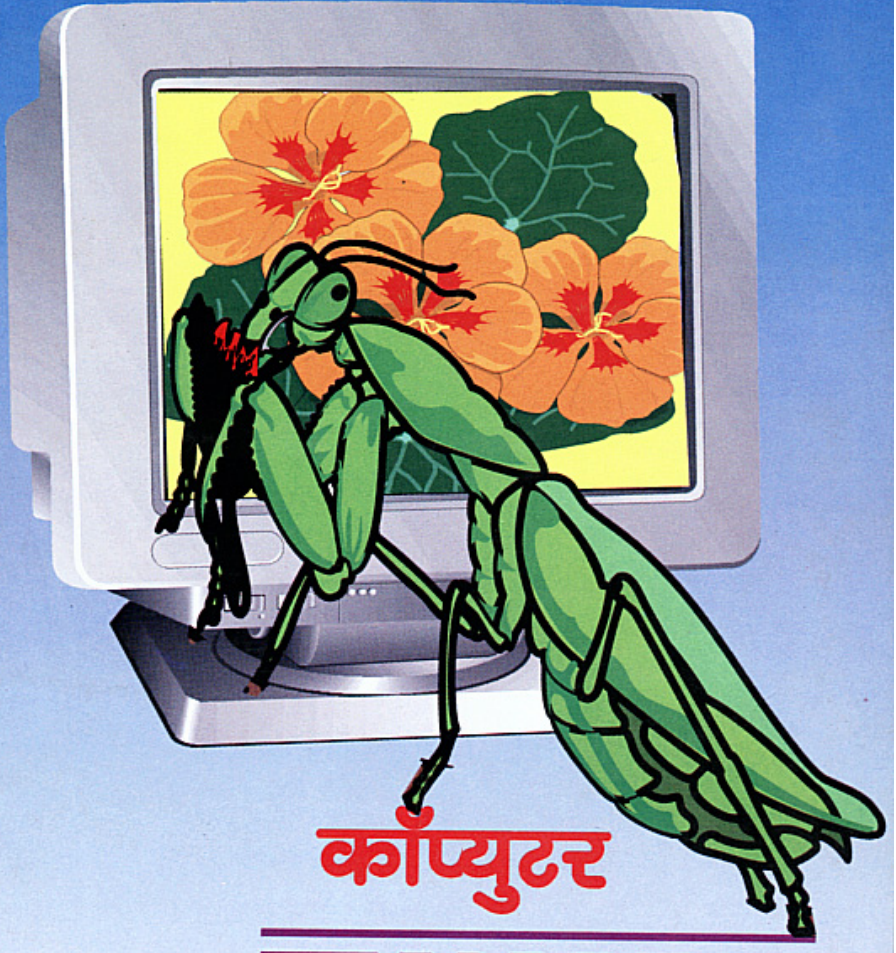
मराठीत प्रथमच



कॉम्प्युटर व्हायरस

स्वरूप आणि उपाय

माधव शिरवळकर

कॉंप्युटर व्हायरस: स्वरुप आणि उपाय

माधव शिरवळकर

अंगण प्रकाशन

काँप्युटर व्हायरस: स्वरुप आणि उपाय

ई - आवृत्ती

मुखपृष्ठ / सजावट /अक्षररचना
संगणक प्रकाशन, कलाविभाग

किंमत ११० रुपये

प्रकाशक
विश्वनाथ खांदारे
संगणक प्रकाशन
५-६ शांती निवास, संत रामदास रोड,
मुलुंड (पूर्व), मुंबई -४०००८१.

दूरध्वनी/फॅक्स: ५६८१६५०/५६८८६८२

E mail: prakashan@indiatimes.com

माझा मुलगा **चि. आदित** यांस,
त्याच्या पिढीसाठीच तर
अशा पुस्तकांची खरी निकड आहे.....

अनुक्रमणिका

अनुक्रमणिका

वाचकहो,

'कॉंप्युटर व्हायरस: स्वरुप आणि उपाय' हे ह्या विषयावरील केवळ मराठीतीलच नव्हे, तर सर्व भारतीय भाषांमधले पहिले पुस्तक आहे. इंग्रजीत सध्या 'ण्दस्ज्लू एाम्ल्ूद' हा विषय 'हॉट' मानला जातो. 'हॉट' विषयावर फटाफट पुस्तके देणे हे 'इंग्रजी' चे वैशिष्टय. त्यामुळे इंग्रजीत 'कॉंप्युटर व्हायरस' हा विषय ह्यापूर्वीच अनेक लेखकांनी पुस्तकात आणलेला आहे. मात्र ही पुस्तके खूप क्लीष्ट आणि तांत्रिकतेनी भरलेली आहेत. 'व्हायरस' हाही शेवटी एक प्रोग्रामच आहे. त्यामुळे प्रोग्रामिंग लॅंग्वेजेस आणि कोडस त्यात येणे अपरिहार्य आहे. पण प्रोग्रामिंग व कोडस आली की पुस्तक सामान्य माणसाच्या आवाक्याबाहेर जाते. ह्या पुस्तकात क्लीष्टपणा आणि कोडस् टाळलेले आहेत. कारण सामान्य मराठी वाचकाला हा विषय कळावा यासाठी हे पुस्तक आहे. व्हायरस कसा तयार करावा हे शिकवणारे पुस्तक काढावे असा विघातक उद्देश मूळातच असू शकत नाही. त्यातही पुढे जाऊन दृष्टीकोन असा आहे की 'कॉंप्युटर व्हायरस'चे स्वरुप कळल्यानंतर, आत्तापर्यंतचा त्या संदर्भातील इतिहास कळल्यानंतर व व्हायरसवरील उपायांची माहिती मिळाल्यानंतर कुणालाही असे वाटू नये की आपण व्हायरस तयार करुन पाहू या. दुसऱ्या बाजूला संगणकाचे जुजबी ज्ञान असणारांना, किंवा अगदी सर्वसामान्यांनाही ही 'व्हायरस' चीज काय आहे हे कळावे, ह्या संदर्भात काय काळजी घ्यावी याची जागरुकता त्यांच्यात यावी असाही मानस ह्या पुस्तकामागे आहे. थोडक्यात कॉंप्युटर सायन्सचे विद्यार्थी व सर्वच तमाम वाचकांसाठी हे पुस्तक आहे.

संगणकाच्या जगात 'व्हायरस'च्या मागे एक भिती युक्त आणि गूढ त्याचे वलय आहे. जगभर आजही संगणक वापरणाराच्या मेंदूत ह्या व्हायरसची एक सूक्ष्म भिती असतेच. ही भिती निर्माण करणारे जे मेंदू आहेत त्या व्हायरस रायटर्सची मानसिकता नेमकी कशी आहे त्याचे प्रकरणही ह्या पुस्तकात आहे. 'व्हायरसेस'ची माहिती पुस्तकाबाहेर जाऊन मिळणारांसाठी सोयीचे व्हावे म्हणून प्रमुख वेब साईटसची यादी व त्यांचा परिचयही दिला आहे. एकूणच पुस्तक उपयुक्त होता होता मनोरंजकही व्हावे यासाठी आटोकाट प्रयत्न केला

आहे. ह्या क्लीष्ट विषयाला मनोरजंक करणे हे आव्हानच होते. ते आव्हान येथे कितपत पेलले आहे हे वाचकांनीच सांगायचे आहे.

ह्यापूर्वी आलेल्या 'वेब डिझायनिंग:तंत्र आणि मंत्र' तसेच 'ई मेल व चॅट' ह्या माझ्या दोन पुस्तकांच्या प्रस्तावनेत मी मराठी शब्द, मराठी भाषा आणि संगणकाच्या जगात रोज नव्याने येऊन पडणारे इंग्रजी शब्द याबद्दल लिहिले होते. पुस्तके मराठीतून हवीत कारण इंग्रजी पुस्तके अनेक मराठी वाचकांच्या पचनी पडत नाहीत. आपल्या मातृभाषेतून हा विषय समजावून घेणे सोपे जाते. हवेसे वाटते. पण प्रत्येक इंग्रजी शब्दाला मराठी पर्याय शोधायचा अट्टाहास आता अशक्य आणि अव्यवहार्य झालेला आहे. तात्पर्य, वर्णनासाठी सोपी मराठी, स्पष्टीकरण सोप्या मराठीत समजेल (हे महत्वाचे !) असे द्यावे व मूळ इंग्रजी शब्द तसेच ठेवावे अशी भूमिका ह्याही पुस्तकाचे वेळी कायम आहे. पूर्वीच्या दोन्ही पुस्तकांचे स्वागत महाराष्ट्रभर झाले. कित्येकांनी ही पुस्तके वाचून आपल्या वेब साईटस् तयार केल्या. कित्येकांना ह्या क्षेत्रात अधिक रस वाटू लागला. तुमच्या पत्रांवरून आणि शेकडो ई मेलवरुन जेव्हा हे कळले तेव्हा समाधान वाटले. श्रमांचे चीज झाले असे वाटले.

मित्रहो, मराठीत ह्या विषयावर मूळातच कमी पुस्तके. मात्र ग्रामीण भाग, जिल्हयाच्या ठिकाणी शिकणारे हजारो विद्यार्थी यांचेसाठी अशी मराठी पुस्तके असायला हवीत अशी दृष्टी ठेवून 'संगणक प्रकाशन' ने आपले कार्य चालविले आहे. आपला ह्या पुस्तकावरील अभिप्राय माझा आणि 'संगणक प्रकाशना'चा उत्साह वाढविण्यासाठी सहाय्यभूत होईल आपण आपल्या सूचना, अभिप्राय अवश्य पाठवा. पुढल्या पुस्तकांसाठी, आवृत्त्यांसाठी त्यांचा उपयोग होईल. ह्याच पुस्तकाच्या जोडीने '१००१ सर्वोत्कृष्ट वेबसाईट डिरेक्टरी' प्रकाशित झाली आहे. भारतीय भाषेत अशी सर्वोत्कृष्ट वेबसाईटस् सचित्र देणारी डिरेक्टरी आमच्या तरी माहितीत नाही. ही पुस्तके आपल्याला वाचून आवडली तर संगणक वापरणाऱ्या आपल्या दुसऱ्या मित्राला 'संगणक प्रकाशन' च्या कार्याची व पुस्तकांची माहिती 'ई मेल'ने जरुर कळवा. 'संगणक प्रकाशना'च्या प्रसारासाठी तुमचा हा सहभाग ह्यापुढेही हवा आहे...

mshirvalkar@hotmail.com

कहाँ से तू आया और कहाँ तुझे जाना है ?

बऱ्यापैकी बजेट बांधून आपण घरी किंवा ऑफिसात काँप्युटर आणतो. कधी बँकेचं कर्ज घेऊन तो आणलेला असतो किंवा कधी साठवलेले पैसे खर्चून त्याचे आगमन झालेले असते. मग आपण त्याला जपत असतो. त्यात धूळ जाऊ नये, कुणी त्याला हात लावू नये अशी काळजी घेतली जात असते. ''एवढे पैसे टाकलेत, हा काँप्युटर बिघडणार तर नाही ना?'' असं एक टेंशन डोक्यावर असतं. ''आपल्याला त्यातलं काही कळत नाही, उगाच बिघडायला नको'' म्हणत घरचे आजी-आजोबा आणि वडीलधारी मंडळी त्यापासून चक्क चार हात लांब राहतात. घरात साफसफाईचे काम करणारा नोकर किंवा कामवाली बाई यांना तिथे न जाण्याची ताकीद दिलेली असते. बंद असलेल्या काँप्युटरवर चक्क टोपडं आणि पांघरुण चढवलं जात असतं. पाळण्यातल्या बाळाला सांभाळावं तसं आपण आपल्या काँप्युटरला सांभाळत असतो.

खूप सांभाळून सुध्दा कधी-कधी बाळाला सर्दी होते. थोडासा ताप चढतो. सारखं रडं सुरु होतं. सर्वांना काळजी उत्पन्न होते. मग डॉक्टरांची पायरी आपण चढतो. डॉक्टर बाळाला तपासतात. पोट दाबून पाहतात. स्टेथास्कोपने तपासून पाहतात, आणि म्हणतात ''घाबरण्यासारखं काही नाही. थोडं व्हायरस इन्फेक्शन आहे. औषध देतोय. दोन दिवसात ठीक होईल.'' डॉक्टरांच्या औषधाने खरच बरं वाटतं. बाळ पुन्हा हंसू-खेळू लागतं. ताप कुठल्या कुठे पळून गेलेला असतो. सर्दी खोकल्याचा मागमूस

उरलेला नसतो. थोडक्यात काय, तर डॉक्टरांच्या त्या औषधाने बाळाच्या शरीरात शिरलेला 'व्हायरस' हद्दपार तरी झालेला असतो, किंवा नाहीसा तरी झालेला असतो. मराठीत 'व्हायरस' ला आपण विषाणू म्हणतो. विषाने भरलेला अणू-रेणू असाच त्यामागचा अर्थ आहे. मध्येच काही कारणाने हवेत म्हणा, पाण्यात म्हणा, खाण्यापिण्यात म्हणा कुठले तरी व्हायरस येतात आणि मग त्यांची एक साथच सगळीकडे पसरते. फक्त आपल्याच घरातलं बाळ 'व्हायरस इन्फेक्शन' ने कण्हत असतं असं नाही. आसपासची बाळंही डॉक्टरांकडे आलेली असतात. मग आपण म्हणतो ''सध्या तापाच्या 'व्हायरस' ची साथ आलीय सगळीकडे.'' दुसरं एखादं निरोगी बाळ पाहून त्याच्या आईला आपण म्हणतो ''सांभाळा होऽ, काळजी घ्या. सध्या 'व्हायरस' ची साथ आहे. आमच्या बाळाला इन्फेक्शन झालय.'' मग इन्फेक्शन झालेल्या बाळाजवळ आपण दुसऱ्या निरोगी बाळाला येऊ देत नाही. कारण इन्फेक्शन एकाकडून दुसऱ्याकडे पसरु शकतं.

आपल्या आजारपणातला व्हायरस आणि काँप्युटरचा व्हायरस यांच्यात अनेक प्रकारचं साम्य आहे. व्हायरस माणसाच्या शरीरात शिरतो, तर काँप्युटरचा व्हायरस त्याच्या हार्ड डिस्कमध्ये अन्य एखाद्या प्रोग्राममध्ये किंवा मेमरीत शिरतो. वैद्यकीय व्हायरस शिरल्याने सर्दी, खोकला, ताप वगैरे लक्षणं दिसू लागतात. माणसाला अशक्तपणा वाटू लागतो. तसच काँप्युटरचंही आहे. काँप्युटरमध्ये व्हायरस शिरला की कधी काँप्युटर मंद चालू लागतो. चित्रविचित्र संदेश दिसू लागतात. कधी-कधी आपल्याला हवा तो काँप्युटर मधला डेटा गाळला गेलेला असतो. कधी आपल्याला अनोळखी अशा फाईल्स किंवा डेटा अचानक काँप्युटरमध्ये दिसू लागलेला असतो. थोडक्यात सांगायचं तर काँप्युटरच्या 'त्या' व्हायरसमुळे आपला काँप्युटर चक्क आजारी पडलेला असतो. आपल्या बाळाची जशी केविलवाणी अवस्था झाली होती तशीच काहिशी आपल्या काँप्युटरचीही झालेली असते. आता काँप्युटरलाही बाळासारखाच काहीतरी उपाय करण्याची वेळ आलेली असते. व्हायरस नेमका कसला आहे, हे तपासण्याची आवश्यकता निर्माण झालेली असते. तो तपासून निदान होईल तेव्हा औषध कोणते द्यावे ते ठरणार? म्हणजेच 'डायग्नोसिस'ही आले, आणि 'मेडिसिन' ही आले. आपल्या ह्या पुस्तकाचा विषयच हा आहे. पुढली सर्व प्रकरणे आपण

व्हायरसचे स्वरुप पाहणार आहोत आणि त्यावरचे उपायही लक्षात घेणार आहोत.

आतापर्यंतचं भारुड ऐकल्यानंतर म्हणजे वाचल्यानंतर तुम्ही मला एक साधा प्रश्न विचाराल. तुम्ही म्हणाल ''अहो ऽ काँप्युटर म्हणजे एक यंत्र आहे. काँप्युटर यंव करतो, त्यंव करतो असं म्हणता, मग अशी सोय का करीत नाही की काँप्युटरमध्ये व्हायरस शिरुच शकणार नाही. माणसाला सुध्दा आपण पोलीओचा डोस, बीसीजीची किंवा देवीची वगैरे लस टोचतो. मग ते व्हायरस निष्प्रभ होतात. असा काही शोध काँप्युटरच्या बाबतीत लागलाय की नाही?''

तुम्ही विचारलेला प्रश्न अगदी बिनतोड आहे. माणसासाठी जर लस असू शकते, तर काँप्युटरसाठी का नाही असू शकत? तुमच्या प्रश्नाचं उत्तर असं आहे की ''काँप्युटरसाठीही प्रतिबंधक उपाय आहेत. पण अनेकदा प्रतिबंधक उपाय योजूनही काही वेळा व्हायरस आत शिरतातच''. वातावरणात जसे वेगवेगळे व्हायरस निसर्ग तयार करीत असतो, आणि अशा नवनव्या व्हायरसमुळे कधी कधी डॉक्टरांनाही निदान होऊ शकत नाही असे ताप किंवा खोकले वगैरे साथीने येत असतात तसंच काँप्युटरचंही आहे. नवनवे व्हायरस काँप्युटरच्या विश्वातही तयार होत असतात, मग त्यांचे निदान करायचे आणि नंतर त्यावर उपाय शोधायचा असा प्रकार करावाच लागतो. हा उपाय निघेतो जीव मुठीत धरुन बसण्याची पाळी येते. माणसं डोळ्यात तेल घालून दक्षता घेऊ लागतात. आणि, तरीही वृत्तपत्रात आपण बातम्या वाचतोच. 'लव्ह लेटर' नावाचा व्हायरस आलाय. 'बबल बॉय' नावाच्या व्हायरसने सगळीकडे हा:हाकार उडवलाय. मेलिसा व्हायरसने जग हादरले वगैरे वगैरे.

मंडळी, तुम्ही कुठलंही क्षेत्र घ्या. त्यात 'पॉझीटीव्ह' आणि 'निगेटीव्ह' असे दोन्ही घटक हे असणारच. संगणकाचं क्षेत्र त्याला अपवाद कसं असणार? संगणक मानवजातीच्या सेवेसाठी एक देवदूत उभा रहावा तसा उभा राहिला आहे. त्याच्या विकासासाठी चाललेल्या कामात म्हणजे सकारात्मक किंवा विधायक किंवा 'पॉझीटीव्ह' कामात 'व्हायरस' सारखा एखादा निगेटीव्ह प्रकार आला नसता तरच नवल झाले असते. कोणत्याही क्षेत्रात चांगल्या-वाईटाची लढाई नेहमीच चालू असते. पूर्वीही होती, आजही आहेच. हिरो असला की व्हीलन आलाच. काळा रंग आणि पांढरा रंग

असायचेच. थोडक्यात काय, तर आजमितीस तरी कॉंप्युटर व्हायरसवर ठाम आणि रामबाण असा सर्वसमावेशक उपाय उपलब्ध नाही. नवनवे व्हायरस येणार, त्यावर नवनवे उपायही येणार. नवे व्हायरस आले की ते नुकसान करणार, अनेक संगणकांना ताप आणणार, अशक्तपणा आणणार, मग त्या तापातून संगणक पुन्हा उठणार. बरा होणार आणि पुन्हा कामाला लागणार.

