संगणकीय विषाणू

तो दिवस होता २ नोव्हेंबर १९८८ चा. त्या काळात इंटरनेट बाल्यावस्थेत होते. या दिवशी एका भयानक विषाणूची निर्मिती झाली आणि मानवसमाजाला अचानक जाणिव झाली की खूप मोठ्या प्रमाणात हे संगणकदेखील बंद पडू शकतात.तोपर्यंत संगणक म्हणजे एक वरदान होते मानवसमाजासाठी. या विषाणूचं नाव- ग्रेटवर्म- म्हणजे मोठ्ठा किडा ! विषाणूची निर्मिती जरी झटपट श्रीमंत होण्यासाठी जरी झाली नव्हती खरं. पण आणि महत्वाचं म्हणजे एमआयटी आणि स्टॅनफोर्डच्या तथाकथित भयानक बुध्दिमान तज्ञांना चकमा देत अमेरिकन शास्त्रीय विभागापर्यंत पोहचून ३००० संगणक बंद पाडण्याचे काम या संगणकीय विषाणूने केले होते.

या विषाणूचा निर्माता होता रॉबर्ट मॉरिस. पण याने आपल्या कर्तृत्वाच्या टिमक्या मारल्या होत्या.पण पुढच्या विषाणूंच्या निर्मात्यांनी मात्र ही खबरदारी घेतली. आणि मग संगणकातल्या विषाणूंचा, जीवाणूंचा,जंतूंचा,किड्यांचा सुकाळ चालू झाला.सध्या फिनाल्डो व गॉनर या नवीन विषाणूंचे वारे जोरात आहेत. क्वचितच एखादा आठवडा असा असतो जेव्हा नवीन विषाणू आल्याबद्दल वर्तमानपत्रात बातमी नसते संगणक आणि माहिती तंत्रज्ञान क्षेत्रातल्या मंदीमुळे अनेक संगणक तज्ञ सध्या विषाणू तयार करायचे कार्यक्रम लिहीत असलेले दिसतात. सध्याच्या युवा पिढीचा कल संगणकातील इतर कोणत्याही प्रकारची माहिती घेण्यापूर्वी विषाणूंची माहिती घेण्याकडेच आहे.

संगणकीय विषाणू ही संगणकास लागलेली किड असते ज्याच्या आगमनामुळे संगणकाची काम करायची गति मंदावते , संगणक अचानक बंद पडायला लागतो. संगणकाच्या संदर्भात ही संज्ञा वापरायच्याआधी माणसाच्या आजारासंदर्भात ही संज्ञा वापरली जात असे. डॉक्टरकडे गेल्यावर ताप कशाने आला आहे? हा प्रश्न विचारल्यावर ब-याचदा एकच उत्तर असते काही नाही व्हायरल इनफेक्शन झालं आहे यावरुन आपण अंदाज बांधतो की हे दुखणे गंभीर नसून तात्पुरत्या स्वरूपाचे आहे .. त्याचप्रमाणे सुरवातीस व्हायरसचा संगणकात होणारा शिरकाव हा संगणकास तात्पुरत्या स्वरुपाची इजा करीत असे पण आता मात्र या विषाणूंची संहारकता वाढत चालली आहे...

नवीन नवीन संगणकाचा अभ्यासक्रम पूर्ण करणारे विद्यार्थी केवळ मजा म्हणून तर कधी सूड बुध्दीने तर कधी नवीन अनुभव म्हणून या निर्मितीच्या परिणामांचा विचार न करता अशा प्रकारच्या विघातक विषाणूंची निर्मिती करताना दिसतात.

व्हायरस हा अशा संगणकीय संदेशांचा (Instructions) कार्यक्रम (program) आहे ज्यायोगे संगणकावरची पूर्ण माहिती पुसली जाउ शकते , संगणक आपोआप बंद होउ शकतो. संगणकाच्या जाळ्यातील (network) एकाही संगणकावर विषाणूचा प्रवेश हा संपूर्ण संगणकीय जाळ्यास धोकादायक असू शकतो कारण या विषाणूंकडे स्वतःला अनेक विषाणूंमध्ये परावर्तित करायची क्षमता असते. या विषाणूंना संगणकातून बाहेर काढून संगणकाची कार्यपध्दति पूर्ववत करणे यातच लाखो रुपयांचा दरवर्षी चुराडा होत असतो.

