम सिस्टमशी छेडछाड केली जाते, ज्यामुळे पीडित व्यक्ती बनावट वेबसाईटला खरी वेबसाईट समजतो. म्हणजे तुम्ही www.asianlaws.org **टाईप कराल पण कोणतीतरी दुसरीच साईट ओपन होईल! आणि अशा प्रकारच्या गोष्टी स्थानिक आणि आंतरराष्ट्रीय पातळीवर देखील झालेल्या आहेत.**

उदाहरण:

ग्लोबल फायनानशिअल सर्व्हिस कंपनीतील शेकडो लोकांना एका प्रसिद्ध ऑनलाईन स्टोर कडून ईमेल आला ज्यात काही DVDs **आणि पुस्तक मोठया सवलतीवर उपलब्ध होती, या ईमेल मधील लिंक वरती क्लिक केल्यावर एक खोटी साईट ओपन होत असे जी खऱ्या सारखीच दिसत असते,बर्याच जणांनी आपले क्रेडीट कार्ड वापरून ऑर्डर दिली, पण कोणाला काही मिळाले नाही आणि महिन्याच्या शेवटी मोठे क्रेडीट कार्ड बिल आले. याबाबती तपास केल्यावर असे आढळले कि नेटवर्क ॲडमिनीस्ट्रेटरनीच हा फिशिंग हल्ला केला होता.**

46. *पिग्गी बॅकिंग*

दुसऱ्याच्या वायरलेस कनेक्शनच्या क्षेत्रात आपला कॉम्प्युटर नेऊन त्याचे वायरलेस इंटरनेट कनेक्शन त्याच्या नकळत किंवा परवानगीशिवाय वापरणे याला पिग्गी बॅकिंग म्हणतात. जगातील वेगवेळ्या कायद्याच्या अधिकार क्षेत्राप्रमाणे हे कायदेशीर किंवा नैतिकदृष्टॅ वादग्रस्त प्रथा आहे. अवैध गोष्टी लपवण्यासाठी पिग्गी बॅकिंगचा उपयोग केला जातो उदा: लहान मुलांचे अश्लील व्हीडीओ डाऊनलोड करणे, ओळख चोरी करणे हे सर्व काहीही पुरावा मागे न ठेवता केल्याने, याची सर्व जबाबदारी नेटवर्कच्या मालकाकडे जाते. समजा एक ग्राहकाने हॉटेलकडून उपलब्ध करून दिलेली वायफाय सुविधा वापरतो यास पिग्गी बॅकिंग म्हणता येणार नाही,तरी पण जे लोक हॉटेलचे ग्राहक नाहीत किंवा हॉटेलच्या आवारातील लोकांनी वायफाय सुविधा वापरली तर त्यांना पिग्गीबॅकर्स म्हणतात. पिग्गी बॅकिंग हे वॉर ड्रायव्हिंग पेक्षा वेगळे आहे. वॉर ड्रायव्हिंग असुरक्षित वायरलेस ॲक्सेस पोइंटची माहिती नेटवर्क सर्व्हिसचा वापर नकरता गोळा करते.वॉर ड्रायव्हिंग मध्ये लोगिंग किंवा ॲक्सेस पोइंटच म्यापिंग केले जाते, तर अनाधिकृत पणे नेटवर्कचा वापर करण्याला पिग्गी बॅकिंग म्हणतात.

47. पायरसी ऑफ सॉफ्टवेअर

इतर गोष्टी जशा तुम्ही विकत घेऊन त्याची मालकी मिळवता, तसे सॉफ्टवेअरच्या बाबतीत नसते. त्याऐवजी तुम्ही त्याचे परवानाधारक वापरकर्ते बनत असता, तुम्ही सॉफ्टवेअर एक कॉम्प्युटरवर वापरण्यासाठीचे हक्क विकत घेत असता, आणि तुम्ही हे सॉफ्टवेअर एकच कॉम्प्युटरवर वापरू शकता,इतर कुणालाही ते तुम्ही देऊ शकत नाही. सॉफ्टवेअर पायरसी म्हणजे अवैध पणे वितरण, सॉफ्टवेअर अनधिकृत पुनरुत्पादन व्यवसाय किंवा वैयक्तिक वापरासाठी करणे. सॉफ्टवेअर पायरसी मुद्दामहून केली असो वा नसो ती अवैधच आहे आणि कायद्याने शिक्षेस पात्र आहे.

सॉफ्टवेअर पायरसीची मुळ १९६० च्या सुरवातीच्या काळात सापडतील, जेव्हा कॉम्प्युटर प्रोग्राम मेनफ्रेम हार्डवेअर बरोबर मोफत वितरीत केली जात होती. १९६० मध्ये उत्पादक सॉफ्टवेअर, हार्डवेअर पेक्षा अलग विक्री करू लागले. सॉफ्टवेअर डेव्हलपर चांगले सॉफ्टवेअर तयार करण्यासाठी खूप मेहनत घेत होते. आणि जर सॉफ्टवेअर जर पायरेटेड असेल तर तर त्यांचा महसुल बुडेल त्याचे कंपनीला नुकसान होईल. अशा प्रकारे सॉफ्टवेअर पायरसीची संपुर्ण जागतिक अर्थव्यवस्थेवर परिणाम करू शकते. अर्थतंज्ञानच्या मते २००७ मध्ये सॉफ्टवेअर पायरसीची मुळे ३९. ६ बिलिअन डॉलर्स नुकसान झाले आहे. सॉफ्टवेअर पायरसी म्हणजे बरेच जॉब, पगार घालवणे आणि हि एक अयोग्य स्पर्धा

देखील आहे. सॉफ्टवेअर पायरसीशी झगडण्यासाठी काही कंपनी अन्ती सॉफ्टवेअर पायरसी तंत्रज्ञानाचा वापर करतात ज्याची परिणीती चांगली उत्पादन आणि सेवा देण्याचा वेग कमी होतो.

अन्ती- कॉपीराईट इंफ्रींजमेंट संस्था:

Business Software Alliance (BSA)

Canadian Alliance Against Software Theft (CAAST)

Entertainment Software Association (ESA)

Federation Against Software Theft (FAST)

International Intellectual Property Alliance (IIPA)

उदाहरण:

२००८ साली चीनमध्ये ११ लोकांना नॅशनल कॉपीराईट कायद्याचे उल्लंघन आणि मायक्रोसोफ्टच्या सॉफ्टवेअरचे उच्च प्रतीची बनावट तयार करून विकल्याबद्दल त्यांना दोषी ठरवण्यात आले. ह्या लोकांचा गट आंतरराष्ट्रीय पातळीवर उच्च दर्जाच्या आणि व्यवस्थित पणे प्याकिंग केलेल्या CDs **आणि** DVDs **निर्माण करून विकत होता. अंती पायरसी उपाय योजून सुद्धा हा प्रकार घडला होता. या संस्थेने** Windows XP **आणि** Office 2007 **सारखे सॉफ्टवेअर पायरसी करून प्रचंड प्रमाणात तयार केले.**

आणि त्याची सर्व इंटरनेटद्वारे विक्री केली व चीनमधून अमेरिका आणि युरोपला निर्यात केली. आंतरराष्ट्रीय पातळीवर त्यांची २ बिलियन डॉलरच्या वरती विक्री झाल्याचे सांगण्यात आले. गुन्हेगारी कॉपीराईट इंफ्रींजमेंट अंतर्गत तो दोषी ठरवण्यात आला होता.

48. पॉड स्लरपिंग

पोर्टेबल डाटा स्टोरेज उपकरण जसे कि iPOD, USB **स्टिक्स , फ्लॅश ड्राइव्ह**, PDAs **आणि ऑडिओ प्लेयरचा वापर करून डाटा चोरी करणे म्हणजे पॉड स्लरपिंग. अवैधपणे मोठया प्रमाणावर संवेदनशील आणि गोपनीय माहिती संस्थेच्या कॉम्प्युटर सिस्टममध्ये थेट एक फ्लॅश ड्राइव्ह जोडून डाऊनलोड करता येते. आजकाल हे स्टोरेज उपकरण आकाराने लहान पण स्टोरेज क्षमता वाढवत आहेत, ज्यामुळे कंपनी आणि सरकारी एजन्सीसाठी सेक्युरिटी धोका होऊन बसल्या आहेत. पॉड स्लरपिंग हे हॅकरच्या भात्यातला नवीन बाण आहे. आणि याचा उपयोग फक्त उच्च प्रतीचे हॅकरच नाहीतर नवोदित हि करू शकतात. यासाठी जरूर आहे ती फक्त एक उपकरण,स्लरपिंग सॉफ्टवेअर आणि कॉम्प्युटरला ते जोडण्याची संधी.**

२००४ मध्ये सेक्युरिटी तज्ञ अबे उशर याने एक प्रोग्राम तयार केला ज्याचे नाव "slurp.exe" **होते, आणि त्यांनी त्याचा** iPOD **वरून कॉम्प्युटर वरून माहिती कशी सोप्या पद्धतीने स्लरप करता येते याचे प्रात्येक्षिक दाखवले. ह्या प्रोग्राममुळे वर्ड आणि एक्सेल फाइल्स शोधणे अगदी सोपे झाले.**

उदाहरण:

गोलू हा त्याच्या वार्षिक कामगिरी पुनरावलोकन आणि पगार वाढ न झाल्यामुळे दुःखी होता ,त्याने याचा बदला म्हणून त्यांच्या ह्युमन रिसोर्सचा कॉम्प्युटर ॲक्सेस करायचे ठरवले. त्यांनी त्याचा iPOD वापरून त्या कॉम्प्युटर मधून स्लरप करून सर्व माहिती डाउनलोड केली .

49. *पॉयझनिंग द सोर्स*

या प्रकरणात आपण पाहणार आहोत कि कशा प्रकारे सॉफ्टवेअर बाजारात येण्यापूर्वीच त्यात ट्रोजन इन्सर्ट केला जातो ! सॉफ्टवेअर डेव्हलपमेंट आणि टेस्टिंगच्या वेळेसच हॅकर सॉफ्टवेअर ट्रोजनाइज करू शकतात. हॅकर सॉफ्टवेअर डेव्हलपमेंट कंपनीत काम करू शकतो किंवा ओपन सोर्स सॉफ्टवेअर डेव्हलपमेंट मध्ये मदत करू शकतो. एक डेव्हलपर किंवा टेस्टर म्हणून कोड मध्ये छोटासा बॅकडोर इंस्टाल करू शकतो. जो कि शेकडो मेगाबाईटच्या अधिकृत कोड मध्ये हुडकणे खुप अवघड आहे. हे सॉफ्टवेअर घेणारे नकळत ट्रोजनाइज झालेल सॉफ्टवेअर त्यांच्या कॉम्प्युटरवर इंस्टाल करतात.

केन थोम्पसन, UNIX चे सहनिर्माते आणि C प्रोग्रामिंग लॅग्वेजचे गुरु, यांनी सोर्स कोडवर नियंत्रण ठेवण्याबाबत चर्चा केली होती आणि कदाचित त्यात बॅकडोर प्लांट केले होते, त्यांच्या १९८४ सालचा पेपर ज्याचे नाव होते "Reflections on Trusting Trust,". त्यात त्यांनी वर्णन केले होते कि कशा पद्धतीने कंम्पायलरचा सोर्स कोड बदलू शकतो ज्यामुळे तो प्रत्येक कंम्पाइल करणाऱ्या प्रोग्राम मध्ये बॅकडोर तयार करेल. हा हल्ला खरोखरच भयानक होता.

थोम्पसन यांच्या शब्दात,

“You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. In demonstrating the possibility of this kind of attack, I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect.

A well installed microcode bug will be almost impossible to detect”.