आपले आजचे आयुष्य हे संगणकाविना कल्पनेतही आणता येणार नाही. ३१ डिसेंबर १९९९ च्या रात्री बारा वाजता 'वायटूके' चा प्रॉब्लेम होणार म्हणून जग केवढे धास्तावले होते हे लक्षात आहे ना? काहींना वाटत होते की ह्या 'वायटूके' मुळे विमाने पडणार, बँका बुडणार किंवा बंद पडणार, वृत्तपत्रेही यायची नाहीत, वाहतूक व्यवस्था ठप्प होईल, क्षेपणास्त्रे आपोआप उडतील, बॉम्ब आपोआप फुटतील. कदाचित मानव जातीचाच संहार होईल इथपर्यंतची चर्चा तेव्हा झाली होती. कल्पना करा, एका 'वायटूके'च्या दोषामुळे, म्हणजे संगणकाच्याच एका दोषामुळे काय काय होणार अशा काळजीने जगभरची मानव जात चिंतेत सापडली होती. हेच संगणक एखाद्या भयानक व्हायरसमुळेही अशा गोंधळात सापडू शकतात, आणि म्हणूनच आजकाल 'कॉंप्युटर सिक्युरिटी' हे एक नवेच क्षेत्र उदयाला येऊ लागले आहे. ह्या क्षेत्रातला महत्वाचा भाग 'कॉंप्युटर व्हायरस'च्या अभ्यासाने भरलेला आहे.

कल्पना करा, की १९८१ साली आय.बी.एम. कंपनीने पहिल्यांदा पर्सनल कॉंप्युटर बाजारात आणला. तत्पूर्वी सामान्य माणसाला 'कॉंप्युटर'हा प्रकार कधी आपल्या घरात येईल याची कल्पनाही नव्हती. १९८१ साली जेव्हा आय.बी.एम. कंपनीने पीसी कॉंप्युटर आणला तेव्हा काही वर्षांतच आपल्यापुढे 'व्हायरस'नावाचे संकट कायमचे उभे राहणार आहे, याची स्पष्ट कल्पना त्यांनाही नव्हती. म्हणजेच, पर्सनल कॉंप्युटरच्या व्हायरसचा इतिहास हा अगदी गेल्या २० वर्षांतला म्हणजे आताआताचाच आहे. पण गेल्या तीन चार वर्षांत हे प्रकरण जगापुढे एक भयानक आव्हान म्हणून उभे आहे. जसजसा इंटरनेट, ई मेल, चॅट, फाईल्स डाऊनलोडींग वगैरे सुविधांचा प्रचार आणि प्रसार होतो आहे, तसतशी ही व्हायरसची समस्या अधिकाधिक उग्र होत चालली आहे.

आता एवढी चर्चा मी केल्यानंतर तुम्ही मला काय विचारणार हे मी

जाणून आहे. तुम्ही विचारणार की वातावरणातले व्हायरस हे जिवाणू असतात. पाणी, हवा, अन्न किंवा अन्य मार्गाने हे जीव शरीरात जातात. तेथे राहतात वस्ती करतात. वाढतात मग उपद्रव करतात. कधी कधी त्यात माणूस दगावूही शकतो. हे जिवाणू निसर्गच जन्माला घालत असतो. काँप्युटरचे व्हायरस नेमके कसे असतात? तेही जिवाणू असतात का? ते काँप्युटरमध्ये आत कसे शिरतात? आत जाऊन ते वस्ती करतात का? वाढतात का? नेमके काय होते? काँप्युटर रुममध्ये जाताना चपला -बूट बाहेर काढायला सांगतात. त्याचे कारण व्हायरस लागू नये हेच आहे का?

मंडळी, तुम्ही मला अनेक प्रश्न एकाच वेळी विचारलेले आहेत. अगदी बुनियादी म्हणावे असे प्रश्न आहेत. तुमचे ''व्हायरस' कीस झाड की पत्ती है'' हे तुम्हाला जाणून घ्यायचय. ''व्हायरस'' कहाँसे तू आया और, कहाँ तुझे जाना है'' हा तुमचा सवाल आहे. मला वाटतं की हे जाणण्यासाठी आपण वळू या पुढल्या प्रकरणाकडे, आणि तोपर्यंत घेऊ या एक ब्रेक - जाहिरातींसाठी नाही, थंड डोक्याने 'व्हायरस' जातीचा समाचार घेण्यासाठी.....

'व्हायरस' म्हणजे नेमके काय?

मला दोन घडलेले प्रसंग आठवतात. बहुधा १९८८ साल असावे मी एका छोट्या वृत्तपत्राचे काम पहात असे. ह्या वृत्तपत्राचा मजकूर तेव्हा नव्यानेच कॉंप्युटरवर कंपोज होऊ लागला होता. बाहेरच्या एका डीटीपी सेंटरमध्ये आम्ही लिहीलेली पाने घेऊन जायचो. तिथे प्रत्यक्ष तिथले ऑपरेटर तो कंपोज करीत आणि आम्हाला प्रुफे देत. तिथली कॉंप्युटर रुम म्हणजे एक काचेची पॅकबंद पेटीच होती. बाहेर मोठा बोर्ड लावलेला होता - ''कृपया आपले बूट आणि चपला बाहेर काढा.'' तिथले ऑपरेटर हा नियम अगदी कटाक्षाने पाळत. स्वत:ही चपला बाहेर काढत. दुसऱ्यांनाही त्याचे गांभिर्य समजावून देत. मला क्वचित त्यांच्या त्या काचेच्या पेटीत जाण्याची वेळ येई. मग मीही निर्मळ मनाने चपला-बूट बाहेर काढी.

एक दिवस मी सकाळी प्रुफे घेण्यासाठी त्या डीटीपी सेंटरमध्ये गेलो. तिकडे शुकशुकाट होता. काचेच्या पेटीत दोन ऑपरेटर बसले होते. बहुधा त्यांना मी आल्याची चाहूल लागली. त्यांनी वळून माझ्याकडे पाहिले. दोघांचाही चेहेरा त्रासिक होता. चेहेऱ्यावर चिंताही पसरलेली दिसली. 'मी बाहेरच थांबावं' अशा अर्थाची खूण त्यातल्या एकाने मला केली. मी त्याबरहुकूम बाहेरच्या बाकावर बसलो. बराच वेळ झाला. अजून दोघेही आतच होते. बसून बसून मी अस्वस्थ झालो. बाकावरून उठलो आणि काचेच्या दरवाज्यावर ''टकऽ टकऽऽ'' केली. पुन्हा त्यांचा त्रासिक भाव. दोघे आपसात काहीतरी बोलले आणि मग त्यातला एकजण जड पावलांनी बाहेर आला. म्हणाला, ''प्रॉब्लेम झालाय. प्रुफे आता मिळणार नाहीत.''

''काय झालं ?'' मी विचारलं.

''व्हायरस आलाय काँप्युटरमध्ये. बहुतेक डेटा उडालाय.'' तो म्हणाला. मी अगम्य चेहेरा केला. काँप्युटरला आजकाल व्हायरस वगैरे लागतो अशी चर्चा मी तेव्हाही ऐकलेली होती. पण प्रत्यक्ष तो लागल्याचे मी प्रथमच पहात होतो. उगाचच काहीतरी विचारायचं म्हणून मी विचारलं '' व्हायरस आलाय? तो कसा काय?''

''काय माहित? इथे बोर्ड लावून सुध्दा लोक ऐकत नाहीत. चपला बूट घालून आत येतात. व्हायरस लागणार नाही तर काय होईल?'' त्याचे आपले तत्वज्ञान.. त्यात मी काँप्युटरचा अडाणी...

काँप्युटरच्या बाबतीत तेव्हा पूर्ण अनभिज्ञ असल्याने त्या पुढे मी काही बोलावे याची सीमा संपली होती. कुणीतरी चपला-बूट घालून काँप्युटरच्या रुममध्ये गेल्याने काँप्युटरमध्ये 'व्हायरस' शिरला असा माझा गोड गैरसमज झाला. 'व्हायरस' शिरल्याने प्रॉब्लेम झाला आणि त्यामुळे आता प्रुफे मिळणार नाहीत हे तात्पर्य समजून घेऊन मी तेथून सटकलो.

'व्हायरस' आणि काँप्युटर यांची एकत्र गाठ माझ्या ज्ञानात तेव्हा प्रथमच पडली होती. कुणीतरी माझा हा गोड गैरसमज आणखी पुढे वाढवला. काँप्युटरला अजिबात धूळ चालत नाही. म्हणूनच काँप्युटर रुमला एसी लावतात. धूळीमुळे काँप्युटरला व्हायरस इन्फेक्शन होतं असं नवं आणि चुकीचं ज्ञान माझ्या डोक्यात घुसलं होतं, आणि ''असेल बुवा व्हायरस धूळ आणि घाणीमुळे पसरत असेल आणि काँप्युटरमध्ये शिरत असेल'' असं म्हणून मी माझ्या कामाकडे वळलो होतो. किती तरी महिने पुढे माझा हा भोळेपणा आणि गोड गैरसमज कायम होता.

१९८९ साली पहिल्यांदा माझ्याकडे पीसी-एटी २८६ हा काँप्युटर मी ऑफिसमध्ये आणला. आता आम्ही बाहेरच्या डीटीपी सेंटरमध्ये काम देणे बंद केलं होतं. कार्यालयातल्या नव्या काँप्युटरवरच प्रुफे, कंपोज वगैरे काम सुरु झाले होते. काँप्युटरच्या की बोर्डला तेव्हा मी हलकेच स्पर्श करुन पाहिला होता. एक दिवस दुपारची वेळ होती. आमचा ऑपरेटर माझ्याकडे घाबरलेल्या मुद्रेने आला, म्हणाला ''साहेब मला वाटतं काँप्युटर बिघडलाय, 'व्हायरस'चा मेसेज येतोय. इंजिनीयरला बोलवाव' लागणार '' तो घाबरलेला पाहून मीही जरा चरकलो. पण सावरुन माहीतगाराचा आव

आणत म्हणालो ''काय मेसेज काय येतोय?'' आम्ही दोघे मॉनिटरशी गेलो. लाल चौकटीत बटबटीत मोठ्या अक्षरात मेसेज होता '' Alert! Your system is infected by 'Miechalangelo Virus'. 'व्हायरस' चा संदेश स्पष्टच होता. काळजीयुक्त मनाने आम्ही इंजिनीयरला पाचारण केले. फोनवरून त्याला संदेश सांगितला. 'हार्ट अॅटॅक' आल्यावर आपण डॉक्टरला फोन करताना आपला स्वर कसा असेल, तसाच आमचा स्वर होता.

''हं आजकाल मिक आहे सगळीकडे'' फोनवरून आमचा इंजिनीयर सहज शब्दात म्हणाला.

'' 'मिक' नाही, मायकेलअँजलो व्हायरसचा मेसेज आहे.'' मी त्याची चूक दुरुस्त करीत म्हणालो.

आमच्या इंजिनीयरने माझे अगाध अज्ञान ओळखले असावे. तो म्हणाला ''काँप्युटर 'ऑफ' करा मी आलोच.'' काही वेळाने इंजिनीयर महाशय बॅग घेऊन आले. आम्ही त्यांच्या आज्ञेप्रमाणे 'ऑफ' केलेला काँप्युटर त्यांनी ऑन केला. आता मी आणि आमचा ऑपरेटर दोघेही उत्सुकतेने पाहू लागलो होतो. इंजिनीयर आता नेमकं काय करणार याची आम्हाला उत्सुकता होती. काँप्युटर 'ऑन' झाल्यानंतर पुन्हा तोच मेसेज आला. " Alert! Your system is infected by 'Miechalangelo Virus". आमच्या इंजिनीयरचा चेहेरा स्थित प्रज्ञच होता. त्यांने शांतपणे बॅग उघडली. आतून एक फ्लॉपी काढली. ती काँप्युटरमध्ये घातली. काँप्युटर 'ऑफ' करुन पुन्हा ऑन केला. आत मात्र तो व्हायरस मेसेज आला नाही. इंजिनीयरने काहीतरी टाईप केले. मला आठवते की त्याने 'र्ण्तीह : स्म्म्' असे काहीतरी टाईप केले होते. काही क्षणांनी संदेश आला '' Miechalangelo' removed system cleaned."

आमच्या इंजिनीयरने एका साध्या फ्लॉपीने काही क्षणात 'मायकेलएंजेलो' नावाचा व्हायरस काढल्याचे पाहून त्याच्याबद्दलचा माझा आदर द्विगुणित नव्हे, चक्क शतगुणित झाला. मी त्याच्यासाठी आदबीने 'स्पेशल चहा' मागवला. आता माझी व्हायरसबद्दलची उत्कंठा जागृत झाली होती.

''आम्ही कधीही बूट चपला घालून काँप्युटरजवळ जात नाही. मग हा व्हायरस कसा आला?'' मी इंजिनीयरला सवाल केला.

''बूट-चपला आणि 'व्हायरस'चा संबंधच काय?'' त्यानेच मला उलटा सवाल केला.

''धूळ घाणीमुळेच व्हायरस लागतो ना?'' मी आता माझे अज्ञान प्रकट केले.

''छे छे, धूळ आणि घाणीचा व्हायरसशी कसलाही संबंध नाही. घाणीमुळे व्हायरस वगैरे पसरतात ते मेडिकल फिल्डमधले काँप्युटरचे व्हायरस असे पसरत नाहीत.'' इंजिनीयरने सांगितले.

''पण मग हा व्हायरस आमच्याकडे कसा आला? सकाळपर्यंत तो नव्हता.'' मी विचारले.

''बाहेरची फ्लॉपी आणली होती का?'' इंजिनीयरने विचारले

मी आमच्या ऑपरेटरला बोलावले.

''अहो हे काय म्हणताहेत? आपण बाहेरची फ्लॉपी आणली होती का?''

ऑपरेटर चपापला. म्हणाला, ''होऽ माझ्या मित्राकडून मी चार फाँट नवे आणले होते. त्याची फ्लॉपी आणली होती''

''त्या फ्लॉपीत व्हायरस असणार बघा'' इंजिनीयर म्हणाला.

''या दाखवतो'' असं म्हणत इंजिनीयरसाहेब उठले.

''अहो नको जाऊ द्या. उगाच पुन्हा व्हायरस लागायचा'' मी काळजीने म्हणालो.

''काही होत नाही. या.'' इंजिनीयर महाशयांनी ती फाँटची फ्लॉपी काँप्युटरमध्ये घातली, आणि व्हायरस स्कॅनचा आमच्याच काँप्युटरमधला एक प्रोग्राम चालू केला. ती फ्लॉपी 'व्हायरस स्कॅन' केल्यानंतर दिसले की त्यात 'मायकेलएंजेलो' व्हायरस आहे.

''हे बघा. ह्याच फ्लॉपीतून तो आला. फ्लॉपी क्लीन करु का?'' त्याने आमच्या ऑपरेटरला विचारले.

''ते फाँट पुसले जाणार नाहीत ना?'' आमच्या ऑपरेटरला मित्राच्या फ्लॉपीची काळजी होती.

''नाही नाही. फक्त व्हायरस काढतो'' म्हणत इंजिनीयरने पुन्हा ती मगासशीच 'Clean : mich' वगैरे कमांड टाईप केली. पुन्हा तोच Miechalangelo' removed. System cleaned वगैरे संदेश आला. आता त्या फ्लॉपीतला व्हायरसही गेला होता.

''तुमच्या मित्राच्या काँप्युटरमध्येही व्हायरस असणार बघा'' इंजिनीयरने ऑपरेटरला सांगितले.

एव्हाना माझ्या लक्षात येऊ लागले होते की आपल्या शरीरातला रोगाचा व्हायरस आणि हा काँप्युटरचा व्हायरस यांचा अर्थाअर्थी काही संबंध नसतो. व्हायरस हा घाणीमुळे किंवा धुळीमुळे वगैरे येत नसतो. मात्र तो फ्लॉपीतून काँप्युटरमध्ये आणि काँप्युटरमधून फ्लॉपीत अशा प्रकारे पसरु शकतो. मला हेही लक्षात आले होते की आमचे व्हायरसबद्दलचे अज्ञान अफाट आणि ज्ञान शुन्य होते, आणि म्हणूनच आम्ही घाबरून गेलो होतो. खरं तर घाबरून काही होणार नव्हते. इंजिनीयरला याची चांगली माहिती होती. त्यामुळेच तो शांत होता. आमच्यासारखा गडबडून -गोंधळून गेलेला नव्हता.

''काय होऽ तुमच्या बॅगेतून तुम्ही तुमची फ्लॉपी काढलीत, आणि काही क्षणात तो व्हायरस क्लीन केलात. तुमची ही फ्लॉपी काही खास आहे का? मी इंजिनीयरला विचारले.

''नाही ही साधीच फ्लॉपी आहे. पण ती क्लीन आहे. त्यात व्हायरस नाही. त्यात 'स्कॅन' आणि 'क्लीन'चा प्रोग्राम आहे. तो वापरूनच मी 'मिक' काढला.''

''तुम्ही 'मिक' म्हणताय. त्याचे नाव तर 'मायकेलएंजेलो' आहे ना?'' मी आता स्वत:चे ज्ञान वाढवायला सरसावलो होतो.

''मिक हे 'मायकेलएंजेलो' चे कोड नेम आहे. व्हायरस लिहिणाराने कोड लिहिताना 'मिक' म्हणून लिहिले आहे.'' इंजिनीयर म्हणाला.

''कोड? कसलं कोड?'' मी विचारलं.

''व्हायरसचं प्रोग्राम कोड'' इंजिनीयर आता माझ्या तावडीतून सुटण्यासाठी बॅग सावरु लागला होता.

'' म्हणजे व्हायरसचं प्रोग्रमिंग वगैरे असतं.'' माझं विचारणं चालूच होतं.

''व्हायरस हा एक प्रोग्रामच असतो. फक्त तो 'नॅस्टी' प्रोग्राम असतो.'' 'नॅस्टी' म्हणजे खोडकर-कुरापती हा अर्थ सुदैवाने मला माहित होता.