विविध प्रकारच्या बाह्य साधनातून विषाणूंचा संगणकात प्रवेश होउ शकतो.पूर्वपरिक्षण न केलेली संगणक प्रणाली (application software) संगणकावर आणणे,

कर्मचा-यांनी त्यांच्या कामासाठी अथवा सुविधेसाठी आणलेल्या विविध प्रकारच्या संगणकीय प्रणाली, इंटरनेटवरुन उतरवून घेतलेले संगणकीय कार्यक्रम (program), विक्रेत्याने संगणकावर उतरवून दिलेले संगणकीय कार्यक्रम अथवा संगणकीय प्रणाली ज्यात विषाणूंचा शिरकाव पहिल्यापासूनच झाला आहे,

प्रात्यक्षिक दाखविण्यासाठी आणलेले संगणकीय कार्यक्रम, विनामूल्य (freeware), वाटतायेण्याजोगे (shareware), अनिर्बंध (uncontrolled) संगणकीय कार्यक्रम, इ-मेलची जोड (attachment) म्हणून

संगणकीय विषाणूचा प्रवेश झाल्यानंतर संगणकाची साठवणक्षमता नाट्यमयरित्या कमी होते, उपलब्ध धारिणींच्या आकारात अचानक वाढ होते, धारिणींमध्ये होणा-या सुधारणांची वेळ बदलते, धारिणींमधला प्रवेश नाकारला जातो, धारिणीमध्ये प्रवेश केलेल्यांची संख्या अशक्यप्राय फुगलेली दिसायला लागते, संगणकाच्या बंद होउन चालू करण्याच्या (system boot up) प्रक्रियेत अडथळे निर्माण होतात, विविध प्रकारचे संदेश आणि चित्रांचे संगणकावर झळकायला लागतात, काही धारिण्या संगणकावरुन नाहीशा होतात आणि न जाणे कोणाकोणाला कायकाय अनुभव येत असतील ?

हे संगणकीय किड्यांचे पण वेगवेगळे प्रकार असतात, त्यांच्यापण जमाति-उपजमाति असतात.

बूटसेक्टर विषाणू (**Boot sector Virus**) :

बूट सेक्टर हा कोणत्याही floppy disk अथवा hard disk चा पहिला तंत्रशुध्द (logical) सेक्टर असतो. ७५ टक्के विषाणू हे या सदराखाली मोडतात. हे विषाणू सर्वप्रथम या बूट सेक्टरची जागा घेतात आणि नंतर या बूटसेक्टरना दुस-या ठिकाणी हलवितात. त्या नंतर ते स्वतःच्या संगणकीय आदेशांची त्या भागात पेरणी करतात जेणे करुन प्रत्येक वेळेस जेव्हा संगणक चालू केला जाइल तेव्हा या आदेशांचे पालन होइल.

"स्टोन्ड" हे या प्रकारच्या विषाणूंचे उत्तम उदाहरण आहे. हा विषाणू Random Access Memory (RAM) 2KB ने कमी करतो आणि संदेश झळकावतो

“Your PC is now stoned”

संगणकीय प्रणालीतील विषाणू (**Application Software Viruses**):

या प्रकारचे विषाणू संगणकीय कार्यक्रमाच्या धारिणीत स्वतःचे स्थान निर्माण करतात आणि मग संगणकीय कार्यक्रम अशा प्रकारे बदलतात की विषाणू दूषित आदेशांचे पालन पहिले होते. “व्हिएन्ना” हे अशाप्रकारच्या विषाणूचे उत्तम उदाहरण आहे.

धारिणींचा आकार ६४८ बाइट्सने वाढतो आणि संगणकास सारख बंद होउन मग चालू होण्यास भाग पाडतो यामुळे संगणक खराब होतात.

होक्सेस (**Hoaxes**):

अनेकदा आपणास काही इ-मेल्स अशा मिळतात ज्यात ती मेल आापल्याला इतर १० जणांना पाठवायला सांगितलेली असते.अशाप्रकारच्या इ-मेलमधून फैलणा-या विषाणूंना होक्सेस असे म्हणतात.या प्रकारच्या विषाणूंमुळे संगणकाचा वेग मंदावतो.