हा प्रकार सॉफ्टवेअर साईट ट्रोजनाइज करण्यापेक्षा भयानक आहे. जेव्हा हल्लेखोर सॉफ्टवेअर वितरण साईट ट्रोजनाइज करतो,तरी सॉफ्टवेअर डेव्हलपरकडे खरी प्रत सुखरूप असते. जिचा पडताळणीसाठी वापर केला जाऊ शकतो. पण जर सॉफ्टवेअर मधेच ट्रोजन एम्बेड केलेला असेल तर आपल्याकडे क्लीन प्रत देखील नसेल. जर हल्लेखोर हुशार असेल तर तो संपूर्ण कोड मध्ये छोटे बॅकडोर ठेवेल, जेणे करून ते काढून टाकणे खूप अवघड होऊन बसेल. सॉफ्टवेअरची सचोटी तपासण्यासाठी सॉफ्टवेअर डेव्हलपरला प्रचंड प्रमाणात कोड स्कॅन करावा लागत असतो, त्यामुळे जेवढा मोठा कोड तेवढाच बॅकडोरचा शोध अवघड होऊन जातो.

कोड मधील चुका शोधणे हे फार महागड होऊन बसलय, सॉफ्टवेअर ट्रोजनाइज करण्यासाठी त्या हल्लेखोराला पूर्ण बॅकडोर सुद्धा

लिहायची गरज नसते. त्याएवजी मालीशीअस डेव्हलपर दोष असलेला कोड तयार करेल ज्यामुळे हल्लेखोराला त्याचे काम सोपे होऊन जाईल. याची फक्त डेव्हलपरला माहिती असल्यामुळे तो त्याचा कोड वापरून कोणतीही सिस्टम नियंत्रित करू शकतो. वेगवेगळे सर्वे आणि विश्लेषण सांगतात कि १००० ओळींच्या कोड मध्ये १०० ते १५० ओळी अपघाताने या डेव्हलपरकडून चुकीच्या लिहिल्या जातात, निश्चित पणे हि चूक नकळतच होत असते. यातील बऱ्याचशा चुका या चुकीच्या सिनटॅक्समुळे होतात, पण काही दोष सुरक्षेच्या दृष्टीने गंभीर असू शकतात. खरेतर या मागील हेतू हल्ले खोराचा उद्देश साध्य करणे असा असतो. मायक्रोसोफ्ट XP ओप्रेटींग सिस्टमच्या अंदाजे ४५ मिलियन लाईनचा कोड आहे! मग ह्याचा अर्थ असा होतो का कि त्यात ४,५०,००० दोष आहेत? या बद्दल कुणालाच माहिती नाही. पण एक गोष्ट नक्की XP ओप्रेटींग सिस्टम जेव्हा बाजारात रिलीज झाली तेव्हा मायक्रोसोफ्टने मेगाबाईट्स मध्ये पॅच रिलीज केल्या होत्या.

50. *पोर्नोग्राफी*

पोर्नोग्राफी किंवा अश्लीलतेची कोणतीही निश्चित व्याख्या अस्तित्वात नाही. जी गोष्ट अमेरिकेत फक्त लैंगिक समजली जाते तीच गोष्ट भारतात अश्लील समजली जाऊ शकते. इंटरनेटवरती अश्लील मजकूर हटवण्याच्या संदर्भात जगभरातून सरकार आणि कायद्याची अंमलबजावणी करणाऱ्याकडून प्रयत्न सुरु आहेत पण यात खूप कमी यश मिळाले आहे. इंटरनेटवर पोर्नोग्राफी विविध स्वरुपात उपलब्ध आहे. यात फोटो, व्हिडीओ, साउंड फाईल, आणि गोष्टींचा समावेश होतो. इंटरनेट देखील कॉम्प्युटर स्क्रीनवरून अशा प्रकारचे अश्लील चाळे करण्यास बढावा देत. जर भारतीय संविधान भाषा आणि अभिव्यक्ती स्वातंत्र देत असल तरी, अश्लीलते विरोधातील कायदे संविधानिक आहेत. सर्वोच्य न्यायालयाने अश्लीलते बाबत म्हण्टले आहे " विनयशीलता किंवा सभ्यतेला आक्षेपार्ह; असभ्य, अश्लील."

उदाहरण:

डिसेंबर २००१ मध्ये सायबर पोर्न केस मध्ये एका फास्ट ट्र्याक कोर्टाने चेन्नई मधील हाडाचे डॉक्टर प्रकाश यांना जन्मठेप आणि बाकी ३ जणांना वर्षाची सक्त मजुरीची शिक्षा झाली. प्रकाश यांनी एक महिलेचे

नग्न चित्र त्यांच्या US मधील भावाच्या मदतीने इंटरनेटवर पोस्ट केले होते.

उदाहरण :

दिल्ली पब्लिक शाळेच्या १७ वर्षीय मुलाने एक २.३७ मिनिटांचा एक पोर्नोग्राफिक MMS तयार केला होता,त्याचे अवैध वितरण केले आणि Baazee.com वर त्याचा लिलाव पण केला. अवनीश बजाज Baazee.com चे CEO यांना दिल्ली हाय कोर्टाने या संदर्भात बोलावून चौकशी केले होती , कि हा MMS आपल्या साईटवर लिलाव करण्यासाठी आपण परवानगी दिलीच कशी? त्या क्लिप मधील दोघ अल्पवयीन असल्यामुळे त्यांना कोणतीही शिक्षा झाली नाही.

51. robots.txt ***फाईल***

robot **प्रोग्राम आपोआप इंटरनेटवरील साईटसला भेट देतो आणि मग सर्व सलग्न फाईल्स पुनर्प्राप्त करतो. वेब रोबॉटसला काही वेळेस वेब वांडरर, क्राउलर किंवा स्पायडर म्हणूनही संबोधले जाते. हि गोंधळात टाकणारी नाव आहेत कारण कि यावरून असे वाटते कि सॉफ्टवेअर स्वतःच साईटसवरती व्हायरससारखा फिरत असतो. पण असे काही होत नाही, रोबॉट फक्त साईटसला विझिट करतो आणि त्यांच्या कडून डोक्युमेंटची मागणी करतो.**

रोबॉटसची लिस्ट आणि त्यांची वैशिष्टे पाहण्यासाठी:

http://www.robotstxt.org/wc/active.html

सर्व रोबॉटसला वेबसाईट विझिट करण्यापासून रोखण्याकरिता सर्व्हरवरील robots.txt **फाईलमध्ये खालील दोन ओळी टाईप करा**

User-agent: *

Disallow: /

उदाहरण:

User-agent: webcrawler

Disallow: /tmp

Disallow: /logs

चा अर्थ असा होतो कि webcrawler **नावाचा रोबॉट** /tmp or /log **ने सुरु होणाऱ्या वेबसाईट विझिट करू शकणार नाही**. **वेबमास्टर** robots.txt **फाईल अशा प्रकारे तयार करतो कि संवेदनशील माहितीला रोबॉट विझिट करू शकणार नाही**. **हॅकर** robots.txt **फाईलचे विष्लेषण करून ठरवू शकतो कि वेबसाईटच्या कोणत्या भागावर हल्ला करायचा आहे**.

52. *पोर्ट स्क्यानिंग*

कॉम्प्युटरच्या भाषेत पोर्टची दुहेरी व्याख्या आहे. खुद्द कॉम्प्युटरला अनेक प्रकारचे पोर्ट असतात. प्लग इन माउस, कीबोर्ड, USB डिव्हायसेस, प्रिंटर इ . पोर्ट असतात. मात्र, माहितीच्या सुरक्षेच्या दृष्टीने TCP/IP मधील व्हरचुअल पोर्ट जास्त संबंधित असतात. TCP/IP हा इंटरनेटवरील मुलभूत असा संवाद प्रोटोकॉल आहे. पोर्ट हे तुमच्या कॉम्प्युटरवरील चॅनेल सारखे असतात. साधे वेब किंवा http ट्र्याफिक पोर्ट ८० चा वापर करते , POP३ ईमेल पोर्ट ११० चा वापर करतो.हे पोर्ट तुम्ही चाली बंद करून तुमच्या नेटवर्क वरील येणारा जाणारा डाटा नियंत्रित करू शकता. पोर्ट स्क्यानिंग हे सुरक्षा रक्षकाने त्याच्या सभोवताली फिरून प्रत्येक घराची दार, खिडक्या तपासल्या सारख आहे. पोर्ट स्क्यानिंग म्हणजे पद्धतशीर पणे कॉम्प्युटर पोर्ट स्कॅन करणे होय. पोर्टचा वापर करूनच माहिती कॉम्प्युटर मध्ये येजा करत असल्याने, पोर्ट स्क्यानिंग मुळे कुठले पोर्ट ओपन आहेत हे समजते. पोर्ट स्क्यानिंग अधिकृत पणे नेटवर्कचे काम करण्यासाठी वापरले जाते, पण याचा नेटवर्क मधील दुर्बल ॲक्सेस बिंदु शोधण्यासाठी गैरवापर करता येतो. कोणकोणत्या सर्व्हिस सुरु आहेत हे तपासण्यासाठी हि पोर्ट स्क्यानिंगचा वापर केला जातो. एखादा प्रोग्राम दुर्बलता शोधण्यासाठी कॉम्प्युटर किंवा नेटवर्कला सतत माहिती मागत असेल तर त्यास पोर्ट स्कॅनर म्हणतात. जगभरात इंटरनेटवर संवाद साधण्यासाठी TCP/IP प्रोटोकॉलचा वापर

केला जातो ज्यात TCP (Transmission Control Protocol) आणि UDP(User Datagram Protocol) चा समावेश असतो. यात प्रत्येकी ० ते ६५५३५ पोर्ट असतात,म्हणजे कॉम्प्युटरला ६५,००० पेक्षा जास्त दरवाजे असतात. त्यातील पहिले १०२४ पोर्ट हे सुप्रसिद्ध आहेत ज्यांचा संबंध HTTP, FTP (File Transfer Protocol) SMTP (Simple Mail Transfer Protocol) किंवा DNS (Domain Name System) अशा सर्विसेसशी येतो. पोर्टच्या सविस्तर माहितीसाठी http://www.iana.org/assignments/port-numbers भेट द्या. जर कुणी वाईट हेतूने पोर्ट स्क्यानिंग करत असेल तर नेटवर्क ॲडमिनीस्ट्रेटर सेक्युरिटी सॉफ्टवेअरचा वापर करू शकतो जे अशा प्रकरच्या घटना घडताना सुचित करेल. पण यापासून वाचण्यासाठी हल्लेखोर स्टेल्थ मोडचा वापर करू शकतो. लक्ष्य असलेल्या कॉम्प्युटरचे सर्वच पोर्ट स्कॅन करण्यापेक्षा ठरविक पोर्ट स्कॅन करावेत, यामुळे स्क्यानिंगसाठी कमी वेळ लागेल आणि कुणाच्या लक्षात हि येणार नाही. अशा प्रकारे पोर्ट स्कॅन करण्याचे अनेक प्रकार आहेत.

53. *रूटकिटस*

कॉम्प्युटरची दुर्बलता वापरून किंवा पासवर्ड क्रयाक करून युझर पात्रतेची ॲक्सेस मिळाल्यावर एक क्रयाकर सर्व प्रथम कॉम्प्युटरवर रूटकिट इंस्टाल करतो. एकदा का रूटकिट इंस्टाल झाले कि क्रयाकरला कॉम्प्युटरची रूट किंवा विशेष ॲक्सेस मिळते आणि कदाचित नेटवर्क वरील इतर मशीनलाही. रूटकिट मध्ये स्पायवेअर किंवा इतर प्रोग्राम असू शकतात जे ट्र्याफिक किंवा किस्ट्रोकवरती देखरेख ठेवतात, हॅकरसाठी बॅकडोरची निर्मिती करतात, लॉग फाईलमध्ये बदल करतात किंवा नेटवर्क मधील इतर मशीनवर हल्ला करतात. रूटकिटचा शोध घेणे अवघड आहे कारण त्याचा शोध घेणाऱ्या सॉफ्टवेअरलाच ते बंद पाडते. यासाठी ओप्रेटिंग सिस्टम परत इंस्टाल करणे हाच एक उपाय आहे. जेव्हा फर्मवेअर रूटकिटचा प्रश्न असतो तेव्हा ते हटवण्यासाठी हार्डवेअरच बदलून टाकावे लागेल.