आलेला स्पेशल चहा संपवून बॅग आवरून इंजिनीयर गेला खरा, पण जाता जाता तो माझे गोड गैरसमज दूर करून गेला होता. आता मी आत्मविश्वासपूर्वक इतरांना समजावून सांगू शकत होतो की 'व्हायरस म्हणजे दुसरे-तिसरे काही नसते. तोही एक प्रोग्रामच असतो, फक्त तो 'नॅस्टी'प्रोग्राम असतो.'

आम्ही आमच्या प्रुफांसाठी आणि कंपोजिंगसाठी तेव्हा व्हेंचुरा आणि पेजमेकर हे प्रोग्राम वापरायचो, हे प्रोग्राम आम्ही पैसे मोजून त्या त्या कंपनीकडून विकत घेतले होते. कारण ते प्रोग्राम्स त्या कंपन्यांनी बनविलेले होते.

इंजिनियर गेल्यानंतर मला हाच प्रश्न पडला की 'व्हायरस' हाही जर पेजमेकरसारखा एक प्रोग्रामच असेल तर तो कोण बनवितो? पेजमेकर हा उपयुक्त प्रोग्राम आहे. व्हायरस हा डोकेदुखी आणणारा विध्वसंक प्रोग्राम आहे. तो कोण कशासाठी तयार करेल?

व्हायरसबद्दलचे माझे अज्ञान अजून अफाट पसरलेले आहे याची मला तेव्हा कल्पना आली. पण माझ्या ज्ञानाचा पहिला धडा गिरवून झाला होता. माझ्या कार्यालयात तो घडलेला 'मायकेलएंजेलो' व्हायरसचा प्रसंग मला हे शिकवून गेला होता की 'व्हायरस हा एक कॉंप्युटर प्रोग्रामच असतो' आणि ज्या अर्थी तो कॉंप्युटर प्रोग्राम आहे त्या अर्थी कुणीतरी माणसानेच तो बनविलेला असणार. कारण प्रत्येक कॉंप्युटर प्रोग्राम हा मानवनिर्मितच असतो.

'व्हायरस' चे ज्ञान मला देणारे हे दोन गुरु एक तो प्रसंग म्हणजे अनुभव आणि तो इंजिनीयर (साक्षात गुरुच की तो) यांना मी कधी विसरु शकेन का?'

व्हायरस: एक नको असलेला पाहुणा

कल्पना करा की तुमच्या घरी एक अनाहूत पाहुणा अचानक येतो. येतो कसला, खरं तर तो तुमच्या घरी जबरदस्तीने घुसतो. हा पाहुणा तसा निरुपद्रवी आहे. तो तुम्हाला मारत नाही, घराची मोडतोड करीत नाही. तुमच्या घरातलं काही खात सुध्दा नाही. मात्र हा पाहुणा एका भुताटकीने पछाडलेला आहे. तो आपले अनेक डबलरोल तयार करतो. म्हणजे ह्या पाहुण्यासारखाच आणखी एक पाहुणा तुमच्या घरात तयार होतो. हे डबल रोल वाढतच जातात. दहा होतात, शंभर होतात, हजार होतात, आणि पुढे ही संख्या वाढतच जाते. यामुळे तुमच्या घरातल्या माणसांना अडचण होते. घरचं सगळं 'घरपण' संपून जाऊ लागतं. तुम्हाला वाटतं की ह्या पाहुण्याला हाकलून द्यावं. आपल्या घरात हाही नको, त्याची ती डबल रोल रुपेही नकोत...

काँप्युटर व्हायरस ह्या पाहुण्यासारखाच असतो. तो तुमच्या नकळत, तुमची परवानगी न विचारता तुमच्या काँप्युटरमध्ये शिरतो. तिथे आपले डबल रोल निर्माण करु लागतो. नकळत आणि विनापरवानगी शिरणे आणि आपल्या अनेक प्रतिमा किंवा प्रती तयार करीत राहणे हे काँप्युटर व्हायरसचे प्रमुख गुणधर्म आहेत.

आता आपण वर घेतलेलं ते अनाहूत पाहुण्याचं उदाहरण थोडं पुढे नेऊ. समजा, हा अचानक शिरलेला उपटसुंभ पाहुणा तुमच्या घरातल्या माणसांना, नातेवाईकांना मारु लागला तर! तुमच्या घरातल्या सामानाची तोडफोड करु लागला तर? घराच्या भिंती, दरवाजे, खिडक्यासुध्दा

उखडू लागला तर? आणि हे क्रौर्यकर्म करण्यासाठी त्याने आपले असंख्य डबल रोल करुन ती सगळी मंडळी असाच विघातक उच्छाद मांडू लागली तर?

तर आपल्याला ह्या पाहुण्याचा समाचार घ्यावाच लागणार. त्याला आपल्या घरातून त्याच्या सर्व डबल रोलसकट हुसकून बाहेर काढावं लागणार. प्रसंगी पोलीसांना बोलवावं लागणार. आणि जर हा पाहुणा तरीही हल्ला चालूच ठेवू लागला तर पोलीस त्याला बंदुकीने ठार करणार. हे सारं ओघानच आलं.

काँप्युटर व्हायरस हा पूर्ण निरुपद्रवीही असू शकतो, आणि तो पूर्ण उपद्रवीही असू शकतो. उपद्रवी व्हायरस संगणकात राहणं फारच धोक्याचं असतं. निरुपद्रवी व्हायरस काही काळ राहिल्याने तसा मोठा फरक पडत नसतो.

व्हायरस काय करतो?

आपण गेल्या प्रकरणात पाहिलं की 'व्हायरस' हाही एक प्रोग्रामच असतो. फक्त तो चोरासारखा असतो. तो गुपचुप संगणकात शिरतो. गुपचुप म्हणजे कसा? तर, तुमच्या मित्राच्या घरुन आणलेल्या फ्लॉपीतून तो आत शिरु शकतो. तुम्ही जेव्हा फ्लॉपी टाकता आणि त्यात काय आहे हे पाहण्यासाठी 'ए' ड्राईव्हवर माऊसने डबल क्लीक करता तेव्हा प्रथम फ्लॉपीच्या बूट सेक्टरचे काम सुरु होते. फ्लॉपीचा तुमच्या संगणकाशी संपर्क प्रस्थापित करण्यासाठी काही प्रोग्रामिंग कोडस् आवश्यक असतात. ह्या प्रोग्राममधून लपून व्हायरससाहेबही आत शिरतात. अशा प्रकारे लपून आणि गुपचुप शिरावं अशी ती योजनाच असते. अगदी जाणून बुजून केलेली. एकदा आत शिरला की त्याने काय करावं याचेही नियोजन व्हायरस प्रोग्राम तयार करणाराने विचारपूर्वक करुन ठेवलेले असते. म्हणजेच, व्हायरस हा कुणीतरी माणसानेच अत्यंत विचारपूर्वक तयार केलेला एक उपद्रवी आणि नतद्रष्ट प्रोग्राम असतो.

काँप्युटरसाठी लागणारा चांगला व उपयुक्त प्रोग्राम असो की व्हायरससारखा नकोसा आणि घातकी प्रोग्राम असो प्रोग्रामरला तो तयार करावा लागतो. ह्यालाच आपण प्रोग्राम लिहिणे असेही म्हणतो. म्हणूनच

'व्हायरस रायटर', 'ऑथर ऑफ द व्हायरस' वगैरे शब्दप्रयोगही इंग्रजीत वापरले जातात. कोणताही प्रोग्राम तयार करायचा तर त्यासाठी कॉंप्युटरच्याच प्रोग्रामिंग लँग्वेजेस वापराव्या लागतात. Delphi, Assembly, Visual Basic वगैरेसारख्या प्रोग्रामिंग भाषा व त्यांचे कोडस् वापरुनच प्रोग्राम लिहावे लागतात. ह्या भाषा व कोडस् अत्यंत जिकीरीच्या काहीशा कंटाळवाण्या आणि क्लीष्ट असतात. त्या वापरुन एखादी निर्मिती करायची असो की काही विध्वंस करायचा असो, त्यासाठी पुरेसा विचार, नियोजन व परिश्रम हे करावेच लागतात. प्रत्येक प्रोग्राम हे प्रोग्रामरसाठी एक अखंड आव्हानच असते.

आपण पाहतो की 'मायक्रोसॉफ्ट वर्ड' सारखा एक उपयुक्त प्रोग्राम लोक घराघरात वापरतात. शेवटी 'विंडोज' हा तरी काय आहे? मायक्रोसॉफ्टने तयार केलेले तोही एक प्रोग्रामच आहे. त्यात विविध क्रिया अंतर्भूत आहेत. ह्या प्रोग्रामच्या सहाय्याने तुमचा स्पीकर चालत असतो. मॉनिटरवर रंग येत असतात, चित्रे लहान-मोठी होत असतात, टेलिफोनमधून संपर्क प्रस्थापित होत असतो. थोडक्यात प्रोग्रामिंगच्या भाषा मध्ये प्रचंड ताकद असते. त्यांचा वापर करुन तुमच्या संगणकाच्या स्पीकरवर तुम्ही छानसे गाणे ऐकू शकता. पण हाच प्रोग्रामिंग भाषांचा दुरुपयोग करणारा असेल तर? तो असेही प्रोग्रामिंग करील की दर वेळी 'एंटर' बटण दाबलत तर तुम्हाला गाण्याऐवजी एखादी घाणेरडी शिवी ऐकायला येईल. स्फोटाचा आवाज येईल. एखाद्या अशा प्रोग्रामने तुमच्या कॉंप्युटरमध्ये गुपचुप शिरुन शिव्या द्यायला सुरुवात करणे हाही एक व्हायरसचाच प्रकार म्हणावा लागेल.

पण समजा तुम्ही मनोरंजनाच्या मूडमध्ये आहात. तुमच्या एक मित्राने तुम्हाला एक गंमतीदार प्रोग्राम दिला. हा प्रोग्राम लोड केल्यानंतर जर तुम्ही की बोर्डवरचे बटण दाबलेत तर विशिष्ट आवाज येतो. म्हणजे समजा 'ए' बटण दाबले तर वाघाचा आवाज येतो. 'बी' दाबले तर चिमणीचा आवाज येतो वगैरे. आता हा प्रोग्राम तुम्ही तुमच्या इच्छेने तुमच्या संगणकात लोड केला आहे. बटण दाबल्यानंतर तो शिवी देईल किंवा वाघाचा आवाज काढील. जे काही प्रोग्राममध्ये असेल तशा क्रिया होतील. नंतर तुम्ही हवं तर तो प्रोग्राम काढून टाकाल. एक्झीट कराल.

किंवा अनइन्स्टॉल' कराल.

व्हायरस प्रोग्राम आणि कंन्स्ट्रक्टीव्ह (विधायक-चांगला) प्रोग्राम यात फरक हा की विधायक प्रोग्राममध्ये त्यातील विशिष्ट क्रिया तुमच्या मनाप्रमाणे व इच्छेप्रमाणे होतात, तुम्हाला त्या नियंत्रित करता येतात. तो प्रोग्राम बंद करण्याची वा संगणकातून काढून टाकण्याची सोयही प्रोग्रामरने केलेली असते. मुख्य म्हणजे तो प्रोग्राम तुम्हाला मदत करण्यासाठी, सोय-सुविधा तुम्हाला मिळावी यासाठी तयार केलेला असतो. असे प्रोग्राम तयार करताना त्यात नजरचुकीने काही दोष वा उणीवाही राहून जात असतात. त्यांना आपण 'बग' (Bug) असे म्हणतो. हे दोष वा उणीवांमुळे काही वेळा संगणकात अडथळे वा व्यत्यय येऊ शकतात. पण 'बग'ला आपण 'व्हायरस' असे म्हणत नाही.

'व्हायरस' हा प्रोग्राम तुम्हाला मदत करण्यासाठी तयार झालेला नसतो. तो काहीतरी चेष्टा-कुचेष्टा व कुरापती काढण्यासाठीच जन्माला घातलेला असतो. तुमचे चांगले चालणारे प्रोग्राम बंद पडावे, उत्तम वेगवान पध्दतीने चालणारा संगणक अचानक गोगलगायीसारखा संथ चालू लागावा, तुमच्या संगणकातला डेटा गाळला जाऊन तुमची त्रेधा-तिरपीट उडावी असाच त्यामागे हेतू असतो. ही गंमत केवळ फक्त तुमच्याच संगणकावर व्हावी असा काही उद्देश नसतो. खरा उद्देश हा असतो की ही त्रेधा-तिरपीट सगळीकडे पसरावी. एका संगणकातून दुसरीकडे जावी. एका फ्लॉपीतून दुसऱ्या फ्लॉपीत जावी. संपूर्ण नेटवर्कवरच्या सर्वच्या सर्व संगणकांमध्ये त्यांचा शिरकाव व्हावा. हा व्हायरस जेवढा अधिक धुमाकूळ घालील तेवढी मजा व्हायरस रायटरला वाटत असते. थोडक्यात काय, तर 'व्हायरस' ह्या विघातकी प्रोग्रामची निर्मिती माणसाच्याच विकृतीभऱ्या मेंदूतून निर्माण होत असते. माणसात 'विकृती' निर्माण होत नसती तर ह्या जगात तुम्हाला एकही व्हायरस दिसला नसता. प्रोग्रामिंग शिकायचे, त्यासाठी मेहनत करायची आणि ते मिळवलेले ज्ञान लोकांची त्रेधा-तिरपीट उडवण्यासाठी, विध्वंसासाठी वापरायचे ही विकृती नाही तर काय?

तुम्हाला कदाचित माहीत असेल किंवा नसेल 'जोशी' नावाचा एक व्हायरस आहे. हा व्हायरस काय करतो? तो वर्षभर काहीही करीत नाही. कसलेही नुकसान करीत नाही, की संगणकात मंदपणाही आणत नाही.

फक्त १८ जानेवारी उजाडली की त्याच्या अंगात येते. संगणक चालू केल्या बरोबर तो संदेश देतो की 'Type Happy Birthday Joshi'. म्हणजे तुम्ही तुमच्या की बोर्डचा वापर करुन ' Happy Birthday Joshi'. असे टाईप करावे असा त्याचा आदेश असतो. जर तुम्ही ते टाईप केले नाहीत तर तो तुमचा संगणक लॉक करुन ठेवतो. तुम्हाला काम करु देत नाही. पण तुम्ही 'Happy Birthday Joshi'. असे टाईप केलेत तर तो तुम्हाला काम करु देतो. पण पुन्हा काही वेळाने 'Type Happy Birthday Joshi'. असा हुकूम फर्मावतो. आता हे वाचताना तुम्हाला हंसू येत असणार. सगळा विनोदी प्रकार वाटत असणार. पण, ''कोणत्या जोशाचा हा १८ जानेवारीचा वाढदिवस माझ्या नशिबी आला'' असं त्या काँप्युटरवाल्याला वाटत असतं, तो बिचारा घाम पुसत असतो त्याचं काय?

पण किंचित विकृती ही तर सर्वांमध्येच असते. बालिश बुध्दी असेल तर मग आणखी विचारायलाच नको. श्री कृष्णाच्या बाललीला आपण कृष्णचरित्रात वाचतो. तो झाडावर चढून लपून गवळणींची मडकी दगड मारुन फोडायचा. किंवा त्यांच्या घरचं लोणी गुपचूप खाऊन टाकायचा तर असेच हे व्हायरसचेही प्रकार.. पण ते कधी कधी तोंडाला फेस आणतात. अब्जावधी रुपयांचं नुकसान करतात. चार पैसे जवळ नाहीत म्हणून माणसाला अन्न मिळत नाही, अणि भूकबळी पडावे लागते असा आपला देश आहे. रहायला निवारा नाही, अंगात घालायला पुरेसे कपडे नाहीत म्हणून थंडीने गारठून माणसे मरतात. कुपोषणाने मुलं बाल्यावस्थेतच झिजत असतात. पण दुसरीकडे रिकामा वेळ असलेल्या विकृत मेंदूतून निघालेले व्हायरस करोडो रुपयांचे नुकसान केवळ गंमत बघण्यासाठी करीत असतात. आजपर्यंत जगात थोडे थोडके नाहीत ५०,००० पेक्षा अधिक व्हायरस लिहिले गेले आहेत. त्यांनी आजपर्यंत किती नुकसान केले असेल ह्याचा विचार करा.

पण हे कधी संपायचे नाही. कारण माणसातील विकृती ही ह्या जगाच्या अंताबरोबरच संपेल असे प्रोग्रामिंग विधात्यानेच करुन ठेवलेले आहे. ऋषी-मुनींनी तप करायचे आणि राक्षसांनीही तप करुन विचित्र वर मिळवून ऋषी-मुनींना छळायचे हा तर इतिहासच आहे. हेच गुणधर्म संगणक जगतातल्या व्हायरसना आणि एकूणच संगणक क्षेत्राला लागू होतात..

आता हे एवढं वाचल्यानंतर तुमचा एक निश्चित प्रश्न असणार की हा '' व्हायरसचा उच्छाद मागे लागू नये म्हणून काय करावे ?''

पुढल्या प्रकरणात तुम्हाला सांगतो एकूण दहा नियम, जे 'व्हायरस'चा यशस्वी सामना करण्यासाठी तुम्हाला कायमचे उपयोगी पडतील.

टेन कमांडमेंटस्, अर्थात दहा कानमंत्र

गेल्या प्रकरणात आपण पाहिलं की व्हायरसचा जन्म विकृतीतून होतो आणि ही विकृती इतरांचे नुकसान करुन त्यातून आनंद मिळवणारांची असते. आपला संगणक अशा विकृतीला, म्हणजे अर्थातच व्हायरसला बळी पडू नये यासाठी दहा कानमंत्र ह्या प्रकरणात दिले आहेत. हे कानमंत्र कटाक्षाने पाळलेत तर 'व्हायरस' चा प्रवेश तुमच्या संगणकात होण्याची शक्यता अगदी दुर्मिळ राहील.

नियम पहिला

'अँटी व्हायरस' प्रोग्राम वापरा, आणि हा प्रोग्राम अद्ययावत ठेवा.

संगणक वापरणारांचे जे सर्वेक्षण केले गेले आहे त्यातून दिसून आले की सुमारे ५५ टक्के संगणक व्हायरस प्रतिबंधक प्रोग्राम (Anti-Virus) वापरत नाहीत. त्यांना असे वाटते की अशा प्रोग्रामची त्यांना आवश्यकताच नाही. बऱ्याच जणांना यातले गांभिर्य कळत नाही, त्यामुळेच ते अँटी व्हायरस प्रोग्राम घेण्यात चालढकल करीत असतात. प्रत्येक देशाला जसे सैन्य हवे तसे प्रत्येक संगणकाला आपला अँटी व्हायरस प्रोग्राम हवा हा पहिला आणि अगदी साधा असा मूलभूत नियम आहे. 'व्हायरस' चे आक्रमण काही रोज होत नाही हे खरे आहे. पण जेव्हा कधी होईल तेव्हा तुमचे अँटी व्हायरस प्रोग्रामचे सैन्य हजर नसेल तर तुमच्या संगणकाचा सहज आणि दारुण पराभव ठरलेला.