स्टेल्थ विषाणू (**Stealth Virus**) :

या प्रकारचे विषाणू सतत सरड्यासारखा आपला रंग बदलत असतात.शोध लागू नये म्हणून ते Dos Interrupt Calls ना दाद देत नाहीत.४०९६ नावाचा विषाणू हा या प्रकारच्या विषाणूंचे उत्तम उदाहरण आहे. या विषाणूचा प्रवेश झाल्यावर धारिणीचा आकार ४०९६ bytes ने वाढतो.आणि संगणकावर FRODO LEAVES अशा प्रकारचा संदेश झळकायला लागतो .२१ सप्टेंबरला दूषित धारिणी उघडल्यास मात्र संपूर्ण संगणक खराब व्हायची शक्यता असते.

म्युटेशन इंजिन विषाणू (**Mutation engine Virus**):
अल्गोरिदम तयार करण्यासाठी खास भाषेचा वापर केला जातो ज्या योगे मूळ अल्गोरिदमच्या अनेक प्रति बनविल्या जाउ शकतात.पण स्टेल्थप्रमाणे यात धारिणींचा आकार वाढत नाही. प्रत्येक वेळेस नवीन आदेश लिहले जातात. "पोग" हे या प्रकारच्या विषाणूंचे उत्तम उदाहरण आहे. त्या फक्त .COM अशी जोड असणा-या धारिण्यांनाच दूषित करतात त्यातही ज्यांचा आकार ६१४३९ bytes पेक्षा कमी आहे अशाच धारिण्यांना. १मे ला अथवा इतर दिवशी सकाळी ९ वाजताच्या आत दूषित धारिणी उघडल्यास या विषाणूंमुळे विविध प्रकारचे आवाज येतात.

संगणकीय जाळ्यात स्वतःला पसरवणारे विषाणू **(network Viruses)**:
संगणकीय जाळ्यात एक संगणक मुख्य संगणक (Server) असतो आणि बाकीचे सामान्य संगणक (workstations) असतात.विषाणू हे प्रामुख्याने मुख्य-संगणकावरील धारिणींना इजा पोचविण्यासाठी बनवलेले असतात. सध्या युरोपात अशाप्रकारचे दोन विषाणू सापडतात जीपी-१ आणि सीझेड२९८६ . जीपी-१ हा नोवेल(Novell)च्या सुरक्षा कवचास भेदण्यासाठी बनवलेला होता. तर सीझेड२९८६ हा १५ पासवर्डस जमवून त्यांना एका दूषित धारिणीत साठवतो आणि मग याचा उपयोग संगणकीय जाळ्यात अनधिकृतपणे प्रवेश करण्यासाठी होतो.

विविध संकेतस्थळे :
खालील संकेतस्थळांवर संगणकीय विषाणूंबद्दल काही महत्वाची माहिती मिळू शकते.
www.symantec.com: संगणक क्षेत्रात सुप्रसिध्द अशा आणि मोठ्या प्रमाणावर प्रतिबंधात्मक संगणक प्रणाली बनविणा-या या कंपनीचे Norton Antivirus हे महत्वपूर्ण उत्पादन या संकेतस्थळावर उपलब्ध आहे.नवीन येणारे विषाणू आणि त्यांच्यावर कंपनीने तयार केलेल्या उपायांची पण माहिती या संकेतस्थळावर मिळते.
www.vmyths.com: इथे विविध प्रकारच्या संगणकीय उत्पादनांबरोबरच गोष्टीही ऐकायला मिळतात. ओसामा बिन लादेन आपले संगणक सहज नष्ट करु शकतो पण तो का करत नाही वैगरे
www.research.ibm.com: हे जगप्रसिध्द IBM कंपनीचे संकेतस्थळ आहे.अनेक संशोधकांनी केलेल्या संशोधनाची माहिती येथे उपलब्ध आहे.विषाणू कसे तयार होतात त्यांना रोखायला करण्यात येणारे नवीननवीन उपाय या संदर्भात येथे माहिती उपलब्ध आहे.
www.download.com : या संकेतस्थळावरुन आपल्याला अनेक प्रकारची माहिती संगणकावर विनामूल्य उतरवून घेता येते.थोडासा शोध घेतल्यास कोणते विषाणूप्रतिबंधक कार्यक्रम उपलब्ध आहेत आणि ते किती प्रसिध्द आहेत याची पूर्ण माहिती इथे दिलेली असते.

मयूर शरद जोशी
mayur_cfe@rediffmail.com