54. सालामी थेफ्ट

आर्थिक गुन्हेगारी करण्यासाठी अशा प्रकारचा हल्याचा उपयोग केला जातो. यातील गाभा असा आहे कि एखादा बदल इतक्या छोट प्रमाणात करा कि कुणाच्याही नजरेस पडणार नाही. असे समजा कि, एका बँक कर्माचाऱ्याने बँकेच्या सर्व्हरमध्ये एक प्रोग्राम ठेवला जो प्रत्येक ग्राहकाच्या खात्यातून फार थोडी रक्कम वजा करतो (उदा: २ रुपये). हि अनधिकृत पणे वजावट झालेली रक्कम सहजपणे कुणाच्याही निदर्शनास येणार नाही. पण त्या बँक कर्माचाऱ्याकडे खुप रक्कम जमा होत असेल. मग ह्याला सालामी हल्ला का म्हणायचे? काही सुरक्षा तज्ञानच्या मते हा प्रकार म्हणजे डाटा अलगदपणे बारीक कापल्या सारख आहे. तर काही जण म्हणतात कि हे सलामी सारखं छोट छोट तुकडया पासून मोठी गोष्ट तयार करण्यासारखं आहे.

उदाहरण:

जानेवारी १९९३ मध्ये USA फ्लोरिडा मधील एक रेंटल कार शाखेतील ४ कार्यकारी अधिकाऱ्याना सालामी हल्ला वापरून कमीत कमी ४७,००० लोकांना फसवल्याबद्दल शिक्षा झाली होती. त्यांनी कॉम्प्युटर मधील बिलींग प्रोग्राम मध्ये फेरफार करून त्यांच्या वाहनामध्ये जास्तीचे ५ ग्यालन ग्यास भरण्याची सोय केली होती. १९८८ पासून १९९१ पर्यंत

प्रत्येक ग्राहकाने चढवलेल्या दराने पैसे भरले होते, तो दर २ ते १५ डॉलर पर्यंत वाढीव होता, जी पिडीत व्यक्तींना समजण्यासाठी अवघड होता.

उदाहरण:

जानेवारी १९९७ मध्ये USA मेरीलॅंड विल्स रॉबिन्सन यांना त्यांचे Taco Bell drive-up-window क्याश रजिस्टर रीप्रोग्राम करून पैशाची अफरातफर केल्याबद्दल १० वर्षाची कारावासाची शिक्षा झाली होती. हा प्रकार उघडकीस येई पर्यंत त्यांनी ३६०० डॉलर कमावले होते. अगोदर हा प्रकार हार्डवेअर किंवा सॉफ्टवेअर मधील दोष आहे असे वाटत होते पण याबाबती आपल्या सहकाऱ्यान समोर बढाई मारताना विल्स यांना पाहिल्यावर हा प्रकार उघडकीस आला.

उदाहरण:

तेजा नावाच्या एका गुन्हेगाराने बँकेचा कॉम्प्युटर वापरून वेगवेगळ्या ग्राहकांच्या खात्यातून थोडे पैसे आपल्या बनावट खात्यावर ट्रान्स्फर करत होता. तो एका वर्षात एका ग्राहकाच्या खात्यातून फक्त तीनच वेळा पैसे काढायचा. त्यामुळे ग्राहकाच्या एवढी छोटी बाब लक्षात येत नव्हती.

उदाहरण:

होलु होलु बँकेतील श्रीयुत सोनावाला ग्राहकाच्या मासिक स्टेटमेंटमधील अपूर्णांक संख्या, नजीकच्या पूर्ण संख्ये मध्ये बदलत होते. त्यांनी त्याच बँकेत एक बनावट खाते उघडले होते ज्यात हि फेरफार केलेली रक्कम जमा होत होती.

55. *अवैध वस्तूंची विक्री*

अंमली पदार्थ औषधे, हत्यारे, वन्यजीव इ वस्तूंची इंटरनेट वापरून बेकायदेशीर पणे विक्री करणे वरचेवर वाढत आहे. अशा प्रकारच्या वस्तुची माहिती विक्रीसाठी लिलावाच्या वेबसाईटवर किंवा बुलेटीन बोर्डवर पोस्ट केली जाते . प्रत्यक्षात गुन्हेगाराना अशा प्रकारे अवैध वस्तूंची विक्रीकरण्यासाठी वेबसाईटची निर्मिती करण्यापासून रोखणे अश्यक्य आहे. याव्यतिरिक्त, काही ऑनलाईन पेमेंट गेटवे आहेत जे एका बटन क्लिकवर जगभरात कुठेही पैसे ट्रान्स्फर करता येतात. इंटरनेटने देखील अशा प्रकारच्या वस्तूंच्या विक्रीसाठी एक प्रकारचे मार्केट उपलब्ध करून दिलेले आहे. काही वेबसाईट अवैध पणे औषधांची विक्री करतात. जो एक गंभीर प्रश्न होऊन बसला आहे. व्यापक पोहोच, निनावीपणा,जुन्या वेबसाइट काढून आणि नवीन तयार करणे सहज करू शकत असल्यामुळे कायद्याची अंबलबजावणी करणारयांचे काम कठीण होऊन बसले आहे.

उदाहरण:

मार्च २००७, पुणे ग्रामीण पोलिसांनी एक अवैध रेव पार्टी वर छापा घालून शेकडो लोकांना अवैध पणे ड्रग्स वापरताना पकडले होते. सोशल नेटवर्किंग साईट Orkut.com वरून या अवैध ड्रग्स पार्टीचे आयोजन करण्यात आले होते.

56. *स्क्यावेनजिंग*

स्क्यावेनजिंगला डम्पस्टर डायविंग म्हणूनही ओळखले जाते. स्क्यावेनजिंग म्हणजे दुसऱ्याच्या कचऱ्यामध्ये खजिना शोधणे. हा शोध फक्त कोड आणि पासवर्डसारख्या खजिन्या पुरता मर्यादित नसतो तर, यात संवेदनशील माहितीचाही (पत्ते,फोन नंबर, क्रेडिट कार्ड पावत्या, सामाजिक सुरक्षा नंबर,कॅलेंडर किंवा त्यांचा संघटनात्मक तक्ता) समावेश होतो.अशा प्रकारचा डाटा हल्लेखोरास कॉम्प्युटर किंवा नेटवर्क ॲक्सेस करून गुन्हा करण्यासाठी मदत करतो.

उदाहरण:

२०१० मध्ये विलिअम फ्रेलिक्स आणि अजून ११ जणांना इतर लोकांची ओळख आणि क्रेडीट कार्ड नंबर वापरून १,००,००० डॉलर पेक्षा जास्त वस्तू आणि सेवा खरेदी केल्या होत्या. विलिअम फ्रेलिक्स या सर्व टोळीचा प्रमुख होता ज्यांनी इतर लोकांना वेगवेगळ्या हॉटेल्स मध्ये जाऊन लोकांना जाळ्यात अडकवण्यासाठी पाठवले होते.

57. *स्मिशिंग*

SMS आणि फिशिंग या दोन्हीच्या मिश्रणातून स्मिशिंग हा शब्द तयार झाला आहे. हे फिशिंग सारखेच आहे ज्यात आपल्याला बनावट ईमेल येतात,पण यामध्ये ईमेलची जागा टेक्स्ट SMS घेतो जो तुमच्या फोनवर येतो.

उदाहरण:

कुणालला त्याच्या फोनवर एक मेसेज आला ज्यात एक लिंक होती आणि बॉलीवूड आणि हॉलीवूडच्या अभिनेत्रीचे फोटो पाहण्यासाठी ती वापरा असे सांगण्यात आले होते. त्या लिंकवर क्लिक केल्यावर wow.com हि साईट ओपन झाली ज्यावर प्राण्यांचे गमतीदार व्हीडीओ होते, पण दहा मिनिटाच्या आतच कुणालचा फोन क्ष्याश झाला.

उदाहरण:

जोयच्या मोबाईलवर मेसेज आला कि तो एका स्पर्धेमध्ये आपण ५०० रुपयाचा बॅलन्स जिंकला आहात, आणि हा बॅलन्स मिळवण्यासाठी आपल्याला एक मेसेज पाठवावा लागेल. मेसेज पाठवल्या नंतर जोयच्या लक्षात आले कि त्याला कोणताही बॅलन्स न मिलता उलट त्याचा असलेला बॅलन्सच संपून गेला.

58. सोशल इंजिनिअरिंग

कॉम्प्युटरच्या जगात हि अतांत्रिक अशी गोष्ट आहे ज्यात एखाद्या व्यक्तीला फसवून त्याच्या नकळत संवेदनशील किंवा गोपनीय माहिती काढून घेणे म्हणजे सोशल इंजिनिअरिंग होय.सोशल इंजिनिअरिंगमध्ये पीडीत व्यक्तीला मानसिक पातळीवर भुरळ घालून त्याकडून पाहिजे ती माहिती काढून घेतली जाते, त्यामुळे हा घोटाळा आहे हे त्याच्या लक्षातच येत नाही. यातील बऱ्याच प्रकरणान मध्ये हल्लेखोर, पीडीताच्या समोरच न येता हे काम करतो. लोकांना त्यांच्या जवळच्या माहितीची किंमत माहित नसल्यामुळे हल्लेखोर या गोष्टीचा फायदा घेतात. एक सोशल इंजिनिअर नेहमी एक बनाव तयार करत असतो ज्याद्वारे लोकांच्या चांगुल पाणाचा गैरफायदा उठवतो.

उदाहरण:

एका व्यक्तीने AOL च्या टेक सपोर्टला फोन लावून तेथील कर्मचाऱ्याशी एक तास बोलला,ज्यात त्याने अशी माहिती दिली कि त्याची कार खूप चांगल्या किंमतीत विकण्यासाठी तो तयार आहे. त्या कर्मचाऱ्याने यात रस दाखवल्याने त्याने एका ईमेलवरून त्याला कारचा फोटो पाठवला. कारच्या फोटो ऐवजी एक बॅकडोर ओपन झाला आणि फायरवॉल मधून AOL साठीचे एक कनेक्शन ओपन झाले. ज्यामुळे त्यास AOL च्या अंतर्गत नेटवर्कला प्रवेश मिळाला, ज्याद्वारे काही सिस्टीमची

सुरक्षेशी तडजोड करण्यात आली आणि २०० पेक्षा जास्त खात्यांचा गोपनीय डाटा उघड करण्यात आला.

59. स्प्यामबॉट

स्प्यामबॉट स्वयंचलित कॉम्प्युटर प्रोग्राम असतो, जो अनपेक्षित पणे अनपेक्षित भरपूर मेसेज पाठवतो.

हे प्रोग्राम इंटरनेटवर वेब, न्युजरूम,चॅटरूम इ. वरून भरपूर ईमेल अड्रेस गोळा करतो आणि या सर्वांची एक लिस्ट तयार करून ईमेल पाठवतो ज्यास स्प्याम असे म्हणतात.

साधारणतः यासाठी बनावट ईमेल खाती उघडण्यात येतात आणि स्प्याम पाठवले जातात,तर काही स्प्यामबोट पासवर्ड क्र्याक करून दुसऱ्या लोकांचे ईमेल खाते वापरून स्प्याम पाठवतात.