सैन्याचेच उदाहरण आपण पुढे चालू ठेवू. लक्षात घ्या की सैन्य सुध्दा

अद्ययावत ठेवावे लागते. एकेकाळी सैन्याकडे ढाली-तलवारी असत. घोडे असत. भाले, दांडपट्टे, हत्ती, रथ असत. आता ते नसतात. पण समजा, एखादा मागासलेला देश ढाली-तलवारींचे सैन्य बाळगू लागला तर ? त्याच्या सैन्यावर विमानातून एक बॉम्ब टाकला की शत्रूचे काम फत्ते! त्याचे तलवारधारी सैन्य विमानावर तलवार फेकू शकतात काय? त्यासाठी रडार आणि विमानविरोधी तोफाच हव्यात. थोडक्यात काय, जुने कालबाह्य बाजूस ठेवून नवे अद्ययावत तंत्रज्ञान तुमच्याकडे संरक्षणार्थ असायलाच हवे. सैन्य असो की अँटी व्हायरस दोघांनाही हाच नियम लागू नाही का? 'व्हायरस' लिहिणारे किंवा तयार करणारे हे तुमच्या संगणकाचे शत्रूच असतात. त्यांचे व्हायरस म्हणजे तुमच्या संगणकाच्या दिशेने फेकलेली क्षेपणास्त्रे असतात. तुमचा संगणक ज्याचा मुकाबला करु शकणार नाही अशी व्हायरसरुपी क्षेपणास्त्रे शोधण्यात येते. मग्न असतात. त्यांनी शोधलेले एखादे नवे व्हायरस क्षेपणास्त्र तुमच्या अँटी -व्हायरस सैन्याला समजले नाही तर ? आणि कसे समजणार?? कारण तुमचा अँटी व्हायरस चार महिन्यांपूर्वीच्या व्हायरसना ओळखतो. त्यानंतरचे व्हायरस तो ओळखत नसेल तर त्यांचा मुकाबला करण्याचा प्रश्न कुठे उद्‌भवतो? म्हणूनच अँटी व्हायरस प्रोग्रामच्या संदर्भातला महत्वाचा भाग हा की तुमचा अँटी-व्हायरस प्रोग्राम अद्ययावत ठेवा.

नॉर्टन, मॅकफी, डॉ. सोलोमन वगैरे सुप्रसिध्द अँटी व्हायरस कंपन्यांच्या वेब साईटस् आहेत, आणि ह्या सर्व कंपन्या सतत नवनव्या व्हायरसच्या संरक्षणाच्या दृष्टीने संशोधन करुन आपल्या ग्राहकांना अद्ययावत सुधारित पुरवण्या इंटरनेटवरुन थेट देत असतात. नवा व्हायरस आला की तो ओळखून त्याला थोपविण्याच्या दृष्टीने आवश्यक ते कोडस् आणि तंत्र ह्या सुधारित भागांतून तुम्हाला मिळत असते. त्यांना 'लाईव्ह अपडेट' असे म्हंटले जाते. नव्या व्हायरसच्या खूणांना 'व्हायरस डेफीनीशन्स' असे म्हंटले जाते. 'लाईव्ह अपडेट' मधून नव्या 'व्हायरस डेफीनीशन्स' तुम्हाला मिळत जातात. त्यामुळे अगदी काल-परवाकडेच नवा आलेला व्हायरस असला तरी तुमचा संगणक त्याला अचूक ओळखतो आणि त्याचा सामना करुन त्याला नामोहरम करतो.

म्हणूनच, इथे सांगावेसे वाटते की चांगल्या अँटी व्हायरस प्रोग्रामसाठी

खर्चिलेली रक्कम ही खरे तर उत्तम गुंतवणूकच माना, आणि सतत हा 'अँटी व्हायरस' प्रोग्राम 'लाईव्ह अपडेट' चा उपयोग करुन अद्ययावत राखा.

नियम दुसरा

अनपेक्षित अॅटॅचमेंटस् उघडू नका

तुम्हाला कृष्णचरित्रातील पुतनामावशीची गोष्ट माहीत आहे ना? बाळकृष्णाला कुशीत घेऊन प्रेमाने आपले दूध पाजायला आलेली पुतनामावशी नेमकी कशासाठी आली होती? एखाद्या व्यक्तीविषयी आपल्याला निरतिशय प्रेम असले, आस्था असली की आपण म्हणतो '' मला त्याच्याबद्दल किंवा तिच्याबद्दल अॅटॅचमेंट आहे. अशी अॅटॅचमेंट पुतनामावशीला बाळकृष्णाबद्दल होती का? ती वर वर प्रेम दाखवित होती. कृष्णाने त्याला फसावे व आपले विषारी दूध प्यावे असा तिचा कपटी डाव होता. कृष्णाने तो ओळखला आणि तिचा डाव तिच्यावरच उलटवून तिला पळवून लावले. पण कृष्णाने तिची ही अॅटॅचमेंट ओळखली नसती तर?

मी तुम्हाला 'अॅटॅचमेंट' बद्दल ह्या 'व्हायरस'च्या पुस्तकात काही सांगतो आहे ते 'ई मेल' बरोबर येणाऱ्या 'फाईल अॅटॅचमेंट' बद्दलच असणार हे तुम्ही ओळखले आहे. पण मी मुद्दामच तुम्हाला पुतनामावशीचे उदाहरण दिले. कारण व्हायरस भऱ्या 'ई मेल अॅटॅचमेंटस्' ह्या नेहमी फसव्या असतात. वरुन त्या उपयुक्त असल्याचा आभास असतो, मात्र आतून त्या पुतनामावशीचे विष घेऊन आपल्या संगणकरुपी कृष्णाला जीवे मारायलाच आलेल्या असतात. उदाहरणार्थ सांगतो. २००१ सालच्या फेब्रुवारी महिन्यात आलेला 'अॅना कॉर्निकोवा' हा व्हायरस आठवा. तोही एका साध्या फाईल अॅटॅचमेंटमधूनच पसरत गेला. एका फाईलबरोबर 'अॅना कॉर्निकोवा'ह्या मादक आणि मदमस्त सुंदरीचे छायाचित्र आहे, तो पहा असा संदेश होता, आणि सोबत त्या छायाचित्राची 'जेपेग'(jpeg) फाईल अॅटॅच केलेली होती. प्रत्यक्षात तो फोटो नव्हता. तो व्हायरस होता. ज्यांनी ही खोटी अॅटॅचमेंट ओळखली ते वाचले. ज्यांनी ओळखली नाही ते कोसळले.

'लव्ह बग' किंवा 'लव्ह लेटर' नावाचा २००० साली आलेला व्हायरसही असाच एक अॅटॅचमेंटच होता. 'ई मेल बरोबर तुम्हाला एक लव्ह लेटर

आहे ते पहा असा संदेश आणि बरोबर 'लव्ह लेटर' ची फाईल अॅटॅचमेंट होती. त्यात ना 'लव्ह' होते ना 'प्रेम'. आत होता एक महाभयानक व्हायरस की ज्याने अब्जावधी डॉलर्सचे नुकसान केले आणि कित्येक दिवस काम बंद पाडले.

बऱ्याचदा ह्या अॅटॅचमेंटस् तुमच्याकडे येतात त्या तुमच्या अगदी जवळच्या मित्राकडून किंवा नातलगाकडून. त्या चटकन उघडून पाहण्यासाठी तुम्ही स्वाभाविकच अधीर असता. पण ही अधीरता आवरा. थोडा सुज्ञपणा दाखवा. कदाचित तुमचा तो मित्र वा नातेवाईक त्या 'फाईल अॅटॅचमेंटला' फसला असेल, आणि त्या फसवणूकीतूनच निष्पाप मनाने ती 'ई मेल' त्याने तुमच्याकडे 'फॉर्वर्ड' केली असेल तर? किंवा तो मित्र /नातेवाईक उपस्थित नसताना त्याच्या नकळत त्याच्या संगणकाचा वापर करुन कुणीतरी तिसऱ्यानेच ही अॅटॅचमेंट मुद्दाम पाठवली असेल तर? काहीही असू शकेल. म्हणूनच प्रथम सावध व्हा. आपल्या अँटी व्हायरस प्रोग्रामचा वापर करुन ती फाईल अॅटॅचमेंट 'स्कॅन' करुन घ्या. त्यात व्हायरस नसल्याची खात्री झाल्यानंतरच मग अशी अॅटॅचमेंट उघडा.

अनपेक्षित आलेल्या अॅटॅचमेंटमध्ये व्हायरस असण्याची शक्यता ५० टक्के असते हा अनुभव आहे.

नियम तिसरा

तुमचा काँप्युटर वापरण्याचा अधिकार इतरांसाठी मर्यादित ठेवा.

सामान्यतः तुमचा काँप्युटर हा तुम्हीच वापरा. इतरांसाठी तो मूळातच खुला करु नका. पण बरेचदा हे शक्य होत नाही. एकच काँप्युटर अनेक जण वापरत असतात. अशा वेळी ह्या दहाही कानमंत्रांचे प्रशिक्षण तुमचा काँप्युटर वापरणाऱ्या इतरांनाही मिळेल अशी व्यवस्था करा. विशेषतः बाहेरची फ्लॉपी, सीडी किंवा तत्सम प्रकारची माध्यमे वापरात येणार असतील तर चांगला व अद्ययावत अँटी व्हायरस आणि मोजक्या व्यक्तींनाच त्या वापरण्याचा अधिकार अशी शिस्त तुम्ही ठेवणं आवश्यक राहील. कुणी मुद्दामून आणून व्हायरस टाकणार नसेलही, परंतु बरेचदा अज्ञानातून वा भोळसटपणातून चुका होतात आणि धूर्तांचे व्हायरस आपला डाव साधतात.

नियम चौथा

वेळच्या वेळी सॉफ्टवेअर पॅचेस लावून घ्या.

किल्ल्याला उत्तम तटबंदी असते, पण कुठेतरी एखादे भोक राहून जाते आणि शत्रूचे सैन्य तिथूनच आत येते अशी उदाहरणे इतिहासात कमी नाहीत. 'विंडोज' हा प्रोग्राम आपण बुहसंख्य मंडळी वापरत असतो. 'ई मेल'साठी 'आऊटलूक' आणि 'आऊटलूक एक्सप्रेस' हे मायक्रोसॉफ्टचेच प्रोग्राम्स असंख्य मंडळी घराघरातून आणि कार्यालयांतून वापरत असतात. पण 'मेलिसा', 'लव्ह लेटर' आणि 'ॲना' व्हायरसेसनी ह्या 'आऊटलूक' आणि 'आऊटलूक एक्सप्रेस' मधील सिक्युरिटी होलचा उपयोग करुनच आपले व्हायरस जगात पसरवले ही वस्तुस्थिती आहे. मेलिसा व्हायरस १९९९ मध्ये येऊन गेल्यानंतर मायक्रोसॉफ्टने एम.एस.ऑफिससाठी एक पॅच (एक पुरवणी सुधारणा प्रोग्राम) आपल्या वेब साईटवरून मोफत दिला होता. पण अनेकांनी ह्या 'पॅच'कडे दुर्लक्ष केले. ज्यांनी हा 'पॅच' लावला होता त्यांना नंतरच्या व्हायरसेसचा त्रास झाला नाही. पण ज्यांनी दुर्लक्ष केले त्यांच्यावर कपाळाला हात लावायची वेळ आली.

म्हणूनच आपण जे प्रोग्राम्स वापरतो त्यांचे पॅचेस वेळच्या वेळी लावून घ्या. हे पॅचेस म्हणजे रोगांच्या प्रतिंबधक लसीसारखेच असतात.

नियम पाचवा

फ्लॉपी / सीडी वापरण्यापूर्वी प्रथम व्हायरस स्कॅन करा.

१९९९ साली सुप्रसिध्द 'कॅस्परस्की व्हायरस लॅब' ने पायरेटेड सॉफ्टवेअर्सच्या सुमारे १०० सीडीज व्हायरस स्कॅन केल्या. त्यांना आढळून आले की त्यातल्या २३ सीडीजमध्ये व्हायरस होते. आजकाल व्हायरस पसरण्याचे प्रमाण 'ई मेल' मध्ये सर्वाधिक म्हणजे ८५ टक्के असते हे खरे आहे. परंतु आजही फ्लॉपीज व सीडीजमधून व्हायरसचा धोका थांबलेला नाही. फ्लॉपी स्कॅन करण्यासाठी आजच्या वेगवान अँटी व्हायरस प्रोग्राम्सना फक्त काही सेकंदच लागतात पण त्यामुळे पुढचे अनेक तासांचे मनस्ताप टळतात. तर मग ही दक्षता का घेऊ नये?

नियम सहावा

सॉफ्टवेअर डाऊनलोड करताय? सीडीतून इन्स्टॉल करताय? सावधान!

असं नेहमी सांगितलं जातं की पायरेटेड सॉफ्टवेअर्समधून व्हायरसेस पसरतात. त्यामुळे पायरेटेड सॉफ्टवेअर्सपासून व्हायरसचा खरा धोका आहे. तसा धोका सुप्रसिध्द कंपन्यांच्या अधिकृत सीडीज किंवा त्यांच्या अधिकृत साईटवरुन डाऊनलोड करुन घेतलेल्या सॉफ्टवेअर्समध्ये नसतो. पण सत्य परिस्थिती ही आहे की पायरेटेड सॉफ्टवेअर्स सीडीज असोत की डाऊनलोडस्, त्यामधून व्हायरसेसचा जेवढा धोका असतो तेवढाच धोका ख्यातनाम कंपन्यांच्या सीडीज वा डाऊनलोडस्मध्ये असू शकतो. त्यामुळे सॉफ्टवेअर इन्स्टॉल करण्यापूर्वी सर्व सोर्स फाईल्स व एकूणच सॉफ्टवेअर व्हायरस स्कॅन करुन घ्या. व्हायरस स्कॅनसाठी दिलेला वेळ हा कधीही निरर्थक समजू नका. ती प्रक्रिया एक आवश्यक प्रक्रिया आहे. एखाद्या अनोळखी बाटलीतलं रंगीत पाणी कसलीही चौकशी न करता तुम्ही प्याल काय? नक्कीच नाही! कारण ते पाणी काहीही असू शकेल. अगदी विषसुध्दा!! म्हणूनच आपण नीट तपासल्याशिवाय ते घशाखाली ओतणार नाही. सॉफ्टवेअर्सही अशीच त्या अनोळखी रंगीत पाण्यासारखी तपासून म्हणजे स्कॅन करुन घ्या. एकच उदाहरण सांगतो. ते 'मॉयक्रोसॉफ्ट' बद्दलचे आहे. म्हणजेच पुरेसे आहे. 'मायक्रोसॉफ्ट'च्या साईटवरील एका फाईलमध्ये कित्येक आठवडेपर्यंत 'कन्सेप्ट' नावाचा मॅक्रो व्हायरस होता. नंतर ही केस खूप गाजली. सांगायचे तात्पर्य एवढेच की प्रसिध्द कंपनी आहे म्हणून डोळे झाकून व्यवहार नको. डोळे उघडे ठेवूनच काम करा.

सॉफ्टवेअर्सच्या संदर्भातील आणखी एक गोष्ट म्हणजे जेव्हा तुमचा काँप्युटर मेंटेनन्ससाठी किंवा रिपेरींगसाठी वर्कशॉपमध्ये पाठवला जातो तेव्हा कित्येकदा तिथून तो व्हायरस घेऊन येतो. कारण तेथील तंत्रज्ञ एकच सीडी व फ्लॉपी विविध काँप्युटर्ससाठी वापरत असतात. त्यामुळे एका काँप्युटरमधून दुसऱ्यात व्हायरस शिरण्यास वेळ लागत नाही. म्हणूनच रिपेअर होऊन आल्यानंतर तुमचा काँप्युटर व्यवस्थित स्कॅन करुन घ्या.

नियम सातवा

अँटी -व्हायरस प्रोग्राममधील उपलब्ध तंत्रांचा पूर्ण वापर करा!

अनेकांचा असा समज असतो की 'अँटी-व्हायरस प्रोग्राम' म्हणजे व्हायरस स्कॅनर. सामान्यत: केवळ व्हायरस स्कॅनर असेल तर तो आपण सांगू तेव्हा व्हायरस स्कॅन करेल, किंवा शेडयुलींग केलेले असेल तर त्या वेळापत्रकानुसार व्हायरस स्कॅन करेल. परंतु मधल्या वेळात तो 'व्हायरस' प्रतिबंधक संरक्षण देणार नाही. आजकालचे प्रसिध्द अँटी व्हायरस प्रोग्राम्स स्कॅनिंग च्या बरोबरीने अन्यही संपूर्ण संरक्षण देतात. त्यात एक कायम काम करणारा अँटी-व्हायरस मॉनिटर असतो. हा मॉनिटर तुम्ही जरी बेसावध असलात तरी सतत जागरुक असतो. उदाहरणार्थ समजा तुम्ही बूट व्हायरसवाली फ्लॉपी आत टाकलीत तर पुढल्या क्षणी तो संदेश देतो की त्यात व्हायरस आहे. समजा तुम्ही एखादी डाऊनलोड केलेली फाईल उघडत असाल आणि त्यात व्हायरस असेल तर तत्क्षणी तो तशी सूचना देईल. याला 'रिअल टाईम' प्रोटेक्शन म्हणतात. असे मॉनिटर्स हे मेमरी रेसिडेन्ट प्रोग्राम्स असतात. तुमच्या काँप्युटरच्या तळाशी उजवीकडे जेथे सिस्टम ट्रे म्हणजे डे डेटचे व स्पीकरचे आयकॉन असतात तेथेच बाजूला हा मॉनिटर आपला आयकॉन ठेवून तुमच्या संगणकाचे संरक्षण करीत असतो. तो कारणाशिवाय कधीही डिसेबल (अकार्यशील) करु नका.

मेमरी रेसिडेन्ट अँटी -व्हायरस मॉनिटरच्या बरोबरीने दुसरा एक साक्षीदारही अँटी-व्हायरस प्रोग्रामबरोबर येतो. त्याचे नाव 'इंटेग्रीटी चेकर' तो तुमच्या फाईल्स व फोल्डर्स (डिरेक्टरीज) तसेच डीस्क सेक्टर्सवर लक्ष ठेवीत असतो. विनाकारण एखाद्या फाईलची साईज बदलली असेल वा अन्य काही अनाकलनीय बदल त्याला आढळले तर त्याची सूचना तो देत असतो. त्यात काही व्हायरस आहे की काय हे तुम्ही तपासावे असे त्याचे सांगणे असते.

तिसरा प्रकार असतो 'बिहेवीयरल गार्ड.' हा अज्ञात व नव्या व्हायरसचा शोध त्यांच्या कोडवरून नव्हे तर त्यांच्या कृतीतील क्रम तपासून घेत असतो. म्हणजे तुम्ही 'लाईव्ह अपडेट' केल्यानंतर आलेला नवा व अज्ञात व्हायरसही तुम्ही ह्या तंत्राने ओळखू शकता.