वर्ष २०११ मध्ये पाठवल्या गेलेल्या स्प्याम मेसेजची संख्या जवळ जवळ ७ ट्रिलियन च्या घरात होती.

स्प्यामबोटचे अनेक प्रकार आहेत:

स्प्याम: ईमेल वरून अनेपेक्षित पणे भरपूर प्रमाणात पाठवले जाणारे ईमेल

स्पिम: इंस्टंट मेसेंजर वरून स्प्याम पाठवणे

स्प्याट: इंटरनेट टेलिफोनी वरून स्प्याम पाठवणे स्पायवेअर:

स्पायवेअर हा एक मालवेअर सॉफ्टवेअरचा प्रकार आहे जो युझरच्या नकळत त्याचा कॉम्प्युटरवर इंस्टाल केलेला असतो जो युझर पासून लपलेला असतो ज्यामुळे त्याचा शोध लागणे अवघड असते.स्पायवेअर युझरच्या हालचालींवर देखरेख ठेवतात. वैयक्तिक माहिती हि त्यांच्याकडून गोळा केली जाते ज्यात युझरच्या इंटरनेटवरील सर्व हालचालींची माहिती असते. युझरच्या कॉम्प्युटर नियंत्रण करण्याच्या हि ते आड येतात जसे कि जास्तीचे सॉफ्टवेअर इंस्टाल करणे, अनावश्यक साईटसला भेट देणे, इ. स्पायवेअर कॉम्प्युटर सेटिंग हि बदलू शकतात ज्यामुळे कनेक्शनचा वेग कमी होईल.

उदाहरण:

मुव्हीलॅंड किंवा Moviepass.tv किंवा Popcorn.net या नावाने हि ओळखली जाणारी हि एक मुव्ही डाऊनलोड सेवा आहे, ज्याच्या नावाने फेडरल ट्रेड कमिशन आणि इतर संस्थानकडे हजारो तक्रारी दाखल झाल्या आहेत. ग्राहकांची अशी तक्रार आहे कि या साईटवर पैसे भरणा करण्यासाठी सारखे पोप अप येतात आणि असा मेसेज असतो कि , आपण या सुविधेसाठी तीन दिवसासाठी प्रायोगिक तत्वावर वर्गणीदार होता पण तुम्ही वेळीच आपलं सद्यसत्व रद्द न केल्यामुळे तुम्हास २९.९५ डॉलर

भरणे आवश्यक आहे.पण ग्राहकांनी असे काहीही केलेले नव्हते. मग FTC ने मुव्हीलॅडच्या विरोधात तक्रार दाखल करून घेतली,आणि फसवून आणि जुलमी पद्धतीने ग्राहकांकडून पैसे वसुल करण्याचा आरोप ठेवला.

60. SQL ***इंजेक्शन***

SQL **इंजेक्शन अनेक हल्ल्याच्या तंत्रापैकी एक आहे, ज्याद्वारे हॅकर वेबसाईट वरून डेटाबेस मधला डाटा चोरू शकतो. हा प्रकार वेब अप्लीकेशनच्या अयोग्य कोडींगचा गैरफायदा घेऊन हॅकर** SQL **इंजेक्शनचा वापर करून वेबसाईटचा डेटाबेस ॲक्सेस करतात. हे वेब एन्ट्री फोर्ममध्ये** SQL **स्टेटमेंट इनपुट करून अंमलात आणले जाते. या मागील मुख्य उद्देश वेबसाईट सॉफ्टवेअरच्या दुर्बलतेचा फायदा उठवणे हा असतो.**

उदाहरण:

२०११ मध्ये लेडी गागाची वेबसाईट US **मधील** SwagSec **नावाच्या सायबर हल्ला करणाऱ्या गटाकडून हॅककरण्यात आली होती,आणि तिच्या हजारो चाहत्यांची वैयक्तिक माहिती चोरण्यात आली होती. हॅकरसनी कन्टेन डेटाबेस डम्प** www.ladygaga.co.uk **या साईटवरून घेतला आणि ईमेल, पहिले आणि शेवटचे नाव ॲक्सेस केले, व तिच्या चाहत्यांना हि बरेच बनावट मेसेज पाठवण्यात आले होते.**

ऑगस्ट २००९ मध्ये एक अमेरिकी नागरिक अल्बर्ट गोन्झालीस आणि दोन निनावी रशिअन वर SQL **इंजेक्शन वापरून १३० मिलियन क्रेडीट कार्ड नंबर्स चोरल्याचा आरोप ठेवण्यात आला होता.**

61. स्टीलवेअर

स्टीलवेअर हे एक असे सॉफ्टवेअर आहे जे वेबसाईटचे सलग्न कोड फेरफार करून आणि सलग्न कुकीज बदलून प्रभावीपणे वेबसाईटच्या मालकाचे पैसे तृतीय पक्षाला पोहचवते.

उदाहरण:

एक साईट जी इतर साईटसला संदर्भ देऊन कॉस्ट पर ॲक्शन नुसार भले पैसे कमावतात. यात ते युझरला साईटची लिंक फॉलो करयला लावतात ज्यावरून तो काही खरेदी करेल आणि अशा रेफरलसाठी त्यांना काही फी मिळेल. पण दुसऱ्या व्यक्तींनी त्यांचे ट्र्याकिंग कोड बदलून स्वतःचे सेट केले व त्यांचे पैसे आपल्याकडे वळवून घेतले.

हे स्टीलवेअर आहे.

62. *टाइम बॉम्ब*

टाइम बॉम्ब हा एक प्रोग्राम किंवा बॅच फाईल असते जी एका विशिष्ट वेळी हानी पोहचवते. म्हणूनच याचे नाव टाइम बॉम्ब कारण जेव्हा कॉम्प्युटरची तारीख पूर्वनियोजित वेळेस पोहचते त्या वेळेस बरोबर कॉम्प्युटरला काही तरी हानी करण्यात येते. हा असा एक कॉम्प्युटर प्रोग्राम आहे जो योग्य वेळी आपले काम करण्याचे थांबवू शकतो. याचा बहुत करून असंतुष्ट आणि अप्रामाणिक लोकांकडून वापर केला जातो.

उदाहरण:

१९९२ मध्ये The Michelangelo व्हायरस प्रत्येक वर्षी मार्चच्या ६ तारखेला हार्डडीस्क डिरेक्टरी डयामेज करण्यासाठी बनवण्यात आला होता.

उदाहरण:

१९८८ साली Jerusalem नावाचा व्हायरस तयार करण्यात आला होता. जो महिन्याच्या शुक्रवारी आणि १३ तारखेला स्वतःला डुप्लीकेट करत होता, ज्यामुळे कॉम्प्युटर स्लो होत असे.

63. ट्रोजन हॉर्स

१२ व्या शतकामध्ये, ग्रीसने ट्रोय नावाच्या शहरा बरोबर युद्ध पुकारले. स्पार्टाची राणी, ट्रोयच्या युवराजाचा हात धरून पळून गेल्यामुळे या भांडणाची सुरवात झाली. म्हणजेच असे कि त्यांची लग्न करायची इच्छा होती. ग्रीकांनी १० वर्षे ट्रोयशी लढा दिला पण यश नजरेच्या टप्प्यात येत नव्हते. ट्रोय अतिशय मजबूत होते. शेवटच्या प्रयत्नात ग्रीक सेनेने माघार घेतल्याचे ढोंग केले,आणि एका प्रचंड लाकडी घोडयात लपून बसले. ट्रोयच्या लोकांना हे ग्रीकांनकडून भेट आहे असे वाटले. त्यांनी तो घोडा त्यांच्या शहरात आणून ठेवला, त्याच्या आत ग्रीक सैनिक लपलेत याची त्यांना कल्पनाच नव्हती. नंतर रात्री अंधाराचा फायदा घेऊन ते त्या घोड्यातून बाहेर पडले आणि ट्रोय शहरावर हल्ला चढवून ते नष्ट केले.

त्याच प्रमाणे कॉम्प्युटर मधील ट्रोजन हॉर्स, एक गोष्ट करतोय असे ढोंग करतो पण त्याचा उद्देश संपुर्ण पणे दुसरे काही तरी करण्याचा असतो. या धडयामध्ये Ed Skoudis यांच्या लिखाणातील उतारा Addison Wesley यांच्या सौजन्याने देण्यात आला आहे.

ट्रोजन हॉर्स प्रोग्राम हा काहीतरी उपयोगाचा आहे असे प्रथम दर्शनी वाटते पण तो काहीतरी मालीशीयस कार्यक्षमता लपवत असतो. आजकालचे ट्रोजन हॉर्स अशाच प्रकारची युक्ती वापरून कॉम्प्युटरची

सुरक्षा तोडून प्रवेश करतात,साधारण प्रकारचे सॉफ्टवेअरसारखे दिसून खालील प्रकारची कामे करतात.

१. युसर किंवा सिस्टीम ॲडमिनीस्ट्रेटरला भुलवून प्रथम ट्रोजन हॉर्स इंस्टाल करयला लावतात. याठिकाणी ट्रोजन हॉर्स इतर मलिशिअस सॉफ्टवेअरसाठी एन्ट्री पोइंट बनेल.

२. कॉम्प्युटर मधील इतर प्रोग्राम बरोबर मिसळून जाणे. ट्रोजन कॉम्प्युटरचाच एक प्रोग्राम आहे असे भासवतात त्यामुळे ह्यात काही गडबड आहे असा कुणाला संशय येत नाही.

हल्लेखोर लोकांनी मलिशिअस कोड लपवण्याचे निरनिराळे पर्याय शोधून काढले आहेत. यात साधा पण अतिशय कार्यक्षम असा नेमिंग गेम तैनात करणे, एक्झिक्यूटेबल ऱ्यापरचा वापर, सॉफ्टवेअर वितरण साईटवरती हल्ला करणे, सोर्स कोडमध्ये फेरफार करणे, पॉलीमोर्फीक तंत्राचा वापर करून गोष्टींचे सोंग घेणे.

ट्रोजनचे प्रकार:

१. रिमोट अडमिनीस्ट्रेशन ट्रोजन (RATs):

हे खुप प्रसिद्ध ट्रोजन आहेत, हे हल्लेखोराला पीडीताची हार्डडिस्क ॲक्सेस करू देतात, तसेच त्यावर विविध कार्य देखील करू शकतात.

आधुनिक RATs वापरायला खूपच सोपे आहेत. ते दोन फाईल सोबत जोडून येतात, सर्व्हर फाईल आणि क्लायंट फाईल. हल्लेखोर कुणाला तरी भुलवून सर्व्हर फाईल वापरावयास लावतो, ज्यामुळे त्यास कॉम्प्युटरचा IP अड्रेस मिळतो आणि पीडीताच्या कॉम्प्युटरचे पुर्ण नियंत्रण. काही ट्रोजन हल्लेखोराला पोर्ट बदलण्याची संधी देतात, ज्याला पासवर्ड हि ठेवता येतो जेणे करून ज्याने एखादा कॉम्प्युटर इन्फ़ेक्ट केला आहे तोच त्या ट्रोजनचा वापर करू शकतो. काही प्रकरणात हल्लेखोर सर्व्हर फाईल मध्ये स्वतःच बॅकडोर ठेवतो ज्यामुळे त्याला इन्फ़ेक्टेड कॉम्प्युटरचा पासवर्ड न वापरता हि ट्रोजन हाताळता येतो. या प्रकाराला बॅकडोर मधील बॅकडोर असे म्हणतात. उदा: CIA, Netbus, Back Orifice, Sub7.