ह्या सर्व तंत्रांचा एकत्रित उपयोग करुन अँटी-व्हायरस प्रोग्राम वापरला तर 'व्हायरस'चा हल्ला तुमच्या संगणकातील डेटापर्यंत पोहोचणे अशक्यप्रायच आहे.

नियम आठवा

तुमचा काँप्युटर सुरु करु शकणारी एक अशी स्टार्ट अप डिस्क करुन ठेवा की जी १०० टक्के व्हायरसविरहित (क्लीन) आहे. अशी डिस्क वेगळी आणि सुरक्षित ठेवा.

काही वेळा व्हायरस लागलेला काँप्युटर चालू होऊ शकत नाही. त्याचा अर्थ असा नसतो की व्हायरसने त्यातील फाईल्स डिलीट केल्या आहेत. फक्त इतकेच असते की तुमची ऑपरेटींग सिस्टम (म्हणजे विंडोज सारखा प्रोग्राम) सुरु होऊ शकत नाही. अशा वेळी तुमची क्लीन स्टार्ट अप डिस्क कामाला येईल. ती वापरताना तिचे 'राईट प्रोटेक्शन' लावलेले आहे ना हे प्रथम पहा. कारण 'राईट प्रोटेक्शन' नसेल तर व्हायरस तुमची स्टार्ट अप डिस्कही व्हायरसमय करुन टाकेल. 'राईट प्रोटेक्शन' म्हणजे त्या डिस्कवर नवी फाईल कॉपी होणार नाही. मात्र ती फ्लॉपी काँप्युटर 'रीड' करु शकेल, व त्याने काँप्युटर चालू होऊ शकेल. अशा प्रकारे 'क्लीन बूट' करून म्हणजे क्लीन फ्लॉपीने काँप्युटर चालू करून नंतर व्हायरस रिपेअर करता येतो.

आजकाल 'नॉर्टन'सारखे आधुनिक अँटी-व्हायरस प्रोग्राम्स सुधारित अशा 'रेस्क्यू डिस्क्स्' तयार करायला सांगतात. त्या 'रेस्क्यू डिस्कस' अत्यंत उपयुक्त असतात. 'नॉर्टन'चा अँटी-व्हायरस प्रोग्रामही ह्या डिस्कवर असतो, तसेच तो वेळोवेळी 'लाईव्ह अपडेट' मधून अद्ययावतही राखला जातो. तुमच्याकडे जर 'झीप ड्राईव्ह' असेल (त्यांत १०० एम.बी किंवा २५० एम. बी. अशा मोठ्या आकाराची फ्लॉपी वापरली जाते. आपली नेहमीची फ्लॉपी १.४४ एम.बी.ची असते हे तुम्हाला माहितच आहे. 'आयोमेगा' कंपनाचे 'झीप ड्राईव्हज' विशेष प्रसिध्द आहेत.) तर अशा 'झीप ड्राईव्हज' वर तयार केलेल्या व वेळोवेळी अपडेट केलेल्या 'रेस्क्यू डिस्कस्' तुम्हाला व्हायरसच्या विरोधात खूपच चिंतामुक्त करीत असतात. छोट्या फ्लॉपीज (१.४४ एम.बी.च्या) वापरल्या तर रेस्क्यू डिस्क'च्या सेटसाठी सामान्यतः ५ ते ७ फ्लॉपीज लागतात. पण जर त्यातली

एखादी फ्लॉपी अचानक बिघडली की पंचाईत होते. त्यामुळे त्याचे दोन सेट ठेवणे उपकारक असते. हे थोडे वेळखाऊ काम असले तरी निरर्थक नाही. त्याचा उपयोग केव्हा होईल सांगता येणार नाही. जेव्हा त्यांचा उपयोग होईल तेव्हाच त्यांचे खरे मोल तुम्हाला कळेल.

नियम नववा

तुमच्या कॉंप्युटरमधील 'डेटा' चा 'बॅक अप' नियमितपणे ठेवा

ह्या नियमाने 'व्हायरस' ला प्रतिबंध होणार नाही, पण तो 'संकटसमयी बाहेर येण्याचा मार्ग' आहे एवढं नक्की. समजा खूप काळजी घेऊनही एखादा व्हायरस घुसलाच. तर काय? समजा त्यामुळे तुमचा सगळा डेटा डिलीट झाला, किंवा करप्ट होऊन गेला तर काय? तुमची हार्ड डिस्क पूर्ण फॉरमॅट करावी लागली तर काय करणार? अशा वेळी तुमच्या हातात तुमच्या डेटाची दुसरी प्रत असेल तर तुम्ही हंसतमुखाने संकटाला सामोरे जाऊ शकाल. समजा तुम्ही एक छान कविता केलीत किंवा कथा लिहिलीत. ती वर्तमानपत्राला पोस्टाने पाठवलीत, आणि ती नंतर गहाळ झाली तर? तिची दुसरी प्रत तुमच्याकडे असेल तर तुम्हाला काहीच मनस्ताप होणार नाही. पण दुसरी प्रत नसेल तर! तशीच्या तशी कविता /कथा तुमच्या लेखणीतून पुन्हा उतरणं अवघडच. 'बॅक अप' चं महत्व हेच आहे. त्यात फाजील आत्मविश्वास आणू नका. काळजी घेत जा. नियमित 'बॅक अप' करीत जा. बरेच जण 'बॅक अप'चे दोन किंवा तीन तीन सेट ठेवतात. प्रकरण वेळखाऊ असलं तरी उपयुक्तच आहे. आजकाल बँकांचे सर्व व्यवहार कॉंप्युटर्सवरुन होतात. त्यामुळे बँका तीन तीन 'बॅक अप'सेट ठेवतात. त्यांनी 'बॅक अप' ठेवायला टाळाटाळ केली आणि त्यांच्या कॉंप्युटरमधला डेटा डिलीट झाला तर? कल्पना करा काय गोंधळ माजेल! 'बॅक अप' चे महत्व हे असे आहे. डेटा उडणे वा गहाळ होणे हे केवळ व्हायरसमुळेच होईल असे नाही. आग, चोरी, बिघाड अशा परिस्थितीतही 'बॅक अप' चा सहारा म्हणजे खराखुरा 'भगवान का सहारा' समजायला हवा. आजकाल साध्या फ्लॉपींव्यतिरिक्त मॅग्नेटीक टेप्स, सीडीज, झीप ड्राईव्हज इत्यादिंवर 'बॅक अप' घेतला जातो हे तुम्हाला माहितच आहे.

नियम दहावा.

कधीही गोंधळून जाऊन गडबडीत कृती करु नका.

लक्षात घ्या, की सारे काही आहे. अँटी व्हायरसही आहे, 'बॅकअप' ही आहे. सगळं आहे. पण तरीही काँप्युटरला व्हायरस लागलाय. किंवा अँटी-व्हायरसही नाही. 'बॅक अप' ही ठेवलेला नाही, आणि 'व्हायरस' लागलाय. डेटा डिलीट होण्याचा खूप दाट संभव आहे. सगळं संपल्यासारखं वाटतय. आभाळ कोसळल्यासारखं वाटतय. पण तशाही परिस्थितीत कधीही गोंधळून जाऊ नका. आपण फक्त म्हणतो 'आभाळ कोसळलं' पण ते कधीही कोसळत नसतं हे लक्षात घ्या. शांत रहा. गोंधळून जाऊन काहीतरी उलटच करुन ठेवाल, आणि सुखरुप सुटका करुन घेता आली असती तिथे उगाचच फांदा करुन ठेवाल.

शेवटी 'व्हायरस' हा एक प्रोग्राम आहे. त्यांच्यावरही अनेक उपचार आहेतच. तुम्हाला त्याची माहिती नसेल तर माहितगाराला बोलवून घ्या. मुख्य म्हणजे हा माहीतगार तुमचं काम फुकट किंवा चहाच्या एका कपावर करेल अशी अपेक्षा बाळगू नका. त्याचा मेहनताना विचारून घ्या. निश्चित करुन घ्या. कारण फुकटची अपेक्षा कराल तर तो त्याचे काम नीट करणार नाही. त्यात नुकसान तुमचेच आहे. असे हे दहा नियम. हे कानमंत्र पुन्हा पुन्हा वाचा आणि मनोमन ठसवा. संगणकाच्या दुनियेत हे कानमंत्र आत्मसात करणारी व्यक्ती कपाळावर हात मारुन हतबल झालीय असं तुम्हाला कधी दिसणार नाही. अगदी आरशात सुध्दा.

'व्हायरस'चा मनोरंजक इतिहास

१९७७ साल. मुंबईत आज जो वन रुम कीचन फ्लॅट १० लाखांना विकला जातो, तो १९७७ साली जेम तेम ८०,००० रुपयांना मिळत होता. ह्याच १९७७ साली एप्रिल महिन्यात 'ॲपल' कंपनीने 'ॲपल-टू' हा पर्सनल काँप्युटर (पी.सी) प्रथमच बाजारात आणला. तेव्हा त्याची किंमत होती १३०० अमेरिकन डॉलर्स, म्हणजेच अदमासे ६०,००० रुपये. लोकांना त्या काळात ८०,००० चे घर घेण्याची ऐपत नसे, तर ते ६०,००० रुपयांचा 'ॲपल टू' काय घेणार? त्यामुळे भारतात १९७७ साली पर्सनल काँप्युटरचा प्रसार नगण्य होता म्हणा किंवा जवळजवळ नव्हताच. अमेरिकेत त्याचा प्रचार हळूहळू होत चालला होता, पण त्यात प्रचंड झपाटा नव्हता.

१९८१ साली आय.बी.एम. कंपनीने आज तुमच्या आमच्या घरात दिसणाऱ्या पी.सी.चा अवतार प्रथमच जगापुढे आणला. पण एवूणच सामान्य माणूस त्यापासून बराच दूर होता. मोठ्या अवजड उद्योगांमध्ये काँप्युटर आणले तर माणसे बेकार होतील, आणि म्हणून काँप्युटरला विरोध करायचा असे वारे तेव्हा वहात असत. कामगार संघटना तर काँप्युटरला आपला शत्रूच मानत.

पण जसजशी वर्षे मागे पडत गेली तसतसा काँप्युटरचा उपयोग चर्चेत येऊ लागला. १९८२ सालची ही घडलेली गोष्ट पहा:

रिचर्ड स्क्रेंटा, वय वर्षे चौदा. इयत्ता ९ वी मध्ये शाळेत शिक्षण चालू. कुठेही यंत्र दिसलं की रिचर्डच्या मेंदूला किडा चावे. रेडिओ उघड,

टेलिफोन उघड. वायरिंग फिरव असे रिचर्डचे उपद्व्याप चालत. अशा ह्या आधीच 'मर्कट' असलेल्या रिचर्डला १९८२ च्या ख्रिसमसमध्ये वडिलांनी 'अॅपल टू' हा कॉंप्युटर घेऊन दिला. त्याच्या काही मित्रांकडे पूर्वीच असे कॉंप्युटर्स आलेले होते. हे मित्र आपल्या शाळेतून 'गेम्स' कॉपी करुन आणत आणि घरी खेळत. रिचर्डने आता आपले उद्योग रेडिओ आणि टेलिफोनवरुन हलवून कॉंप्युटरवर 'सेट' केले. मित्र जे गेम्स शाळेतून कॉपी करुन आणून घरी खेळत ते काही वेळाने अचानक बंद पडतील आणि त्या जागी रिचर्ड स्क्रेंटाचे वात्रट संदेश दिसतील अशी भंकस रिचर्डने सुरु केली. ह्या प्रकारामुळे रिचर्डचे मित्र हादरले. ते त्याला आपल्या कॉंप्युटरजवळ फिरकू देईनात. इथे रिचर्डलाही गप्प बसवेना. आता त्याने एक छोटा प्रोग्राम तयार केला. तो शाळेच्या कॉंप्युटरच्या ऑपरेटींग सिस्टममध्ये टाकला. ज्या ज्या वेळी त्याचे मित्र आपली फ्लॉपी घेऊन गेम कॉपी करायला येतील तेव्हा त्याचा तो छोटा वात्रट प्रोग्राम गेमबरोबर आपोआप आत शिरेल अशी व्यवस्था रिचर्डमहाशयांनी करुन ठेवली. पुढे त्याच फ्लॉपीतून आणखी तिसऱ्या-चौथ्या कॉंप्युटरवरही हा प्रोग्राम पोहोचावा असे प्रयत्न रिचर्डने सुरु केले. आपण हा व्हायरस लिहितोय याची कल्पना त्यावेळी रिचर्डलाच काय पण जगात कोणालाच

हाच तो रिचर्ड स्क्रेंटा

नव्हती. कारण अशा प्रोग्राम्सना त्यावेळी 'व्हायरस' हे नाव अद्यापि दिले गेले नव्हते. रिचर्डने बनविलेला तो 'Elk Cloner' व्हायरस होता.

पण रिचर्डच्या ह्या भंकसबाजीचा प्रचार ॲपल काँप्युटरवर फारसा झाला नाही. एवूणच 'ॲपल' काँप्युटर आणि आय.बी.एम. चे पीसी यांमध्ये व्हायरसचा खरा धुमधडाका सुरु झाला तो आय.बी.एम.च्याच काँप्युटर्समध्ये. पण तरीही १९८६ सालापर्यंत लोकांना 'व्हायरस' ही नेमकी काय चीज आहे हे माहितीच नव्हतं. याचं कारण आय.बी.एम. पीसीवरचा पहिला व्हायरस तयार झाला तो जानेवारी १९८६ मध्ये. तुम्हाला कदाचित माहितही नसेल पण हा पहिला व्हायरस तयार झाला तो पाकिस्तानात लाहोरमध्ये. हा व्हायरस तयार करणारे दोन भाऊ - बसीत फरुक अल्वी आणि अमजद फरुक अल्वी यांचं एक दुकान लाहोरमध्ये होतं. ते काँप्युटरचे भाग आणि पायरेटेड सॉफ्टवेअर विकत असत. त्यांच्या दुकानाचे नाव होते Brain Computer Services. त्यांच्या ह्या दुकानाच्या नावामुळे त्यांनी तयार केलेल्या व्हायरसला त्यांनीच 'ब्रेन' हे नाव दिले. आय.बी.एम. पीसीवरचा जगातला हा पहिला व्हायरस ३६० के.बी. आकाराच्या फ्लॉपीवर तयार केला गेला.

तसा हा व्हायरस निरुपद्रवी होता. तो हार्ड डिस्कचे नुकसान अजिबात करीत नसे. फ्लॉपीच्या बूट सेक्टरमध्ये त्याची स्थापना करुन तो पसरविण्याचा घाट बसीत-अमजद बंधूंनी घातला होता. 'फ्लॉपी'चा बूट सेक्टर काँप्युटर स्वतःच आपोआप कार्यरत करीत असतो, आणि त्यासाठी फ्लॉपीच्या बूट सेक्टरमध्ये एक प्रोग्राम अस्तित्वात असतो ह्या एवढ्याच तत्वावर 'ब्रेन' व्हायरसची कार्यपध्दती आधारलेली होती. हा व्हायरस फ्लॉपीच्या INT 13 ह्या भागात लपून बसे. एखाद्या माहितगाराने जर 'व्हायरस' चा फ्लॉपीतला भाग वाचण्यासाठी बूट सेक्टर पाहिला तर त्याला केवळ ओरिजिनल बूट सेक्टरच दिसेल अशी व्यवस्था बसीत-अमजद यांच्या सुपीक 'ब्रेन' मधून निघालेली होती. थोडक्यात, शोधूनही सापडणार नाही अशा प्रकारचा म्हणजे 'Stealth' ह्या प्रकारातला हा पहिला व्हायरस होता.

ब्रेन व्हायरस हा व्हॉल्युम लेबल बदलून ते '(C) Brain' असे करीत असे. '(C)' हा प्रकार बहुधा कॉपीराईटसाठी होता, आणि ब्रेन हे दुकानाचे नाव होते. ह्या व्हायरसमध्ये खालील संदेश होता:

Welcome to the Dungeon

(C) 1986 Basit & Amjad (Pvt.) Ltd.
Brain Computer Services
730 Nizab Block Allama Iqbal town
Lahore - Pakistan
Phone: 430791, 443248, 280530
Beware of this Virus
Contact us for Vaccination..... $#@%$@!!

काहींच्या मते बसीत व अमजद यांनी हा व्हायरस तयार करण्यामागे त्यांचे व्यावसायिक कारण होते. पाकिस्तानात पायरेटेड सॉफ्टवेअर विकणे हा गुन्हा मानला जात नाही. आपण विकलेले सॉफ्टवेअर इतर कोणाला पुन्हा कॉपी करुन विकता येऊ नये असा प्रयत्न 'ब्रेन' व्हायरस मागे असावा असे हे मत आहे. पण पुढे 'ब्रेन' व्हायरस अमेरिकेतही पसरला.

१९८६ च्या इतर घटनाही आपण लक्षात घेऊ या. ह्या घटना जागतिक आहेत. त्यांचा व्हायरसशी काहीही संबंध नाही. पण ह्या घटनांचीच नावे नंतर 'व्हायरस' ना दिली गेली आहेत. उदाहरणार्थ १९८६ साली 'हॅलेचा धुमकेतू' जगावरून गेला. रशियात चैर्नोबिल अणू भट्टीत मोठा अपघात झाला. त्याच वर्षी एम.एस. 'डॉस'चे ३.२ हे व्हर्जन बाजारात आले, आणि त्यात ३.५ इंच आकाराची छोटी फ्लॉपी प्रथमच वापरता येऊ लागली.

३.५ इंच आकाराची फ्लॉपी १९८६ साली जन्माला आली.

थोडक्यात ३.५ इंच आकाराची फ्लॉपी १९८६ साली जन्माला आली. ब्रेन व्हायरस ३६० के.बी. च्या ५.२ इंच आकाराच्या फ्लॉपीवरुन पसरला हे त्यामुळे स्पष्ट आहे.

१९८६ च्या डिसेंबरात Virdem नावाचा व्हायरस आला. तो जर्मनीत

तयार केला गेला होता. हा व्हायरस फाईलला इनफेक्ट करणारा होता. Berger Virus आणि Rush Hour Virus हे आणखी दोन व्हायरसही आपला जन्म १९८६ चा असल्याचे सांगतात.

१९८७ साल

एकीकडे आय.बी.एम. पीसीचा प्रसार जोरात चालू होता. दुसरीकडे ह्या काँप्युटरसाठी नवनवी सॉफ्टवेअर्स तयार केली जात होती. मायक्रोसॉफ्टने आपल्या एम.एस.डॉसमध्ये सतत सुधारणा करण्याचा सपाटा चालवला होता. 'विंडोज' प्रोग्राम क्षितीजावर येण्याची चिन्हे दिसू लागली होती, आणि जगातल्या बुध्दीमानांची आणखी भंकसबाजी नवनव्या व्हायरसेसमधून जगापुढे येऊ लागली होती.

ऑक्टोबर १९८७ मध्ये अमेरिकेत डेलवेअर विद्यापीठात 'ब्रेन' व्हायरस अचानक मोठ्या प्रमाणावर पसरला. सुरुवातीचे सारे व्हायरस मग निरनिराळ्या विद्यापीठांतून गाजू लागले. नोव्हेंबर १९८७ मध्ये अमेरिकेतील लीहाय विद्यापीठात नवा व्हायरस आला. त्याचे नावही त्यामुळे 'लीहाय व्हायरस' असेच आहे. हा व्हायरस काँप्युटरमधील Command.com नावाच्या फाईलला लागत असे. Command.com ही फाईल काँप्युटरच्या मेमरीत असते. त्यामुळे तांत्रिक दृष्टया 'Lehigh' हा व्हायरस जगातला पहिला memory resident + file infector प्रकारचा व्हायरस आहे.

इस्त्रायलमधील हिब्रू विद्यापीठात डिसेंबर १९८७ मध्ये Jerusalem नावाचा व्हायरस आला. जेरुसलेम ही इस्त्रायलची राजधानी. त्याचेच नाव ह्या व्हायरसला दिले गेले होते. लीहाय हा जरी मेमरीतील फाईलला लागत असे, तरी तो स्वत: मात्र मेमरीत जागा करून रहात नसे. जेरुसलेम हा जगातला पहिला व्हायरस असा होता की जो मेमरीतल्या फाईल्सना लागण करीत असे, आणि वर स्वत:ही मेमरीत रहात असे. जेरुसलेम हा व्हायरस ज्याने लिहीला त्याने अशा प्रकारचे तीन व्हायरस अगोदर लिहिले होते हे जेरुसलेमचा प्रसार झाल्यानंतर लक्षात आले. अगोदरचे जे तीन व्हायरस त्याने लिहिले त्यांची नावे त्याने Suriv 1,2,3 अशी ठेवली होती. 'SURIV' म्हणजे 'VIRUS' ह्या शब्दाची उलटीकडून मांडलेली अक्षरे. .COM आणि .EXE प्रकारच्या प्रोग्राम फाईल्सना भिडून लागण

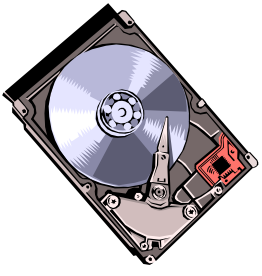
करणारा जेरुसलेम हाच जगातला पहिला व्हायरस आहे. हा व्हायरस अगोदरच लागण असलेल्या फाईललाही पुन्हा लागण करीत असे. हा जेरुसलेममधील एक दोष (Bug) मानला जातो. जेरुसलेम हा डिसेंबर १९८७ मध्ये प्रथमच दिसल्याने तो पसरेपर्यंत १९८८ साल उजाडले होते. त्यामुळे 'जेरुसलेम'चे खरे कर्तृत्व (?) हे १९८८ सालातच दिसले.

१९८७ सालचा आणखी एक भारी व्हायरस म्हणजे 'स्टोन्ड.' 'Stoned' हा पहिला 'मास्टर बूट रेकॉर्ड' (MBR) व्हायरस. न्युझीलंडमधील वेलिंग्टन विद्यापीठातील एका विद्यार्थ्याने तो तयार केला. ह्याच साली ऑस्ट्रीयातील एका शाळकरी मुलाने 'व्हिएन्ना' नावाचा व्हायरस लिहिला. 'जेरुसलेम' आणि 'व्हिएन्ना' ही दोन महत्वाचे शहरे त्यावेळी व्हायरस म्हणून गाजू लागली 'व्हिएन्ना' व्हायरसचे सविस्तर स्वरुप (Source Code) व त्याची 'disassembly (उपाय) यांची माहिती देणारे एक पुस्तकही १९८७ सालीच लगोलग प्रसिध्द झाले. ह्या पुस्तकात 'Burger' आणि 'Number One' ह्या व्हायरसेसचीही माहिती होती.

१३ तारखेच्या शुक्रवारी आलेल्या एका व्हायरसने दक्षिण अफ्रिकेत हाहा:कार माजविला. त्याने ह्या दिवशी (१३ तारीख आणि शुक्रवार) काँप्युटरमधील फाईल्स गाळायला (deletion) सुरुवात केली.

१९८८ साल

आतापर्यंत एम.एस.डॉस ३.० च्याच मालिकेत होता. १९८८ साली प्रथमच डॉसचे ४.० हे व्हर्जन अवतरले. त्यामुळे ३२ मेगॅबाईटपेक्षा मोठी

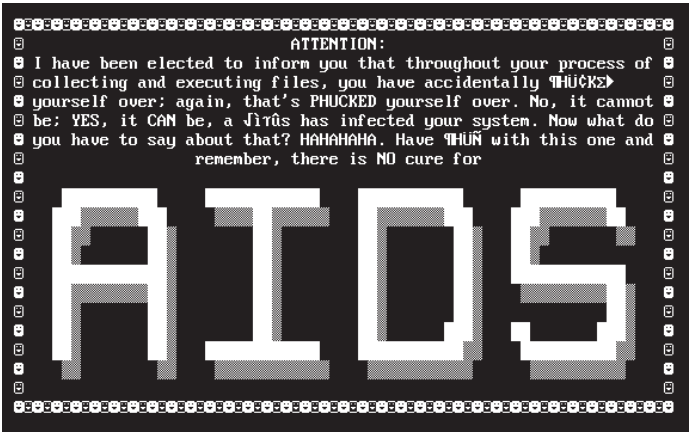


मोठी हार्ड डिस्क

हार्ड डिस्क वापरता येऊ लागली. २००१-२००२ मध्ये आपण २०

जीबीची म्हणजे २०,००० एम.बी.ची हार्ड डिस्क वापरत आहोत. पण १२ वर्षांपूर्वी फक्त ३२ एम.बी वापरता येऊ लागली याचेही अप्रुप होते हे ऐकताना अचंबा वाटतो.

१९८८ सालचे सर्वांत मोठे वैशिष्टय म्हणजे 'अँटी-व्हायरस' स्वरुपाचा व्हायरस प्रथमच पाहण्यात आला. हा व्हायरस म्हणजे 'डेन झुक' (Den Zuk) मार्च १९८८ मध्ये इंडोनेशियातील डेनी यानोर रामधनी यांनी बांडुंग येथे हा व्हायरस बनविला. हा व्हायरस 'ब्रेन' व्हायरस शोधून तो काढून टाकी. एवढेच नव्हे, तर पुन्हा त्या डिस्कला 'ब्रेन' ची बाधा होऊ नये असे तांत्रिक लसीकरणही (immunization) करी. हा व्हायरस तयार करणारे रामधनी यांचे पत्र पुढे फेब्रुवारी १९९१ मध्ये 'व्हायरस बुलेटीन' मध्ये प्रसिध्द झाले. त्यात त्यांनी Den Zuk व्हायरस आपणच बनवला होता हे कबूल केले.



एडस व्हायरसने आपले अस्तित्व अशा चित्राने दाखवले. सामान्यत: व्हायरसबरोबर आलेली चित्रे ही विकृत स्वरूपाचीच होती..

ह्याच वर्षी जर्मनीत कास्केड (Cascade) नावाचा व्हायरस तयार झाला. हा मेमरीत रहात असे, पण काहीतरी सांकेतिक चिन्हे वापरुन तो स्वत:चे स्वरुप बदलून रहात असे. त्याला तांत्रिक भाषेत Encryption असे म्हणतात. कास्केड हा पहिला 'Encrypted' प्रकारचा Virus मानला जातो.

१९८८ हे साल 'व्हायरस' साठी एवढे गाजले की जगातल्या सर्व महत्वाच्या वृत्तपत्रांनी आणि नियतकालिकांनी त्यावर लेख लिहिले. 'बीझनेस वीक' (ऑगस्ट), 'फॉर्च्युन' (डिसेंबर), 'न्युज वीक' (नोव्हेंबर), 'टाईम' (फेब्रुवारी आणि सप्टेंबर दोनदा), 'वर्किंग वुमन' (सप्टेंबर), 'बाईट', 'पीसी मॅगझीन', 'सायन्स' 'फ्युचरिस्ट' अशा अनेक जग प्रसिध्द

'अँटी व्हायरस' गुरू पीटर नॉर्टन.. सुरूवातीस त्यांनी दावा केला होता की व्हायरस नावाचा प्रकारच अस्तित्वात नाही. पण नंतर ते व्हायरसमुळेच अधिक प्रसिद्धीस आले..

नियतकालिकांनी त्यावर सविस्तर वृत्तांत लिहिले. 'पीसी वीक' ह्या संगणकविषयक मासिकाने त्यावर्षी एकूण २० लेख 'व्हायरस' ह्या विषयावर दिले ह्यावरुन हे वर्ष कसे 'व्हायरसमय' झाले होते हे तुमच्या लक्षात येईल.

अनेक अभ्यासकांनी ह्याच वर्षी 'व्हायरसेस' वरील उपायांच्या दृष्टीने संशोधन करायला सुरुवात केली होती. १९८८ सालच्या १३ तारखेला आलेल्या एका शुक्रवारी जगातील अनेक कंपन्या आणि विद्यापीठांच्या कॉंप्युटरमध्ये जेरुसलेम व्हायरस घुसला. अमेरिका, युरोप आणि मध्य पूर्वेतील देशांमधून गोंधळाच्या बातम्या येऊ लागल्या. हा गोंधळ चाललेला असतानाच जगप्रसिध्द कॉप्युटर तज्ज्ञ पीटर नॉर्टन याने एक अफलातून विधान केले. त्याने सांगितले की 'कॉप्युटर व्हायरस' नावाचा प्रकारच मूळात अस्तित्वात नाही. ह्या साऱ्या अफवा आणि दंतकथा आहेत. अर्थात ह्या विधानाच्या पुढच्याच वर्षी 'पीटर नॉर्टन' ची सिमँटेक कंपनी अँटी व्हायरस प्रोग्राम बनविण्याच्या कामाला लागली ही गोष्ट वेगळी.

ह्याच गोंधळात आणखी एका नव्या प्रकाराला ऊत आला. हा प्रकार म्हणजे व्हायरसविषयक अफवा. इंग्रजीत त्यांना 'होक्स' (Hoax) असं म्हणतात. एक अफवा अशी होती की ''जो मॉडेम २४०० बॉड रेटने चालेल त्यातून एक भयानक व्हायरस घुसणार आहे.'' कुणी 'माईक रोचेनले' (काही लोक त्याचा उच्चार माइक्रो चॅनल असा करतात) त्याच्या नावे संदेश हजारो 'बी बी एस' सिस्टम्स वापरणारांकडे पाठवला गेला. यामुळे घाबरुन जाऊन २४०० चा चांगला वेग मिळत असूनही लोक खबरदारी म्हणून १२०० च्या मंद वेगाने मॉडेम वापरु लागले. व्हायरसविषयक अफवा (Hoax) आजही पसरत असतात, आणि त्याने गोंधळ उडू नये म्हणून लोकांना सावधान करणाऱ्या स्वतंत्र वेबसाईटस्ही आज आलेल्या आहेत. त्याची माहिती आपण ह्याच पुस्तकात पुढे एका स्वतंत्र प्रकरणात घेणार आहोत.

नोव्हेंबर १९८८ मध्ये 'मॉरिस' नावाचा एक नेटवर्कवर पसरणारा व्हायरस आला. अमेरिकेतील ६००० काँप्युटर त्याच्या विळख्यात सापडले. 'नासा' चे संशोधन केंद्रही त्यातून सुटले नाही. हा व्हायरस 'इंटरनेट वॉर्म' च्या प्रकारातला होता. तो स्वत:च्या अगणित प्रती तयार करुन नेटवर्कवरील इतर काँप्युटरकडे पाठवून देई. त्यामुळे नेटवर्क ठप्प होत. ह्या 'मॉरिस' व्हायरसमुळे त्या वर्षी सुमारे ४८० कोटी रुपयांचे नुकसान झाल्याची नोंद आहे.

१९८८ साली डॉ. सॉलोमन यांचे अँटी-व्हायरस टुलकीट प्रथमच बाजारात आले. डॉ. सॉलोमन हा सर्वांत जुना अँटी-व्हायरस प्रोग्राम मानला जातो.

१९८९ साल

'वॉशिंग्टन पोस्ट' हे आपल्या 'टाईम्स ऑफ इंडिया' सारखे अमेरिकेचे प्रचंड खपाचे वृत्तपत्र त्याच्या १७ सप्टेंबर १९८९ च्या अंकात मोठ्या मथळ्याची बातमी होती:

" Computer Virus Sparks a User Scare;

Some Analysts say the 'Friday the 13th' Fears Are Overblown"

ह्या बातमीत म्हंटले होते की १३ तारखेच्या शुक्रवारी येणाऱ्या व्हायरसपासून वाचण्यासाठी संगणकधारक आटापिटा करीत आहेत. खरं तर ह्या वृत्तात दोन वेगवेगळ्या व्हायरसचा उल्लेख असायला हवा होता. पहिला म्हणजे 'डाटाक्राईम' व्हायरस. हा १२ ऑक्टोबर नंतर (केव्हाही) येणार होता. तर, दुसरा व्हायरस म्हणजे 'जेरुसलेम' तो १३ तारखेच्या शुक्रवारी येणारा होता. योगायोगाने १३ ऑक्टोबर १९८९ रोजी शुक्रवारच होता. आणि त्यातच वृत्तपत्रांचे मोठमोठे मथळे आल्याने लोकांमध्ये प्रचंड घबराट पसरली होती.

'डाटाक्राईम' व्हायरसने १३ ऑक्टोबर ते ३१ डिसेंबर ह्या काळात हजारो हार्ड डिस्कस चक्क फॉरमॅट केल्या. याच्या बातम्या हॉलंड आणि ब्रिटनमध्ये एवढ्या गाजल्या की 'व्हायरस' हा शब्द कॉंप्युटर जगतात प्रचंड दहशतीचा शब्द बनला.

१९८९ च्या सप्टेंबर महिन्यात 'आय.बी.एम' कंपनीने आपला अँटी-व्हायरस प्रोग्राम बाजारात आणला. एकीकडे व्हायरसेसची संख्या वाढतच होती. 'फूमांचू,' 'व्हॅक्सीना', डार्क अॅव्हेंजर 'फ्रोडो','यांकी,' वगैरे व्हायरसही कुप्रसिध्दी पावतच होते.

१९८९ च्या डिसेंबर महिन्यात AIDS नावाचा एक 'ट्रोजन हॉर्स' व्हायरस जगतात प्रचंड गाजला. AIDS च्या २०,००० डिस्केटस् निर्यात करण्यांत आल्या. त्यावरील लेबलवर लिहिले होते "AIDS Information Diskelte Version 2.0" एकूण ९० वेळा ह्या डिस्केट बुट झाल्या की त्यातील ट्रोजन प्रोग्राम डिस्कवरील सर्वच्या सर्व फाईल्सची नावे बदलून ती अनाकलनीय encrypted भाषेत बदलून टाकी. कोणतीही फाईल ओळखता येत नसे. केवळ एकच फाईल वाचता येई. त्यावर लिहिलेले असे '' १८९ डॉलरचे बिल ते पोस्ट बॉक्स ७, पनामा'' ह्या पत्त्यावर पाठवावे. हा व्हायरस लिहिणाराचा शोध नंतर घेण्यांत आला व त्याला जेलची हवा खाण्यास पाठवले गेले.

१९९०, १९९१ आणि १९९२

१९९० सालची महत्वाची आंतरराष्ट्रीय घटना म्हणजे इराकची कुवेतवर स्वारी. ह्याच वर्षी 'विडोज ३.०' आणि ८०४८६ पध्दतीचा कॉंप्युटर बाजारात आला. एकीकडे ह्या राजकीय, आर्थिक आणि सामाजिक घडामोडी

होत होत्या आणि दुसरीकडे व्हायरस जगतातही प्रचंड उलाढाली चालल्या होत्या.

आय.बी.एम., डॉ सॉलोमनसारखे अँटी-व्हायरस प्रोग्राम्स बाजारात होते. लोक त्यांचा वापरही करु लागले होते. यामुळे आता 'व्हायरस' तयार करणारे विरुध्द अँटी-व्हायरस प्रोग्राम्स अशी लढाई सुरु झाली होती. 'व्हायरस' चे नवनवे असे प्रकार निघू लागले होते की जे अँटी-व्हायरस प्रोग्रामलाही ओळखता येणार नाहीत.

'बल्गेरिया' हा असा देश आहे की जिथे 'व्हायरस' तयार करणे हा गुन्हा मानला जात नाही. त्यामुळे बल्गेरियात 'व्हायरस'ला प्रचंड प्रोत्साहन मिळाले. तेथे एक 'बुलेटीन बोर्ड सर्व्हिस' (बी बी एस) 'व्हायरस'साठी सुरु झाली. ही सर्व्हिस तयार व्हायरस लोकांना देत असे. पण त्यासाठी अट अशी होती की निदान एक तरी नवा व्हायरस त्यांनी सर्व्हिसला दिला पाहिजे. त्यामुळे लोक छोटे-मोठे व्हायरस तयार करुन देऊ लागले. ह्या प्रकारामुळे बल्गेरिया म्हणजे 'व्हायरस'ची एक मोठी फॅक्टरीच बनली.

'अँटी-व्हायरस' ला नमविण्यासाठी जे वेगवेगळ्या प्रकारचे व्हायरस लिहिले जाऊ लागले त्यात १९९० साली प्रथमच 'पॉलिमॉर्फिक' ह्या प्रकारातील व्हायरस पहायला मिळाला. 'पॉलिमॉर्फिक' व्हायरस हा गुप्त सांकेतिक (encrypted) भाषेत असतो, आणि ही भाषा उलगडून पहायच्या (decryption) पध्दती सतत बदलत्या राहतात. त्यामुळे Polymorphic Viruses वर उपाय शोधणे जिकीरीचे होऊन बसते.

'व्हायरस' चा दुसरा नवा प्रकार आला तो 'आर्मरींग'चा. 'आर्मरींग' मध्ये अँटी -व्हायरस प्रोग्राम हा व्हायरस मारुच शकणार नाही अशी व्यवस्था केलली असते.

आत्तापर्यंत जे व्हायरसेस आलेले होते ते 'बूट' प्रकारचे म्हणजे 'बूट रेकॉर्ड' मध्ये राहणारे किंवा 'प्रोग्राम्स' (.Com किंवा exe फाईल) ना बाधा करणारे असत. पण १९९० पासून 'मल्टीपार्टाईट' व्हायरस आले. 'मल्टीपार्टाइट' म्हणजे असे व्हायरस की जे 'बूट' सेक्टरलाही लागतात आणि 'प्रोग्राम्स' नाही बाधा आणतात.