२. पासवर्ड ट्रोजन:

पासवर्ड ट्रोजन पीडिताच्या कॉम्प्युटरवरती पासवर्डचा शोध घेतात आणि तो डाटा हल्लेखोराला किंवा ट्रोजनच्या निर्मात्याला पाठवला जातो. इंटरनेट पासवर्ड असु देत किंवा ईमेल पासवर्ड प्रत्येकासाठी ट्रोजन असतो. सहसा हे सर्व ट्रोजन मिळालेली माहिती हल्लेखोराला ईमेलद्वारे पाठवतात.

३. विशेषाधिकार वाढवणारे ट्रोजन:

सहसा सिस्टीम ॲडमिनीस्ट्रेटरला मुर्ख बनवण्यासाठी या ट्रोजनचा वापर होतो. एक तर ते सध्या सिस्टीम युटीलिटी मध्ये असतात,

किंवा निरुपद्रवी प्रोग्रामचे सोंग घेतात, किंवा काहीतरी कामचे किंवा उपयोगी असल्याचे भासवतात. जर एकदा का सिस्टीम ॲडमिनीस्ट्रेटरने हा ट्रोजन रन केला तर हल्लेखोराला सिस्टीमवर जास्त विशेषाधिकार मिळतील. हा ट्रोजन कमी विशेषाधिकार असलेल्यांना देखील पाठवला जातो आणि हल्लेखोराला त्यांच्या खात्याचा ॲक्सेस मिळतो.

४. कि लोगर्स: हे विघातक नसतात

हे ट्रोजन अतिशय साधे असतात. हे पीडीताच्या कीबोर्ड वरील प्रत्येक कृतीची नोंद हल्लेखोराला ईमेल करतो. कि लोगर्सला जास्त स्टोरेज जागा लागत नाही त्यामुळे त्यांना शोधणे फार कठीण होऊन बसते.

५. जोक प्रोग्राम्स:

जोक प्रोग्राम्स हे विघातक नसतात. ते तुमची हार्डडीस्क फोरमॅट करायचं, किंवा सर्व पासवर्ड हल्लेखोराला पाठवण्याच सोंग घेतील किंवा तुमच्याकडे असलेल्या अवैध अथवा पायरेटेड सॉफ्टवेअरची माहिती पोलिसांना देतो असे सांगतील पण यापैकी ते काहीच करत नाहीत.

६. विघातक ट्रोजन:

हे ट्रोजन पीडीताची पूर्ण हार्डडीस्क खराब करतील, एन्क्रीप्ट करतील किंवा महत्वाच्या फिल्डस गायब करतील. काही जोक प्रोग्राम्ससारखे वाटतील पण प्रतेक्षात ते प्रत्येक फाईल नष्ट करत असतात.

भारतातील एका नोंद न झालेल्या प्रकरणात ट्रोजनमुळे एका पत्रकारचा मृत्यु झाला असता.

ऑनलाईन नातेसंबंधानवर एक तरुण महिला एक लेख लिहित होती. यासाठीचा अभ्यास करण्यासाठी ऑनलाईन बऱ्याच लोकांशी मैत्री केली होती. त्यापैकी एकाने तिच्या कॉम्प्युटरवरती ट्रोजन इंस्टाल केला. ती मुंबई मध्ये एका छोट घरात राहत होती आणि तिथेच तिचा कॉम्प्युटर होता. या कॉम्प्युटरला जोडलेला वेब कॅमेरा आणि मायक्रोफोन ट्रोजनने हायजॅक केला आणि तिची प्रत्येक कृती रेकॉर्ड करत होता, आणि त्यातील बऱ्याच वैयक्तिक गोष्टी त्यानी वेबवरती पोस्ट केल्या, आणि एक वर्षा नंतर जेव्हा तिला हि गोष्ट समजली तेव्हा तिने आत्महत्या करायचा प्रयत्न केला,पण सुदैवाने ती बचावली. ट्रोजन वापरून इतक्या भयानक गोष्टी हि करता येतात.

UK चाइल्ड पोर्न केस:

ब्रिटीश नागरिक जुलिअन ग्रीन यांना ऑक्टोबर २००२ मध्ये अटक झाली होती पोलिसांनी त्याचा घरावर छाप टाकला होता आणि त्यांना त्याच्या कॉम्प्युटर हार्डडीस्कवर १७२ मुलांचे असभ्य फोटो मिळाले होते. ग्रीन US डिफेन्स मध्ये IT कंत्राटदार होते त्यांना दोन मुले होती आणि ते घाटस्पोटीत होते. पीडोफाइल असल्याच्या १३ खटले त्याच्या विरोधात असल्याने त्याची नोकरी गेली होती आणि त्याच्या मुलांना तो भेटू शकत नव्हता. अशा प्रकारचे फोटो बाळगल्याबद्दल ब्रिटीश कायद्यानुसार १० वर्षाची कारावासाची शिक्षा आहे आणि असे दोष कुणाबाबतीत सिद्ध झाल्यास त्याचे पोलिसांकडे ५ वर्षासाठी सेक्स ओफेनडर म्हणून नोंद असेल. ग्रीन यांचे असे म्हणणे होते कि त्यांचा या फोटोशी काही संबंध नाही त्यांना यात रस नाही, त्यांच्या घरी असल्या कोणत्याही प्रकारचे साहित्य आढळणार नाही. ते एक प्रामाणिक आणि सरळ मार्गी व्यक्ती आहेत जे काम करतात जिथ पूर्ण तपासणी करूनच कामावर घेतले जात. ग्रीन यांच्या कॉम्प्युटरची सखोल तपासणी केल्यावर पोलिसांना त्यावर ११ ट्रोजन हॉर्स सापडले जे अवैधपणे कुणाच्या न कळत अयोग्य अशा साईटला भेट देत होते,ग्रीन यांना हा ट्रोजन स्प्यामद्वारे मिळाला होता. मग त्यांची या आरोपातून मुक्तता करण्यात आली.

अशा प्रकारे ट्रोजनचा गैर वापर करता येतो.

2. टेक्सास पोर्ट DOS केस:

आरोन क्याफ्री एक १९ वर्षीय UK **चा नागरिक, त्याच्यावर टेक्सास मधील ह्युस्टन येथिल सिस्टीम क्र्याश केल्याचा आरोप होता. अनधिकृत पणे कॉम्प्युटर मध्ये फेरफार केल्याबद्दल** UK **कोर्टामध्ये शिक्षा झाली होती. खटला चालू असताना असे लक्षात आले कि आरोन क्याफ्रीने फार मोठया गुन्हाची योजना केली होती, ज्यात कॉम्प्युटर हॅकिंग, ओळख चोरी, आणि इतर आर्थिक गुन्ह्यानचा समावेश होता. वकिलाचा असा दावा होता कि क्याफ्री हा प्रकार केला होता कारण कि बुक्की नावाच्या एका महिलेशी त्याचा विवाद झाला होता आणि त्याचा सूड उगवण्यासाठी त्याने हे केले होते. त्याचे असे म्हणणे होते की** US **विरोधी वक्तव्य त्या महिले केल्यामुळे त्यांच्यात वाद झाला होता. क्याफ्री हा एका आजरा पासून पीडित होता त्याचे नाव** Asperger **सिंड्रोम असे होते जो एक ओटीझमचा प्रकार आहे, आणि त्याचे असे पण म्हणणे होते कि जेसिका नावाच्या अमेरिकन मुलीवर त्याचे प्रेम आहे,आणि त्याने त्याच्या कॉम्पुटरचे नाव जेसिकाच ठेवले आहे व हि आटयक स्क्रिप्ट तिलाच समर्पित केली आहे, २० सप्टेंबर २००१ रोजी पोर्ट वरील सर्व कॉम्प्युटरवर हा हल्ला त्याने नियोजित केला होता. हल्ल्यामुळे पोर्टची वेबसाईट बंद पडून सर्व महत्वाची कामे ठप्प झाली होती. जेव्हा तपासात पोलिसांना हल्लेखोराचा** IP **अड्रेस मिळाला जो क्याफ्रीच्या घरचा पत्ता दाखवत होता,**

पण त्याचे असे म्हणणे होते कि कुणीतरी तीसऱ्याच व्यक्तीने त्याची वेबसाईट वापरून हा हल्ला केला आहे, आणि तसेच पोलिसांनी आपले काम नीट केले नाही म्हणून त्याने टिका केली. तपासाच्या शेवटच्या टप्प्यात क्याफ्रीने काबुल केले कि तो Allied Haxor Elite नावाच्या हॅकर ग्रुपचा सदस्य आहे पण त्याने आजपर्यंत एक हि कॉम्प्युटर हॅक नाही केला. त्याने असे सांगितले कि या गटातील सर्व हॅकर कायदेशीर पणे काम करतात म्हणून त्यांना क्रयाकर असे हॅकर म्हणतात ,आणि मी हे कॉम्प्युटर त्याची सुरक्षा तपासण्यासाठी पूर्व परवानगीने हॅक केले होते. कोर्टाने क्याफ्रीचे म्हणणे मान्य केले आणि त्यास निर्दोष मुक्त केले. कोणीतरी ट्रोजन वापरून हा हल्ला केला होता.

उदाहरण :

२००२ मध्ये सप्टेंबर २८ ते ऑक्टोबर आठवडाभर, सर्व प्रसिद्ध ईमेल सर्व्हर सॉफ्टवेअरचे वितरण करणाऱ्या साईटला बंद पाडण्यात आले होते. यासाठी जो मुख्य FTP सर्व्हर होता तोच ट्रोजनने इन्फेक्ट करून त्यात बॅकडोर तयार करण्यात आले होते.

64. URL मॅनीपुलेशन

URL हे Uniform Resource Locator चे संक्षिप्त रूप आहे, हा वेबपेजचा वेब अड्रेस असतो. URL मॅनीपुलेशन वेब सर्व्हर ॲडमिनीस्ट्रेटरच्या सोयीनुसार व हल्ले खोराकडून गैरफायद्यासाठी केल जातो. URL मॅनीपुलेशन मध्ये युझर जेव्हा एखादी साईट व्हीझीट करण्यासाठी प्रयत्न करतो तेव्हा तो एका बनावट साईटला रिडायरेक्ट होतो जी त्याच्या कॉम्प्युटरवर मालीशीअस कोड इन्सर्ट करू शकते. URL चा वापर करून इंटरनेट गुन्हे करणे आजकाल सामान्य बाब झाली आहे. कारण कि हे करणे सोपे आहे. URL म्यानीपुलेशन जर आपल्याला फिशिंग साईटकडे घेऊन जात असेल तर ते भयानक आहे, सहसा हे असच होते कारण फिशिंग साईट ओळखणे अवघड असते. जर तुम्ही URL तपासला नाहीतर खरी आणि फिशिंग साईट ओळखणे अवघड आहे.

उदाहरण :

URL मॅनीपुलेशनचा वापर करून २०१० मध्ये AT&T च्या वेबसाईटवरून iPOD धारकांचा ईमेल आणि इतर माहिती मिळवली होती. हॅकरनी सिटी अकाउंट ऑनलाईन सिस्टीम मधील दोषाचा फायदा उचलून २,००,००० क्रेडीट कार्ड धारकांची माहिती चोरली होती. त्याच्या URL मध्ये ग्राहक खाते क्रमांकावरून हि सिस्टीम चालत होती आणि नुसती तो आकडा बदलून माहिती ॲक्सेस करता येत होती.

65. *व्हायरस हल्ला*

कॉम्प्युटर व्हायरस हा मानव निर्मित प्रोग्राम किंवा कोड असतो जो पीडित व्यक्तीच्या माहिती शिवाय एखाद्याच्या कॉम्प्युटरवर लोड केला जातो आणि त्याच्या इच्छे विरुद्ध चालवला जातो.व्हायरस स्वतःची पुनर्निर्मिती करून जे कि सोपे आहे, अगदी साधा व्हायरस हि भयानक आहे कारण तो सिस्टीम करप्ट करतो. या पेक्षा हि भयानक व्हायरस सुरक्षा व्यवस्थेला फाटा देऊन नेटवर्कवरती पसरतो. व्हायरस ईमेल अटॅचमेंट, डाऊनलोड प्रोग्राम म्हणून किंवा CD तून पाठवू शकतो. ईमेल अटॅचमेंट, डाऊनलोड प्रोग्राम किंवा CD पाठवणाऱ्याला हे माहित नसते कि त्यात व्हायरस आहे.

काही व्हायरस लगेच कार्यरत होतात तर काही तसेच राहतात आणि ठराविक वेळेस कार्यरत होतात.

ईमेल व्हायरस हा ईमेल अटॅचमेंट बरोबरच असतो आणि खूप जणांना जातो, काही वेळेस तर या वर डबल क्लिक न करताही हा कार्यरत होतो. व्हायरसमुळे खालील प्रकारचा त्रास होऊ शकतो:

१. कॉम्प्युटर स्क्रीनवर त्रासदायक मेसेज दिसतात .

२. मेमरी किंवा डिस्क स्पेस कमी करतात.

३. असलेल्या डाटा फेरफार करतात.

४. फाइल्स ओव्हरराईट किंवा नष्ट करतात.

५. हार्ड ड्राइव्ह इरेज करतात.

उदाहरण:

१९९९ मध्ये मेलिसा नावाचा व्हायरस इतका शक्तीशाली होता कि मायक्रोसोफ्ट आणि अशा बऱ्याच मोठया कंपन्यांना हा व्हायरस जाई पर्यंत त्यांच्या ईमेल सिस्टीम बंद ठेवाव्या लागल्या.

उदाहरण:

Chernobyl **किंवा** Spacefiller **हे तैवान मध्ये लिहिले गेलेले कॉम्प्युटर व्हायरस आहेत. हा सर्वात घातक असा व्हायरस आहे जो इन्फेकटेड सिस्टीम मधील संवेदनशील माहिती नष्ट करतो, आणि काही वेळेस** BIOS **सिस्टीम करप्ट करतो.**Chernobyl **व्हायरस** CIH **नावाच्या व्हायरस नंतर अस्तित्वात आला, याचा सबंध युक्रेन मध्ये घडलेल्या नुक्लियर अपघाताशी आहे, हा व्हायरस २६ एप्रिल १९८६ रोजी अपघाताच्या दिवशीच कार्यरत झाला होता.**

66. *वेब डिफेसमेंट*

वेबसाईट डिफेसमेंट म्हणजे मुळचे वेबपेज हटवून त्या ठिकाणी दुसरे (अश्लील किंवा बदनामीकारक स्वरूपाचे) पर्यायी वेबेपेज हॅकरने बदलणे. धार्मिक आणि सरकारी साईट हॅकरकडून नेहमी त्याचा मुद्दा सांगण्यासाठी किंवा निदर्शने करण्यासाठी डिफेस केल्या जातात. यात आक्षेपार्ह मजकूर किंवा फोटोचा वापर केला जातो, आणि हॅकरच्या विशिष्ठ शैलीचे देखील प्रदर्शन होत असते ज्यावरून त्याची ओळख पटते. हि डिफेसमेंट फक्त राजकीय कारणांसाठीच होत नाही तर काही वेळेस मजा म्हणून हि केले जाते. मोठयाला कंपन्याच्या वेबसाईट देखील डिफेस केल्या जातात, म्हणूनच अशा कंपन्या या बाबतीत खूप काळजी घेत असतात. वेबसाईट ह्या संस्थेची प्रतिमा दर्शवित असतात आणि त्यावर केलेला हल्ला हि गंभीर बाब समजण्यात येते. अशा प्रकारामुळे लोकांची वेबसाईट वरील विश्वासार्हता कमी होते व त्याच्या कार्यक्षमते विषयी संशय निर्माण होतो. अशा प्रकारचा हल्ला झाल्यावर साईट काही कळासाठी बंद ठेवण्यात येतात ज्यामुळे हि खूप नुकसान होते.

उदाहरण:

महेश म्हात्रे आणि आनंद खरे(उर्फ डॉ. नेउरकर) यांना २००२ मध्ये मुंबई सायबर क्राईम सेलची वेबसाईट डिफेस केल्याबद्दल अटक झाली होती. त्यांनी पासवर्ड क्र्याकिंग सॉफ्टवेअर वापरून पोलिस

वेबसाईटचा FTP पासवर्ड क्र्याक केला.त्यांनी साईटचे होमपेज अश्लील मजकुराने भरून टाकले तसेच २५५ अमेरिकी नागरिकांचे क्रेडीट कार्ड नंबर चोरल्याचा त्यांच्या वर आरोप होता.

उदाहरण :

२००१ मध्ये २०० भारतीय साईट हॅककरून डिफेस करण्यात आल्या होत्या. हॅकरनी त्यावर मृत्युचे चिन्ह, पाकीइंग, अल्ला हु अकबर असे शब्द लिहिले होते. आणि 123medicinindia.com च्या केस मध्ये "Catch me if uuu can my deraz lazy adminzzz" हा मेसेज पोस्ट केला होता ज्यात त्यांनी सिस्टीम ॲडमिनीस्ट्रेटरला आव्हान केले होते.'Pakistani Cyber Warriors' या नावाने काम करणाऱ्या गटाने हे काम केले होते.

उदाहरण:

२००६ मध्ये iSKORPiTX असे हॅडल वापरणाऱ्या तुर्किश हॅकरने एका सर्व्हर ग्रुपला हॅककेले होते,ज्यामुले त्यांनी एका दिवसात 38,500 साईट

बंद पाडल्या होत्या.

उदाहरण:

रविवार ६ जुलै २००३ मध्ये फस्ट डिफेसर आव्हान झाले होते, ज्यात सर्व प्रथम ६,००० साईट डिफेस करणाऱ्याला विशेष परितोषित होते. हे आव्हान ६ तासांसाठी होते,आणि यात गुण हे सर्व्हरच्या ऑपरेटिंग सिस्टीमच्या आधारे देण्यात आले होते.

Windows: 1 point,

Linux: 2 points,

BSD: 2 points,

AIX: 3 points,

HP-UX: 5 points

Macintosh: 5 points

67. *व्हिशिंग*

मोबाईल बँकिंगचा वाढता वापर आणि आर्थिक व्यवहार ऑनलाईन करायच्या क्षमतेमुळे व्हिशिंग हल्ले हे सायबर हल्लेखोरांच्या आवडीचे बनले आहेत. हे फिशिंगच्या टेलिफोन समतुल्य आहे. हा शब्द व्हॉइस आणि फिशिंगच्या मिश्रणातून तयार झाला आहे. व्हिशिंग हे गुन्हेगारी करण्यासाठी व्हॉइस ईमेलचा वापर करणे होय VoIP (voice over Internet Protocol). **लॅंडलाईन किंवा मोबाईलचा वापर करून वैयक्तिक किवा आर्थिक माहिती मिळवणे आणि त्याचा गैरवापर करणे म्हणजे व्हिशिंग होय. व्हिशिंगचा शोध घेणे म्हणूनच खूप अवघड असते. म्हणून जेव्हा अशा प्रकारची संशयास्पद घटना घडेल तेव्हा लगेच संबंधित अधिकाऱ्याला संपर्क साधा.**

68. *वायर टॅपिंग*

वायर टॅपिंग म्हणजे फोन किंवा इंटरनेट वरील संवाद तृतीय पक्षाने लपून ऐकणे.हे एक इलेक्ट्रोनिक हेरगिरी आहे, ज्यात डाटा किंवा वोईस ट्रान्समिशन अनधिकृत पणे एखादे अवजार वापरून किंवा हेरगिरी करून ऐकणे, किंवा रेकॉर्डिंग उपकरण वापरून, किंवा वायरलेस कनेक्शन असेल तर ब्रोडकास्ट डाटा इंटरप्रीट करणे, अशा प्रकारच्या गोष्टी करतात.वायर टॅपिंग हे इलेक्ट्रोनिक स्वरुपात टेलीफोनिक आणि टेलीग्राफिक संवादावर देखरेख ठेवणे आहे .

उदाहरण:

ग्रीक टेलिफोन टॅपिंग केस २००४-०५ मध्ये १०० पेक्षा जास्त ग्रीकच्या संसदेच्या सदस्यानचे प्रधानमंत्र्यांसह, वरिष्ठ सनदी अधिकारयानचे मोबाईल अवैध पणे एक वर्षा करता टॅप केले होते. ग्रीक सरकारच्या असे लक्षात आले की २००४ ऑलंपिक खेळाच्या सुरक्षेच्या करणावरून परकीय गुप्तहेर खात्याने हि कारवाई केली होती. आणि हे त्यांनी वोडाफोन ग्रीस मोबाईल नेटवर्क सबसिस्टीम अवैधरीत्या वापरून केले होते.

उदाहरण:

राडिया टेप वाद हा नीता राडिया आणि राजकारणी, उद्योगपती,सनदी अधिकारी, पत्रकार इ. संवाद २००८-०९ मध्ये भारतीय आयकर विभागाकडून टॅप करण्यात आले होते. हे संवाद २G स्पेक्ट्रम घोटाळा आणि इतर असंविधानिक गोष्टी करण्यासाठी चालु असलेल्या योजनेचा पुरावा ठरले.

69. *वॉर्म*

कॉम्प्युटर वॉर्म हे स्ट्याड अलोन मालवेअर प्रोग्राम आहे जो कॉम्प्युटर नेटवर्क वापरून सगळीकडे पसरतो आणि इतर कॉम्प्युटर पर्यंत पोहचतो. कॉम्प्युटर व्हायरसप्रमाणे याला कोणत्याही फाईल किंवा प्रोग्रामला जोडण्याची गरज नसते. वोर्म्स हे व्हायरस पेक्षा जास्त घातक आहेत कारण त्यांना पसरण्यासाठी कोणत्याही प्रोग्रामची गरज नसून स्वतंत्र पणे ते रेप्लीकेट होऊ शकतात. एकदा का तुमच्या कॉम्प्युटरमध्ये आला कि तो नेटवर्क मधील अशा कॉम्प्युटरचा शोध घेईल ज्यात सारख्या प्रकारच्या सुरक्षा पळवाटा असतील, आणि जर असे काही सापडले तर वोर्म त्या कॉम्प्युटर मध्ये सरळ प्रवेश करेल, आणि हि प्रक्रिया परत करेल. ऑपरेटिंग सिस्टीम मधिल स्वयंचलित आणि युझरला न दिसणाऱ्या भागाचा वोर्म उपयोग करतो. वोर्मचा प्रसारमुळे जेव्हा सिस्टीम आणि नेटवर्क स्लो होण्यास सुरवात होते तेव्हाच त्यांचे अस्तित्व जाणवून येते.

वॉर्म अनेक प्रकारची कार्ये करू शकतात जसे कि DOS हल्ला, मेलिंग सुविधेला अॅट्याच होऊन अड्रेस लिस्ट मधील सर्वाना मेल पाठवतात,तुमच्या फाईल ओव्हर राईट करतात, तुमचा कॉम्प्युटर स्लो आणि निकामी करतात.