ह्याखेरीज स्वत:च्या आगमनामुळे वाढलेली फाईल साईज लपविणे,

आपले कोड लपविणे अशा प्रकारचे 'स्टील्थ' व्हायरसेस तर १९८६ सालापासूनच प्रचलित होते हे आपण पूर्वी पाहिलेच आहे. 'ब्रेन' हा 'स्टील्थ' व्हायरसच होता.

१९९० साली गाजलेले व्हायरस म्हणजे 'पल्लीप' व्हायरस. हा 'मल्टीपार्टाइट'तर होताच, पण 'पॉलीमॉर्फिक' ही होता. थोडक्यात, 'अँटी-व्हायरस' बनविणारांपेक्षा चार पावले पुढे राहून 'व्हायरस' तयार करत राहणे असे प्रकार जोमाने चालले होते.

१९९० च्या डिसेंबरमध्ये जे महत्वाचे अँटी-व्हायरस' प्रोग्राम्स उपलब्ध होते त्यांची यादी पहा:

१. डॉ. सॉलोमन

२. एफ. प्रॉट

३. थंडरबाईट

४. 'सोफोस'चे व्हॅक्सीन

५. 'आय.बी.एम' चे 'व्हिरुस्कॅन'

६. 'मॅक फी' चे 'व्हिरुस्कॅन'

७. 'आयरीस' चे 'अँटी व्हायरस प्लस'

आणि असेच आणखी डझनभर अँटी व्हायरस प्रोग्राम्स आता उपलब्ध झाले होते. मात्र १९९० अखेरीपर्यंत 'नॉर्टन अँटी-व्हायरस प्रोग्राम' बाजारात आलेला नव्हता. त्याची फक्त चर्चा सुरु झाली होती.

१९९१ साली इराक - अमेरिका युध्दाचा काळ होता. 'मायक्रोसॉफ्ट'ने 'डॉस ५.०' ह्याच वर्षी बाजारात आणला. 'इंटेल' ने कमी खर्चाचे ८०४८६ S हे कॉंप्युटर बाजारात आणले.

मार्च १९९१ मध्ये 'व्ही.सी.एस १.०' हा भयानक प्रोग्राम प्रथमच दिसला. व्ही.सी.एस. म्हणजे 'व्हायरस कंन्स्ट्रक्शन सेट.' थोडक्यात, व्हायरस तयार करण्याचा प्रोग्राम. ह्या प्रोग्रामनंतर असेच आणखी काही सेटस् आणि कीटस बनविले गेले. 'नोव्हेअर मॅन' संघटनेचे 'व्ही.सी.एल' म्हणजे 'व्हायरस कंस्ट्रक्शन लॅब' हा प्रोग्रामरी याच काळात आला. यात

केवळ माऊसने क्लीक करुन नवनवे व्हायरस तयार करता येत होते. यानंतर Phalcon/Skism's यांचे Ps-MPC म्हणजे Phalcon/Skism's Mass Production & Construction of Viruses हा प्रोग्राम आला. त्यामुळे ह्या वर्षी तुम्हाला शेकडो व्हायरसेस असे दिसतील की ज्यांच्या नावात VCL किंवा PS-MPC आहे.

१९९१ साल गाजविणारे व्हायरस म्हणजे Tequila, Spam, Dir II वगैरे. रोज बनणारे शेकडो व्हायरस, मिळणारी अफाट प्रसिध्दी, उडालेला गोंधळ यामुळे 'अँटी-व्हायरस' हे क्षेत्र म्हणजे पैसा कमाविण्याचे क्षेत्र बनले. त्यात 'सिमँटेक' ह्या बलाढ्य कंपनीने आपला Norton Anti Virus बाजारात आणला. अनेक छोट्या छोट्या अँटी-व्हायरस कंपन्या चक्क विकत घेऊन आपली मक्तेदारी निर्माण करायला सुरुवात केली. १९९२-९३ आणि ९४ मध्ये 'सिमँटेक' ने Certus, Fifth Generation, Central Point अशा कंपन्याही विकत घेतल्या.

आता १९९२ चे वर्ष उजाडले. ह्या वर्षातील 'संगणक जगता'तील सर्वांत मोठी घटना म्हणजे 'विडोज ३.०' ची सुधारित आवृत्ती 'Windows 3.1' बाजारात आली. पूर्वीच्या ३.० मधील अनेक दोष ३.१ ने दूर केले होते. लोक आता Dos 5.0 बरोबर 'Windows 3.1' मध्ये गुंतू लागले होते. ह्याच वर्षी अनेक वैशिष्टयपूर्ण आणि नाविन्यपूर्ण व्हायरस निर्माणही झाले. त्यातही काही असे:

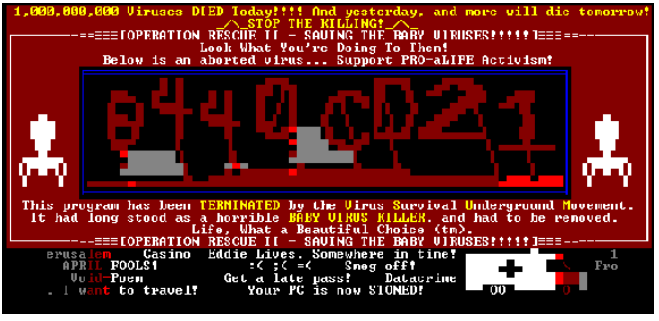
- 'ExeBug' हा व्हायरस CMOS चे कोड बदलून Clean Booting ला प्रतिबंध करु लागला.

– 'Invol' हा 'sys' प्रकारच्या फाईलला लागणारा पहिला व्हायरस आला.

– 'Win Ver 1.4' हा पहिला विंडोज व्हायरस ह्याच काळात आला.

पण हे वर्ष हादरवून टाकले ते 'Michelangelo' ह्या व्हायरसने. सुमारे ५० लाख काँप्युटर्स ह्या व्हायरसने बंद पाडले.

'व्हायरसेस'चे हे लोण पुढे असेच चालणार आणि मग चांगला 'धंदा' होणार अशा आशेने अनेक नव्या 'अँटी व्हायरस प्रॉडक्ट' कंपन्या ह्या वर्षी



मध्यंतरी येऊन गेलेल्या रेस्क्यु व्हायरसने लागल्यानंतर अशा विचित्र चित्राने आपले अस्तित्व दाखविले. सामान्यत: व्हायरसचे लेखक काहीही इमेज टाकत नाहीत, पण काहींनी ती व्हायरसला जोडली होती..

निघाल्या. पण १९९३ सालापासून 'व्हायरसेस' च्या क्षेत्रात काहीसा दुष्काळ दिसू लागला. मग ह्या 'हौशा, नवशा आणि गवशा' कंपन्याही आपोआप बंद पडल्या.

१९९३ आणि १९९४

१९९३ मध्ये 'मायक्रोसॉफ्ट' ने डॉस ६.० बाजारात आणला. ह्या 'डॉस' आवृत्तीबरोबर मायक्रोसॉफ्टने स्वत:चा अँटी व्हायरस प्रोग्रामही दिला होता. हाच प्रकार आय.बी.एम. नेही केला. आपल्या पीसी-डॉस ६.१ बरोबर त्यांनीही अँटी-व्हायरस दिला. १९९३ मध्ये आलेले महत्वाचे व्हायरसेस म्हणजे Tremor, Satan Bug, Monkey, Strange, Cruncher वगैरे.

१९९४ मध्ये 'मायक्रोसॉफ्ट' ने आपली शेवटची डॉस आवृत्ती ६.२२ बाजारात आणली. ह्या वर्षी आलेला 'Kaos4' हा व्हायरस साधी ' txt ' फाईल म्हणून 'Encode'' केलेला असे. पण नंतर तो executable Programme म्हणून decode होई आणि नंतर व्हायरस बनून पसरे. इतर आलेल्या व्हायरसेसमध्ये chill, Junkie, Pathogen, One_Half आणि Natas हे महत्वाचे म्हणता येतील.

१९९५, क्रांतीकारी वर्ष

१९९५ साली 'विंडोज-९५' ची प्रतिक्षा होती. त्याचे पूर्वीचे नाव 'शिकागो'

असे होते. 'विंडोज-९५' हे बारसे नंतर झाले. ह्या नव्या विंडोज आपॅरेटींग सिस्टमचा परिणाम अँटी व्हायरस प्रोग्राम्सवर कसा होईल याची चर्चा आणि चिंता दोन्ही चालू होत्या. त्यावेळचे बहुतेक व्हायरसेस हे बूट व्हायरसेस होते. 'विंडोज-९५' ने 'डॉस' हद्दपार केल्यानंतर बूट व्हायरसेस पसरु शकणार नाहीत हे स्पष्टच होते. त्यामुळे जे जे अँटी व्हायरस प्रोग्राम्स 'डॉस' वर आधारलेले होते त्यांचा मृत्यू आता अटळ होता. पण ऑगस्ट १९९५ मध्ये एक नवाच प्रकार दिसून आला. तो म्हणजे 'कन्सेप्ट' (Concept) व्हायरस. 'कॅन्सेप्ट' हा पहिला 'मॅक्रो' आहे. तो 'WordBASIC' ह्या भाषेत लिहिला गेला. मात्र तो केवळ इंग्रजी भाषेसाठीच होता. 'मॅक' वा 'पीसी' अशा दोन्ही प्रकारच्या काँप्युटर्सवर इंग्रजी भाषेत 'वर्ड' प्रोग्राममध्ये जर तो आला तरच तो कार्यान्वित होत असे. ह्या नव्या 'व्हायरस'चे डिटेक्शन कसे करावे याचा विचार एकीकडे 'अँटी व्हायरस' कंपन्या करीत होत्या, आणि दुसरीकडे १९९५ सालाच्या अखेरीपर्यंत अनेक नवनवे मॅक्रो व्हायरस जन्माला घातले जात होते.

मात्र आता नव्या 'विडोंज' अवतारामुळे 'व्हायरसेस'ना शिरकाव करणे खूपच अवघड झाले होते एवढे नक्की.

१९९६ मागील पानावरुन पुढे....

१९९६ मध्ये 'न्युक्लीयर', एनओपी, 'व झ्झू' वगैरे मॅक्रो व्हायरस आले. पण ते पूर्वीच्या मॅक्रोव्हायरसेस सारखेच होते. १९९६ चे वैशिष्टय हे की खास 'विडोंज-९५' साठी तयार झालेला पहिला व्हायरस 'बोझा' ह्या वर्षी जन्मला. 'अँटी व्हायरस' कंपन्यांनी त्याचा बराच गाजावाजा केला. 'हेअर' (Hare) नावाचा व्हायरसही असाच येऊन गेला. पण त्यात अनेक दोष (Bugs) असल्याने तो पसरला नाही. 'मायक्रोसॉफ्ट एक्सेल' च्या स्प्रेडशीटसना लागण लावणारा पहिला व्हायरस 'लॅरॉक्स' (Laroux) देखील १९९६ ची जन्मतारीख सांगतो.

१९९७

ह्या वर्षीच्या फेब्रुवारी महिन्यात 'लिनक्स' (Linux) ऑपरेटींग सिस्टमला लागणारा पहिला व्हायरस (Linux. Bliss) हा पहिल्यांदाच पहायला मिळाला. 'मायक्रोसॉफ्ट ऑफिस ९७' प्रोग्राम दरम्यान आला होता. त्यामुळे

मॅक्रो व्हायरसेसनी आपला मोर्चा 'ऑफीस-९७' कडे वळवला. Share-Fun हा एक तसलाच प्रकार होता.

नेटवर्कवरुन 'फाईल ट्रान्स्फर प्रोटोकोल' चा (FTP) उपयोग करुन पसरणारा पहिला व्हायरस 'होमर' (Homer) १९९७ चाच.

'mIRC' हा इंटरनेट माध्यमातून चालणारा 'चॅट' चा एक अत्यंत लोकप्रिय असा प्रोग्राम. ह्या प्रोग्राममधून शिरणारे mIRC Worms हे ह्या वर्षी प्रथमच पहायला मिळाले.

पण पुढल्याच सुधारित आवृत्तीमध्ये 'mIRC' प्रोग्रामने सुधारणा केली आणि त्यामुळे हे mIRC Worms दिसेनासे झाले.

ह्याच वर्षी Dr. Solomon आणि Mc Afee ह्या कंपन्यांमध्ये जाहिरात करण्यावरुन वादावादी झाली आणि प्रकरण कोर्टात गेले. ह्या वादात नंतर 'नॉर्टन'ची सिमँटेक कंपनीही सामील झाली. पुढे ह्याच वर्षी 'Mcafee Associates' चे रुपांतर Network Associates ह्या कंपनीत झाले.

१९९८: व्यावसायिक उलाढाली टिपेला

मे १९९८ मध्ये आय.बी.एम. कंपनीने आपला 'अँटी-व्हायरस' प्रोग्राम थांबवला आणि 'नॉर्टन अँटी-व्हायरस' चा हात हातात घेतला. दोघांमध्ये करार झाला आणि 'आय.बी.एम'च्या उत्पादनांबरोबर 'नॉर्टन'चा अँटी - व्हायरस दिला जाऊ लागला. त्यामुळे 'अँटी-व्हायरस' च्या बाजारपेठेत फार मोठा फरक पडला आणि 'नॉर्टन' चा दबदबा कमालीचा वाढला.

एकीकडे 'डॉ. सोलोमन' आणि 'मॅक फी' अँटी-व्हायरस यांच्यात चाललेल्या जोरदार कोर्टबाजी आणि कायद्याच्या लढाईने अचानकपणे वेगळेच वळण घेतले. 'मॅक फी' ने सुमारे ३२०० कोटी रुपये (६४० दशलक्ष डॉलर्स) देऊन चक्क 'डॉ. सोलोमन' कंपनी विकतच घेऊन टाकली. त्यामुळे कोर्टबाजी तर थांबलीच पण 'डॉ. सोलोमन' चे स्वतंत्र अस्तित्व संपले. खरं तर 'डॉ. सोलोमन' हे एक उत्तम अँटी-व्हायरस उत्पादन होते. ह्या साऱ्या व्यावसायिक उलाढाली धक्कादायक अशाच होत्या.

एकीकडे व्यावसायिक जगतात हे व्यवहार होत असताना दुसरीकडे

'विंडोज' साठीचे आणि 'मायक्रोसॉफ्ट ऑफिस' साठीचे व्हायरस येतच होते. नेटवर्क आणि इंटरनेटचा प्रसारही चांगला होत होता. 'Ms. Excel' साठी 'Excel.Laroux' हा व्हायरस, तर ms. Access साठी 'Accessiv' हा व्हायरस प्रथमच जन्माला आले. जून १९९८ मधल्या 'Wing5.CIH' ह्या व्हायरसने थोडा अधिकच धूमाकूळ घातला. जावा भाषेतील फाईल्ससाठी 'Java StrangeBrew' हा पहिला व्हायरसही ह्याच वर्षी ऑगस्ट महिन्यात आला. Visual Basic Scripts वर आधारलेला 'VBScript Rabbit' हा व्हायरस नोव्हेंबर १९९८ मध्ये आला. इंटरनेटची भाषा म्हणजे HTML (Hyper Text Mark Language) त्यावर आधारित 'HTML.Internal' नावाचा व्हायरसही आला.

थोडक्यात, आता हे स्पष्ट झालेले होते की जुना Dos प्रोग्राम आता जवळजवळ संपला आहे, आणि त्याच्यावर आधारित झालेले हजारो जुने व्हायरसही त्यामुळे केराच्या टोपलीत गेलेले आहेत. सुधारित 'विंडोज' प्रोग्रामचे माध्यम व्हायरसेससाठी 'डॉस' सारखे अनुकूल नव्हते. पण 'इंटरनेट' चे माध्यम वाढते असल्याने व्हायरस तयार करणारे इंटरनेटसाठी नवे व्हायरस आणतील अशी शक्यता खूपच होती, आणि १९९९ व २००० सालात ही भिती खरी ठरली.

१९९९ आणि २०००

'इंटरनेट' च्या माध्यमातील 'ई मेल' हा प्रकार जगभर पसरला होता. ह्या 'ई मेल' म्हणजे मुर्तिमंत संचारच होत्या. हा संचार जर व्हायरस प्रसारासाठी वापरला तर काम सोपे होईल असा विचार व्हायरस लिहिणारांच्या डोक्यात येणे अगदी स्वाभाविकच होते. झालेही तसेच. 'मेलिसा' हा जगप्रसिध्द 'ई मेल' व्हायरस १९९९ मध्ये आला आणि त्याने जगभरच्या काँप्युटरर्सना अक्षरशः हादरवले. हा खरा तर Macro प्रकारचा व्हायरस होता. तो 'मायक्रोसॉफ्ट वर्ड' मार्गे काँप्युटरमध्ये येई, आणि मग 'मॉयक्रोसॉफ्ट ऑफीस' मधील 'आऊटलूक' किंवा आऊटलूक एक्सप्रेस ह्या प्रोग्रामकडे वळे, तेथून तो 'ई मेल' मार्गे पुढे पसरे. 'मेलिसा' व्हायरसची प्रचंड चर्चा झाली आणि तो तयार करणाराचा शोध अमेरिकन FBI ह्या गुप्तहेर संघटनेने जगभर घेतला. शेवटी तो लिहिणाराला अटकही झाली. मात्र १९९९ साली व्हायरसपेक्षा मोठी चर्चा होती ती Y2K ची. पण ३१ डिसेंबर

१९९९ च्या रात्री बारा वाजता Y2K च्या भितीचा बार फुसका ठरला. २००० साल सहजपणे आणि फारसे कसलेही नुकसान न करता उजाडले. यावरुन लक्षात आले की बरेचदा साध्या साध्या गोष्टी बेसुमार जाहिरातींमुळे राक्षसासारख्या भासू लागतात, आणि वेळ आली की त्या क्षुल्लक असल्याचे दिसते.

२००० साल हे 'I Love You' व्हायरसने गाजवले. हा व्हायरसही 'ई मेल' मार्गेच पसरणारा होता. माणसाच्या भावनिकतेला स्पर्श करणारी 'फाईल अॅटॅचमेंट' 'ई मेल' बरोबर पाठवली तर माणसं ती फाईल कसलाही विचार न करता पटकन उघडतात आणि त्यातून लाखो-करोडो संगणकांमध्ये व्हायरस शिरु शकतो. हे' आय लव्ह यू' व्हायरसने दाखवून दिले. सोबत तुमच्यासाठी 'लव्ह लेटर' आहे, ते वाचा असा संदेश प्रथम 'ई मेल' देई. ते 'लव्ह लेटर' वाचण्यासाठी ती फाईल उघडली की व्हायरस पसरे. पसरताना तो 'मायक्रोसॉफ्ट आऊटलूक' मधील अॅड्रेस बुकात असलेल्या सर्व 'ई मेल' पत्त्यावर ही व्हायरस इन्फेक्टेड फाईल पाठवून देई. ही प्रक्रिया एखाद्या महागुणाकारा सारखी प्रचंड पसरत जाई. 'Love Virus' किंवा 'Love Bug' असेही वर्णन ह्या व्हायरसचे केले जाते. २००० साली 'अँटी-व्हायरस' प्रोग्राम सक्षम झालेले असल्याने आणि नव्या व्हायरसेसची माहिती इंटरनेटवरुन चटकन दिली जात असल्याने व्हायरसेसचे प्रमाण खूपच कमी झाले होते.