उदाहरण:

Nuwar OL **हा एक वॉर्म आहे, ज्याचा ईमेलद्वारे प्रसार केला जातो. आणि त्या ईमेलचा सब्जेक्ट** "You Are In My Dreams," "I Love You So Much," "Inside My Heart Is You," **इ . अशा प्रकारचा असतो. या मेल मध्ये एक वेब लिंक असते, जर का आपण ती ॲक्सेस केली तर एक मालिशीअस वॉर्म डाऊनलोड होईल. आणि आपला खरा उद्देश लपवण्यासाठी, वॉर्म आपल्याला एक रोमेंटिक भेट कार्ड असलेल्या वेबसाईटला डायरेक्ट करेल. एकदाका वॉर्मने कॉम्प्युटर इन्फेक्ट झाला कि तो अड्रेस बुक मधील सर्वांना असाच मेल पाठवतो. याचा सर्वात दूरगामी परिणाम म्हणजे हा जे काही कॉम्प्युटर किंवा नेटवर्क इन्फेक्ट झाला असेल त्याची कामगीरी खालावण्यास कारणीभूत ठरतो.**

उदाहरण:

I Love You **हा एक व्हायरस आहे ज्याचा ईमेलद्वारे प्रसार केला जातो, आणि त्या ईमेलचा सब्जेक्ट** "I Love You" **असा असतो व त्यासोबत एक अटॅचमेंट असते. जर का हा मेल ओपन करण्यात आला तर** MS Outlook **च्या अड्रेस बुक मधील प्रत्येकाला हा ईमेल पाठवला जातो. आणि हा मेल रिसिव्ह करणाऱ्याच्या हार्डडिस्क मधील** JPEG, MP3 **आणि**

इतर प्रकारच्या फाईल्सला नुकसान पोहचवले जाते. संस्थेच्या नेटवर्कमध्ये ईमेल हाताळण्यासाठी MS Outlook चा खूप वापर केले जातो. अशा संस्थामध्ये युझर ते युझर हा व्हायरस खुप जलद गतीने पसरवता येतो. ४ मे २००० मध्ये हा मेल इतक्या जलद गतीने प्रसारित पावला होता कि फोर्ड मोटारसारख्या मोठया कंपन्यांना देखील त्यांची ईमेल सुविधा बंद ठेवावी लागली होती. एका दिवसात ४९ मिलिअन लोकांना हा मेल मिळाल्याची नोंद झाली आहे.

उदाहरण:

१३ जुलै २००१ मध्ये कोड रेड नावाचा कॉम्प्युटर वोर्म इंटरनेटवर आढळला होता, ज्या कॉम्प्युटरवर मायक्रोसोफ्टचे IIS वेब सर्व्हर चालू होते त्या कॉम्प्युटरवर याचा हल्ला झाला होता. याचे नाव कोड रेड ठेवण्यात आले कारण ह्या व्हायरसचा शोध लावणारे त्या वेळेस कोड रेड माउनटन डयू हे पेय पीत होते.

70. XSS ***हल्ला***

XSS हे क्रोस साईट स्क्रिप्टींगचे संक्षिप्त रूप आहे, या प्रकारच्या हल्ल्यामध्ये एका विश्वासार्ह वेबसाईटमध्ये मालिशीअस कोड दाखल केला जातो. यात हल्लेखोर XSS चा वापर करून संशय येणारनाही अशा युझरला मालिशीअस स्क्रिप्ट पाठवतो. युझरच्या ब्राउझरला स्क्रिप्टची विश्वासार्हता तपासण्यासाठी कोणताही मार्ग उपलब्ध नसल्याने, हि स्क्रिप्ट खरी आहे असे समजूनच रन केली जाते. मालिशीअस स्क्रिप्ट वेबपेज मध्ये दाखल करून, हल्लेखोर संवेदनशील मजकूर, कुकीज, आणि ब्राउझरकडून युझर तर्फे ठेवण्यात आलेली माहिती हि मिळवू शकतो. XSS हल्ल्याचा वाटा सर्व सुरक्षाहल्ल्या पैकी ८०.५% इतका आहे असे सिम्यानटेकनी २००७ च्या अवहालात म्हंटले आहे. ह्यातून होणाऱ्या परिणामांची व्याप्ती मोठी असू शकते.

उदाहरण:

साशाच्या वेबसाईट मध्ये एक कमेंटचा टॅब उपलब्ध होता, ज्याचा वापर अल्बम मधील फोटोवरती कमेंट करण्यासाठी केला जात होता. पण या कमेंट इनपुट होताना कोणतीही तपासणी होत नव्हती. मग गोगो (हल्लेखोर व्यक्ती) साशाच्या वेबसाईटला भेट देतो, जो कि तिच्या

प्रगतीवर जळत असतो. आणि त्यांनी त्या कमेंटच्या जागी खालील कोड दाखल केला

Hi Sasha, very gud job, keep it up!

<img src=”http://google.com/images/logo.gif”

onload=”window.location=’http://sam.com/’” />

ज्यामुळे प्रत्येक वेळी जेव्हा कोणी साशाचा वेबसाईट वरील फोटो पाहण्याचा प्रयत्न करत असे तेव्हा तो गोगोच्या वेबसाईटला डायरेक्ट केला जाई.

71. *झिरो डे अटॅक*

यास झिरो अवर अटॅक असे हि म्हणतात. या प्रकरच्या हल्ल्यात अगोदरच माहित असलेल्या कॉम्प्युटर दुर्बलतेचा गैरफायदा उठवला जातो, आणि ह्यावरील उपाय कुणालाच माहित नसतो. झिरो डे अटॅकचा वापर लक्ष्य केलेल्या सॉफ्टवेअरच्या डेव्हलपरने त्या दुर्बलते बद्दल काहीतरी करण्याअगोदरच हल्लेखोर अटॅक करतो. जसे आपण पहिले कि या दुर्बलते बद्दल काही माहिती नसल्यामुळे अशा प्रकारचे हल्ले रोखणे अशक्य होते. बऱ्याचदा सॉफ्टवेअर बाजारात आल्यावर त्यातील दुर्बलता कंपनीच्या लक्षात येते, अशा वेळी मग त्यावरील पॅच बाजारात परत दाखल केले जातात आणि दुर्बलतेवर मात करण्याचा प्रयत्न केला जातो. सॉफ्टवेअर निर्मात्यांच्या अगोदरच प्रोग्रामरला अशा दुर्बलतेचा पत्ता लागल्यामुळे तो निश्चिंतपणे याचा फायदा उठवतो. आणि या दुर्बलतेवर कंपनीकडून पॅच दिले गेले असले तरी बरेच जण आपले सॉफ्टवेअर वरचेवर अपडेट करत नाहीत.

उदाहरण:

९ नोव्हेंबर २००६ मध्ये झिरो डे अटॅक झाला होता जो Windows च्या काही भागा पुरताच मर्यादित होता, ज्यास XMLHTTP ४. ० ActiveX Control म्हणतात. जेव्हा इंफेक्टेड पेज वेब ब्राउझर मध्ये उघडण्यात येते तेव्हा ते हल्लेखोरास बफर ओव्हरफ्लो घडवून आणण्यास मदत करते.

आणि परत हल्लेखोर इथे स्पायवेअर डाऊनलोड करून युझरचा डाटा देखील चोरू शकतो.

उदाहरण:

२०१० मध्ये अयाडोबनी त्यांच्या रीडर आणि फलाश या उत्पादनान वरती झिरो डे अटॅकची सूचना दिली होती. यासाठी कारणीभूत असलेल्या दुर्बलतेची नोंदणी गंभीर अशी करण्यात आली होती, याचा परिणाम Adobe Flash Player 10.0.45.2 आणि अगोदरच्या Windows, Macintosh, Linux and Solaris या ऑपरेटिंग सिस्टीमला होणार होता. ह्या दुर्बलतेमुळे कॉम्प्युटर क्रयाश हि होऊ शकत होता आणि हल्लेखोराला सिस्टीमचे नियंत्रणही मिळत होते.

72. झयुस

यास Zbot म्हणूनही ओळखले जाते, हा एक ट्रोजन हॉर्स आहे. हा सगळ्यात मोठा आणि खतरनाक बँकिंग ट्रोजन आहे. ह्याचे मुख्य काम पैसे चोरणे आणि बँकेशी संबंधित माहिती चोरणे हे आहे. याचा प्रसार मुख्यत्वे करून ड्राइव्हवरून डाऊनलोड करून, फिशिंगचा वापर करून केला जातो. याचा संबंध सोशल मिडियाशी सुद्धा आहे, बऱ्याच वेळा हा ट्रोजन खोटॅ फ्रेंड रिक्वेस्ट किंवा कनेक्शन मध्ये लपलेला असतो. याचा जुलै २००७ मध्ये प्रथम शोध लागला जेव्हा US Department Of Transport मधून माहिती चोरण्यात आली आणि मार्च २००९ मध्ये त्याला आणखीन प्रसिद्धी मिळाली.

या ट्रोजननी कॉम्प्युटरला इन्फेक्ट केले असले तरी तो सुप्त अवस्थेतच राहतो, पण जेव्हा युझर फोर्म भरण्यासाठी एका विशिष्ठ वेबपेजला भेट देतो तेव्हा हा सतर्क होतो. याचे सगळ्यात महत्वाचे वैशिष्ट असे कि ह्यामुळे आपल्याला ब्राउझर पातळीवरच एखादे इनपुट फिल्ड जोडता येणे शक्य आहे. म्हणजे कि युझरला बनावट वेबसाईटला भेट न द्यायला लावता एखाद्या विश्वासार्ह वेबसाईट वरतीच जास्तीचे फिल्ड जोडून युझरची फसवणूक करता येते. योग्य त्या माहितीचा ॲक्सेस करे पर्यंत हा ट्रोजन सुप्त अवस्थेतच राहतो.

उदाहरण:

मार्च २०१०, म्यानहयाटन फेडरल कोर्टात सायबर फ्रोड डिफेनडंट आरोप होऊन शिक्षा झाली होती. तपासात आढळून आले की ग्लोबल बँक फ्रोड स्कीम मध्ये झयुस ट्रोजनचा वापर झाला होता. आणि इतर मालवेअर वापरून US बँकेच्या खात्यातून मिलियन डॉलर्स चोरण्यात आले होते.

उदाहरण:

निकोलस गारीफुलीन यास ग्लोबल बँक फ्रोड स्कीममधील सहभागामुळे म्यानहयाटन फेडरल कोर्टाने दोन वर्षाची कारावासाची शिक्षा ठोठावली होती. ज्यात मालवेअर हल्ला करून US अकाउंट मधून ३ मिलियन डॉलर्सच्या वरती पैसे चोरण्यात आले होते.

उदाहरण:

बँक फ्रोड स्कीमचा भाग म्हणून पूर्व युरोपातील हॅकरनी सायबर अटॅक करून US मधील लहान मोठया उद्योगांच्या बँक अकाउंट मधून पैसे चोरले होते. आणि या हल्ल्यात झयुस ट्रोजनचा वापर करण्यात आला होता. जो त्यांच्या कॉम्प्युटर वरील किस्ट्रोक्स नोंद करून घेऊन माहिती चोरत होता आणि हॅकर हॅच माहितीचा वापर करून पैसे चोरत होते.

73. झोंबी

कॉम्प्युटर शास्त्र असे सांगते कि झोंबी हा एक असा कॉम्प्युटर असतो कि जो इंटरनेटशी जोडलेला असतो पण ज्याची सुरक्षेशी तडजोड झालेली असते. आणि हॅकर याचा वापर करून पीडीत व्यक्तीचा कॉम्प्युटर गुप्तपणे नियंत्रित करत असतात. साधारणतः युझर या सर्व घडामोडी पासून दूरच असतो कारण हे सर्व त्याच्या नकळत घडत असते. झोंबीचा ईमेल स्प्याम पाठवण्यासाठी खूप वापर केला जातो. २००५ मध्ये याचे प्रमाण ५०-८० % इतके होते. तसेच इतर अनेक सायबर गुन्हे करण्यासाठी याचा वापर करण्यात येतो. झोंबी कॉम्प्युटरचा सुगावा लागण्यासाठी खालील प्रकारच्या गोष्टी आपण तपासू शकतो.

- आपण स्प्याम पाठवत आहात अशा प्रकारचे आरोप करणारे आपणाला ईमेल येतील.

- तुम्ही न पाठवलेला ईमेल मेसेज तुम्हाला तुमच्या ओउट बॉक्स मध्ये दिसेल.

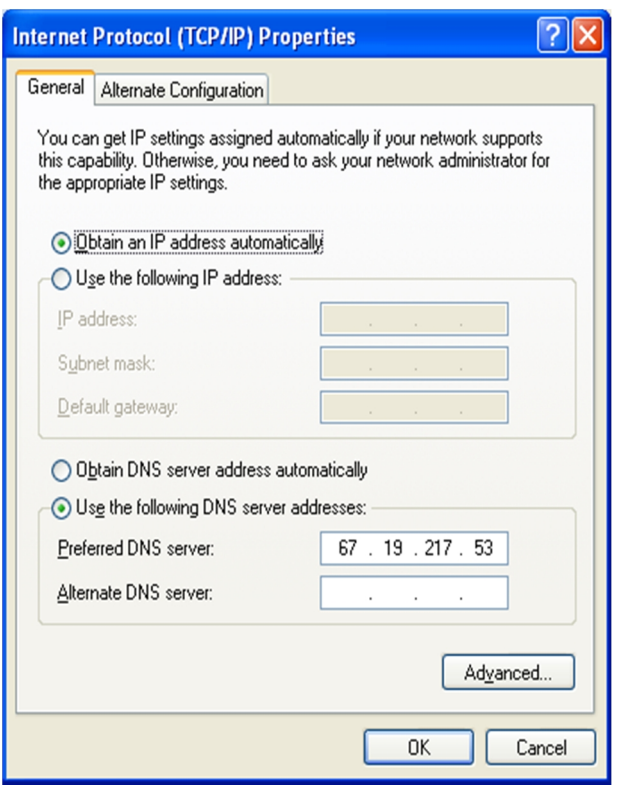
- पूर्वी पेक्षा जास्त प्रमाणात तुमचा कॉम्प्युटर उर्जा वापरेल ज्यामुळे आपली सिस्टीम स्लो होईल.

IP अॅड्रेस

इंटरनेटचे कामकाज समजण्यासाठी सगळ्यात मुलभूत बाब IP **अॅड्रेस (इंटरनेट प्रोटोकॉल अॅड्रेस) म्हणजे काय हे अगोदर पाहिले पाहिजे. इंटरनेटवर असणाऱ्या प्रत्येक कॉम्प्युटरसाठी एक युनिक असा क्रमांक असतो त्यास** IP **अॅड्रेस असे म्हणतात. याचा वापर करून आपल्याला कॉम्प्युटरची ओळख पडताळता येते. कॉम्प्युटर इंटरनेटवर एकमेकांशी या** IP **अॅड्रेसचा वापर करूनच संपर्क साधतात. उदा:** 173.194.36.5 **हा एक** IP **अॅड्रेस आहे. अशाच प्रकरची अजून एक संज्ञा म्हणजे डोमेन नेम. समजा एक वेबसाईट** www.google.com **जी एका कॉम्प्युटरवर होस्ट आहे ज्याचा** IP **अॅड्रेस**173.194.36.5 **आहे. जर तुम्ही वेब ब्राउझर मध्ये** http://173.194.36.5 **असे टाईप केले तर गुगलची वेबसाईट(** www.google.com**) लोड होईल. पण प्रत्येक वेळेस अशा प्रकारे मोठा नंबर लक्षात ठेवणे अशक्य आहे, त्या ऐवजी वेबसाईटचे नाव सोपे असते. आणि या कारणासाठी डोमेन नेम सिस्टीम** (DNS)**चा उगम झाला. साध्या भाषेत सांगायचे तर** DNS **हे एका मोठया टेलिफोन डिरेकट्री सारखे आहे, ज्यात डोमेन नेम आणि त्याच्याशी सल्लग्न** IP **अॅड्रेसचा त्यात समावेश असतो. याच** DNS **यंत्रणेमुळे आपण वेब ब्राउझर मध्ये** http://173.194.36.5 **ऐवजी** http:// www.google.com **असे टाईप करू शकतो, आणि मग साईट लोड होईल.**

उदाहरण:

एखादा व्यक्ती इंटरनेटशी कसा जोडला जातो हे समजण्यासाठी आपण एक उदाहरण पाहू, सान्यानी इंटरनेटचा वापर करण्यासाठी नुडल इंटरनेट सेवा वापरली. त्यामुळे नुडलने तिला एक राऊटर पुरवला जो ती तिच्या घरच्या कॉम्प्युटरला जोडेल. त्या बरोबरच नुडलने DNS **सर्वर ॲड्रेस** (67.19.217.53) **हि दिलेला असतो.**



नुडलकडे त्यांच्या ग्राहकांना देण्यासाठी खुपसाऱ्या IP ॲड्रेसचा संग्रह असतो. जेव्हा सान्या तिचा राऊटर सुरु करेल, नुडल याच संग्रहातून एक IP ॲड्रेस तिला पुरवेल, जो पर्यंत सान्या इंटरनेटचा वापर करेल तो पर्यंत तिचा कॉम्प्युटर याच IP ॲड्रेसचा वापर करेल. पण जेव्हा ती इंटरनेट वापरणे बंद करेल (तिचा राऊटर बंद करेल) तो IP ॲड्रेस नुडलच्या संग्रहात परत जाईल, व इतर इंटरनेट वापरकर्त्यांना पुरविला जाईल.

जर सान्या डायनामिक IP ॲड्रेसचा वापर करत असेल तर प्रत्येक वेळी नवीन पणे जेव्हा ती इंटरनेटशी जोडली जाईल तेव्हा प्रत्येक वेळेस ती नवीन IP ॲड्रेसचा वापर करेल. पण जर ती अधिक पैसे भरून नुडल कडून स्टयाटिक IP ॲड्रेस मिळवू शकते.

समजा सान्याने तिच्या ब्राउझर मध्ये www.google.com असे टाईप केले, तर आता तिच्या ब्राउझर गुगलचा IP ॲड्रेस लागेल, जो कि नुडलच्या DNS सर्वर वरून तिला मिळेल. आणि एकदा का सान्याच्या ब्राउझरला हि माहिती मिळाली कि google.com चा IP ॲड्रेस 173.194.36.5 हा आहे, कि लगेच तो गुगलचे पेज लोड करेल. सान्याचा कॉम्प्युटर काही काळासाठी हि माहिती सेव्ह करून ठेवतो,पुढील वेळेस जेव्हा सान्या www.google.com असे ब्राउझर मध्ये टाईप करेल तेव्हा कॉम्प्युटर मध्ये सेव्ह असलेला IP ॲड्रेसचा वापर होईल, यासाठी आता नुडलच्या DNS सर्वरशी संपर्क साधण्याची गरज भासणारनाही.

IP अॅड्रेस बद्दल अधिक माहिती:

या भागात इंटरनेट प्रोटोकॉल 4 बद्दल चर्चा केली आहे.

प्रत्येक IP अॅड्रेसची ४ ऑक्टेट मध्ये विभागणी असते. आणि पूर्णविराम वापरून त्यांना अलग करण्यात आलेले असते, आणि प्रत्येक ऑक्टेट मध्ये 0 ते 255 पैकी कोणतीही संख्या असू शकते.

0 – 255. 0 – 255. 0 – 255. 0 – 255

उदाहरण: 180.110.200.203

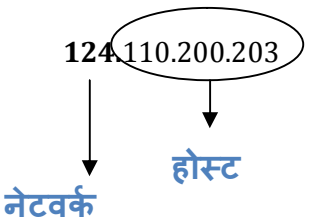
म्हणजेच अशा IP अॅड्रेसची संख्या 256 x 256 x 256 x 256, 4 अरब पेक्षा जास्त आहे. एका ऑक्टेट मध्ये आठ बायनरी बिटस असतात. आणि सर्व चार ऑक्टेट मिळून त्याचे 32 बिटस होतात.

काही IP अॅड्रेस संरक्षित असतात जे कि 0.0.0.0 आणि 255.255.255.255.

IP अॅड्रेसची दोन भागात विभागणी असते, एक भाग नेटवर्क विषयीची माहिती देतो तर दुसरा होस्ट (कॉम्प्युटर) विषयी माहिती देतो. IP अॅड्रेसची ऑक्टेटनुसार त्याची वर्गवारी केलेली असते.

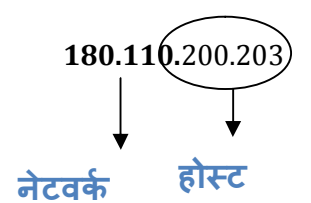
वर्ग A IP अॅड्रेस मध्ये पहिल्या ऑक्टेट मध्ये 1 ते 126 पैकी कोणताही अंक असू शकतो, आणि उरलेल्या ऑक्टेटमध्ये 0 ते 255 पैकी कोणताही अंक असू शकतो. या IP अॅड्रेस मध्ये पहिल ऑक्टेट नेटवर्क विषयी माहिती देत आणि बाकी ऑक्टेट होस्टs (कॉम्प्युटर) विषयी माहिती देतात.

समजा नुडल बँकेचा वर्ग A चा IP अॅड्रेस आहे,ज्यात त्याचा पहिला ऑक्टेट "124" आहे, आणि संपूर्ण IP अॅड्रेस 124.110.200.203



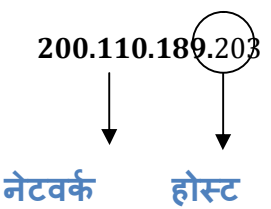
वर्ग B IP अॅड्रेस मध्ये पहिल्या ऑक्टेट मध्ये 128 ते 191 पैकी कोणताही अंक असू शकतो, आणि उरलेल्या ऑक्टेटमध्ये 0 ते 255 पैकी कोणताही अंक असू शकतो. या IP अॅड्रेस मध्ये पहिले दोन ऑक्टेट नेटवर्क विषयी माहिती देत आणि बाकी ऑक्टेट होस्ट(कॉम्प्युटर) विषयी माहिती देतात.

समजा नुडल बँकेचा वर्ग B चा IP अॅड्रेस आहे,ज्यात त्याचे पहिले दोन ऑक्टेट "180.110" आहे, आणि संपूर्ण IP अॅड्रेस 180.110.200.203



वर्ग C IP अॅड्रेस मध्ये पहिल्या ऑक्टेट मध्ये 192 ते 223 पैकी कोणताही अंक असू शकतो, आणि उरलेल्या ऑक्टेटमध्ये 0 ते 255 पैकी कोणताही अंक असू शकतो. या IP अॅड्रेस मध्ये पहिले तीन ऑक्टेट नेटवर्क विषयी माहिती देत आणि बाकी ऑक्टेट होस्ट(कॉम्प्युटर) विषयी माहिती देतात.

समजा नुडल बँकेचा वर्ग C चा IP अॅड्रेस आहे,ज्यात त्याचे पहिले तीन ऑक्टेट "200.110.189" आहे, आणि संपूर्ण IP अॅड्रेस 200.110.189.203



127.0.0.1 हा IP अॅड्रेस लोकल कॉम्प्युटरसाठी आरक्षित असतो. त्याच प्रमाणे जे IP अॅड्रेस 224 आणि त्या पुढचे आहेत ते आरक्षित असतात.

वैयक्तिक नेटवर्कच्या वापरासाठी आरक्षित असलेले IP अॅड्रेस:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.25.255

एशियन स्कूल
ऑफ सायबर लॉज

एशियन स्कूल ऑफ सायबर लॉज
६ वा मजला, कुमार प्राइड सेनेट, सिग्मा हाऊसच्या मागे,
सेनापती बापट मार्ग, पुणे–४११०१६ (भारत).
फोनः (९१) ९२२५५४८६०१
(९१) ९२२५५४८६०२
ईमेलः info@asianlaws.org **वेबसाईटः** www.asianlaws.org