२००१ आणि नंतर

२००१ सालीही इंटरनेट व नेटवर्कवर आधारलेले व्हायरसेसच प्रसारात आहेत. युनिक्स, लीनक्स, विंडोज अशा विविध ऑपरेटींग सिस्टम्स, इंटरनेट, वेब ब्राऊझर्स, चॅट अशा विविध माध्यमांतून नवनवे व्हायरसेस हे भविष्यकाळातही येत राहतील. मात्र आता येणारे नवनवे प्रोग्राम्स, ब्राऊझर्स वगैरे अशा सुधारित स्वरुपात येत आहेत की दिवसेदिवस व्हायरस लिहिणारांचे काम अवघड होत चालले आहे. 'ई मेल' फाईल अॅटॅचमेंट उघडण्यापूर्वी ती तपासून घेण्याची प्रवृत्ती प्रस्थापित होत आहे. थोडक्यात, सुधारित प्रोग्राम्स, सुधारित अँटी-व्हायरस प्रोग्राम्स, नव्या व्हायरसेसच्या डेफिनीशन्स (उपाय) इंटरनेट वरुन त्वरित प्रसारित होणे आणि एकूणच संगणक वापरणारांमध्ये आलेली जागरुकता यामुळे 'व्हायरसेस'चे आव्हान

पूर्वीपेक्षा खूपच कमी धोकादायक राहिले आहे. मात्र ते संपूर्णपणे संपले आहे असे म्हणता येणार नाही. जोपर्यंत 'व्हायरसेस' मागची विकृत अणि विध्वंसक प्रवृत्ती माणसात आहे तोपर्यंत नवनवे व्हायरसेस येतच राहणार. इतिहासात काही ना काही भर ही पडतच राहणार. सारं काही माणसावर अवलंबून आहे. तो 'माणूस' तुम्हा आम्हा सर्वांमध्येच लपलेला आहे.

अफवांचे पीक अर्थात 'व्हायरस होक्सेस'

'अफवा' ही तुम्हा-आम्हाला नवी नाही. एखाद्या राजकीय नेत्याच्या मृत्यूपासून ते 'अमुक एका शहरात दंगल होतेय' वगैरेपर्यंत तऱ्हेतऱ्हेच्या अफवांचे पीक आपण पाहिलेले असते. असे अफवांचे पीक जेव्हा व्हायरसेसबद्दल पसरते तेव्हा गोंधळ, घबराट, चर्चा आणि त्यातून प्रसिध्दी असा क्रम दिसतो. जी मंडळी खराखुरा व्हायरस तयार करतात त्यांचे उद्दिष्ट कुणा एका व्यक्तीच्या कॉंप्युटरला नुकसान पोहोचवावे असा व्यक्तीगत स्वरुपाचा नसतो. ते काही अमुक एकाच्या विरोधातलं शत्रुत्व नसतं. एखाद्या विशिष्ट विभागात गोंधळ माजवावा असाही मर्यादित हेतू त्यामागे नसतो. व्हायरस खूप पसरावा, खूप गोंधळ माजावा, त्यातून खूप चर्चा व्हावी, वृत्तपत्रांतून प्रसिध्दी होऊन घबराट पसरल्यानंतर व्हायरस बनवणाराचा आत्मा थंड होतो. हा असुरी आनंद काही मंडळी व्हायरस तयार न करताही मिळवू पाहतात. त्यासाठी ते 'ई मेल' माध्यमाचा उपयोग करतात. आपल्या सुपीक (?) डोक्यातून ते काहीतरी कल्पना काढतात. ही कल्पना अर्थातच व्हायरसबद्दलची असते. थोडक्यात ते एक काल्पनिक व्हायरसच जन्माला घालतात. आता कल्पनेत काय, वाट्टेल ते करता येते. त्यासाठी प्रोग्रामिंग थोडेच करावे लागते? मग ही अफवा- प्रसारक मंडळी आपल्या कल्पनेतल्या व्हायरसेसबद्दलची 'ई मेल' काही मंडळीना पाठवतात. त्यात ''तो अमूक अमूक व्हायरस येत आहे. त्यापासून सावध रहा. अमुक एका विषयाबद्दल एखादी 'ई मेल'आली तर ती लगेच डिलीट

करा. त्यात महाभयंकर व्हायरस आहे. तो सारी मेमरी खाऊन टाकतो. सारी हार्ड डिस्क खराब करतो. वगैरे वगैरे'' मच मच ही मंडळी करतात. पण त्यातही सर्वांत आणखी महत्वाचा भाग ते विसरत नाहीत. तो म्हणजे ''ही 'ई मेल' तुमच्या सर्व मित्रांना पाठवून त्यांना सावध करा, त्यांचा दुवा घ्या'' असं 'ई मेल' मधून सांगायला ते विसरत नाहीत. त्यासाठी हीच 'ई मेल' पुढे मित्रांना 'फारवर्ड' करा असा सल्ला त्यांनी आपल्या 'ई मेल' मध्येच दिलेला असतो. महाभयंकर व्हायरसची बातमी वाचून तुम्ही प्रथम गंभीर होता, मग तुमच्या मित्रांची काळजीही तुम्हाला करावीशी वाटते आणि 'ई मेल' फॉर्वर्ड करण्याइतकी सोपी गोष्ट दुसरी कोणती? ही फारच सोपी गोष्ट तुम्ही करुन टाकता. मग हे लोण पुढे पुढे पसरत चालले की ज्याने ही अफवा पसरवली त्याचे मनोरंजन होते. तो मनातल्या मनात खूष होतो. हा सारा व्हायरस अफवेचा बाजार इंग्रजीत Virus Hoaxes म्हणून आता प्रसिध्द आहे. आत्ता पर्यंत जगात असे अनेक Hoaxes गाजले. त्यातले काही तर इतके विनोदी होते की लोकांनी त्यावर कसा काय विश्वास ठेवला याचेच आपल्याला आश्चर्य वाटते. समजा उद्या मी तुम्हाला एक अफवेची 'ई मेल' पाठवली की "Switch-2001" नावाचा भयानक व्हायरस आलेला आहे. त्यापासून सावध रहा. हा व्हायरस प्रथम तुमच्या कॉंप्युटरमध्ये शिरतो. तेथून तो हार्ड डिस्कमार्गे कॉंप्युटरच्या पॉवर सप्लायमध्ये जातो. मग इलेक्ट्रीक वायरमार्गे तुमच्या मेन स्विचपर्यंत पोहोचतो आणि तुमचा फ्युज घालवून तुमच्या इलेक्ट्रीक मीटरमध्ये शिरुन तुमचे इलेक्ट्रीक बिल चौपटीने वाढवतो. म्हणूनच सावधान! आपल्या सर्व मित्रांना ही 'ई मेल' फॉर्वर्ड करुन सावध करा. ते तुमचे आभारच मानतील'' आता माझ्या कल्पनेतून आलेला हा "Switch-2001" व्हायरस कॉंप्युटरपासून ते इलेक्ट्रीक मीटरपर्यंत प्रवास करील नाही तर आणखी पुढे जाईल. कल्पनाच शेवटी ती! तिने किती धावावं याला कुठली मर्यादा? पण त्याला आपण किती फसायचं, हे आपल्याला कळलं पाहिजे. जेव्हा आपण अशी अफवेची 'ई मेल' फॉर्वर्ड करतो तेव्हा नकळत आपणच ती अफवा पसरवत असतो, हे आपण लक्षात घ्यायला हवं. तुमचा विश्वास बसावा म्हणून कित्येकदा अशी अफवेची 'ई मेल' बड्या कंपनीच्या नावे वा प्रसिध्द व्यक्तीच्या नावेही केली जाते. म्हणजे उदाहरणार्थ मायक्रोसॉफ्ट व बिल गेटसच्या नावे 'ई मेल' पाठवली जाईल. त्यात बिल गेटस

तुम्हाला सांगेल की 'येत्या बुधवारी 'विंडोज'ला व्हायरसचा धोका आहे. ह्या दिवशी तुमचा कॉंप्युटर चालू करुच नका. मित्रांनाही हे कळविण्यासाठी ही 'ई मेल' फॉर्वर्ड करा.''

थोडक्यात, एव्हाना तुमच्या नीट लक्षात आलेले आहे की Virus Hoax म्हणजे नेमवेक काय, आणि त्याची वासलात कशी लावायला हवी. हे अवश्य करा:

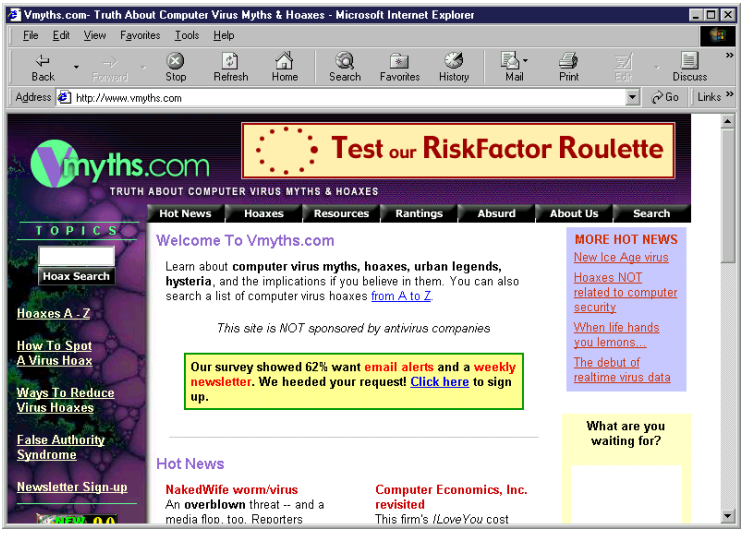
१. खात्री केल्याशिवाय 'ई मेल' फॉर्वार्ड करु नका. http://www.virusbtn.com ह्या साईटला भेट द्या, किंवा http://www.vrnyths.com ह्या साईटला भेट द्या. ह्या साईटस् नव्या व जुन्या व्हायरसेसची तसेच Hoaxes चीही माहिती तुम्हाला विश्वासार्हतेने देऊ शकतात.

२. आलेली 'ई मेल' ही Hoax किंवा अफवा आहे हे कळल्यानंतर ती ताबडतोब डिलीट करुन टाका.

जगात गाजलेल्या अफवा (Hoax)

१. ए.ओ.एल. / टाईम वॉर्नर होक्स

अगदी अलिकडे काही वर्षांपूर्वी 'अमेरिका ऑनलाईन (ए.ओ.एल.)' व 'टाईम वॉर्नर' तसेच 'ई.एम.आय' ह्या कंपन्यांचे एकत्रीकरण झाले हे



तुम्हाला आठवत असेल. ह्या तीन जगातील बलाढ्य कंपन्या आहेत आणि सुमारे ५००० कोटी रुपयांची उलाढाल ह्या एकत्रीकरणामुळे झाली असा अंदाजही व्यक्त केला गेला आहे.

ह्या एकत्रीकरणाची चर्चा चाललेली असतानाच एका 'ई मेल' ने चांगलीच खळबळ उडवून दिली. ह्या 'ई मेल' मध्ये म्हंटले होते की 'ई मेल' माध्यमातून 'संगीत' पाठविण्याच्या उद्योगाचे सर्वेक्षण ह्या तीन कंपन्या करीत आहेत. पाठवलेल्या 'ई मेल'ला एक गुप्त कोडींग केलेले आहे. त्यामुळे ही 'ई मेल' कोणाला पाठवली गेली आहे याचा रेकॉर्ड 'ए.ओ.एल.' कडे आहे. तुम्ही पीसी वापरत असा की मॅकींटॉश. त्याने फरक पडत नाही. 'ई.एम.आय.' कंपनीने जाहीर केले आहे की जर ही मेल तुम्ही १० जणांना फॉर्वर्ड केलीत व त्या दहा जणांपैकी जो जो ही मेल पुढे पाठवील त्या प्रत्येकामागे तुम्हाला १० पौंडाचा चेक पाठविण्यांत येईल.''

ही 'ई मेल' पाठवणारा पुढे म्हणतो की ''मलाही हा प्रकार एखादा 'इंटरनेट स्वॅम' असावा असे पहिल्यांदा वाटले. पण कालच मला 'ई.एम.आय' आणि 'टाईम वॉर्नर' कडून एक 'ई मेल' आली आणि त्याद्वारे माझ्या घरचा पत्ता विचारण्यांत आला. आजच सकाळी मला १० पौंडाचे व्हॉऊचर आणि ५० पौंडाचा चेक मिळाला. व्हावचर वापरुन कुठल्याही 'एच.एम.व्ही' डीलरकडून तुम्ही कॅसेट/सीडी मिळवू शकता''

''ह्या ऑफरचा फायदा तुम्हीही घेऊ शकता. नुसती 'ई मेल' फॉर्वर्ड करण्यात तुमचं काय नुकसान आहे?'' आता ह्या अफवेचा प्रकार पहा. ह्यात व्हायरस कुठेही नाही. मोठी नावे वापरलेली आहेत. योजना वास्तववादी वाटावी, आणि पटावी अशी भाषा आहे. वर नुसती 'ई मेल' फॉर्वर्ड करण्यात आपले काय नुकसान आहे?' असा प्रश्नही विचारलाय. हे सारे पटण्यासारखेच आहे. मग पुढले दहा जण आणखी दहा-दहांना म्हणजे शंभरांना आणि ते पुढल्या हजारोंना ह्या मेल पाठवणार आणि जगातले 'ई मेल सर्व्हर्स' ह्याच मेलनी भरभरून वाहणार. काही 'ओव्हरफ्लो' होऊन ठप्पही होणार. हे सारे झाले की एखादा व्हायरस गोंधळ घालणार नाही एवढा गोंधळ होणार. म्हणजेच 'अफवा' पसरवणाऱ्याचा उद्देश सफल होणार.

२. 'व्हॅलंटाईन' होक्स

'' १४ फेब्रुवारी २००० ह्या 'व्हॅलंटाईन' डे च्या दिवशी तुम्हाला एक 'ई मेल' येईल. त्याचा विषय आहे "Be my Valentine" ह्या 'ई मेल' मध्ये एक भयंकर (deadly) व्हायरस आहे. तो तुमच्या 'विंडोज' प्रोग्राम पुसून टाकील. कृपा करून ही मेल उघडू नका. डिलीट करुन टाका. आणि इतरांनाही सावध करा.''

ही अफवा २७ जानेवारी २००० रोजी पसरवली गेली होती. त्यामुळे अनेक प्रेमिकांनी आपल्या खऱ्याखुऱ्या 'ई मेल' ही न वाचता डीलीट करुन टाकल्या आणि चांगल्या 'व्हॅलंटाईन' ऑफर्स गमावल्या.

काय हा फाजीलपणा!! गाढव कुठले!!!

३. 'ईल्फ बाऊल' गेम होक्स

''तुम्हाला FROGAPULT.EXE आणि ELFBOWL.EXE ह्या दोन फाईल्स गेम म्हणून पाठविण्यांत येतील. त्यात छुपा व्हायरस आहे. हा व्हायरस ख्रिसमसच्या दिवशी कार्यान्वित होतो व तुमची संपूर्ण सिस्टम धुवून टाकतो,'' असा इशारा देणारी एक उलट्या प्रकारची अफवा होती. प्रत्यक्षात ह्या दोन फाईल्स अस्तित्वात होत्या. आणि ते अगदी सामान्य असे गेम्स होते. त्यात 'व्हायरस'चा अंश अजिबात

नव्हता. ख्रिसमसच्या निमित्ताने मुले जे गेम्स एकमेकांना पाठवतात त्यात हे गेम्स खूपच लोकप्रिय होते. अर्थात, एखाद्याला ह्याच फाईल्समध्ये व्हायरस लपवून पाठवायचा असेल तर अशक्यही नव्हते. पण ही प्रत्येक फाईल 'व्हायरसभरीच' आहे हे विधानही खरे नव्हते.

अशाच प्रकारचे अनेक होक्स आजपर्यंत आले आणि पुढेही येत राहतील. भिती दाखविणे ('व्हायरस'ची भिती पाहण्यासारखी असते) किंवा मोहात पाडणे (मोफत, फायदा वगैरेंसारखे शब्द 'मोह' चाळवतात) ह्या दोन मानवी भावनिक तत्वांचा वापर होक्समध्ये असतो. ''ई मेल' फॉर्वर्ड करा, इतरांना कळवा'' असा मन:पूर्वक आग्रह असतो. विश्वास बसावा म्हणून खूपदा मायक्रोसॉफ्ट, ए.ओ.एल, टाईम वॉर्नर वगैरेसारखी मोठी नावे वापरलेली असतात.

एखादा होक्स व्हायरसपेक्षाही मोठे नुकसान करु शकतो हे त्यामुळेच विसरुन चालणार नाही.

वॉर्म्स, ट्रोजन हॉर्सेस आणि लॉजिक बॉम्ब्स

संगणकाची वाढत चाललेली गरज आणि वाढता प्रसार यातून एका संगणकाला जोडून दुसरा संगणक उभा राहिला. एकाच जागी अनेक संगणक आले तेव्हा मग नेटवर्कची गरज निर्माण झाली. सर्व संगणक हातात हात घालून एकमेकांशी संवाद करतील एकमेकांना एकमेकांचा डेटा देतील - घेतील तर वेळ वाचेल हे लक्षात आले. मग ह्या गरजेतून 'नेटवर्क' चा शोध आणि नंतर विकास होत गेला.

१९८२ ची गोष्ट पहा. एखाद्या कागदपत्राच्या फोटोकॉपीला आपण आता सर्रास 'झेरॉक्स कॉपी' असं म्हणतो. प्रत्यक्षात 'झेरॉक्स' हे कंपनीचे नाव आहे. परंतु ह्या कंपनीची 'फोटोकॉपी' करण्याची यंत्रे इतकी प्रसिध्द झाली की लोक त्या कॉपीजनाच 'झेरॉक्स कॉपी' म्हणू लागले. ह्या अजस्त्र मोठ्या 'झेरॉक्स कॉर्पोरेशन' कंपनीत अनेक संगणकांचे नेटवर्क होते. प्रत्येक संगणकात 'नको असलेल्या' टेंपररी फाईल्स तयार होत. ह्या टेंपररी फाईल्स आपोआप काढून टाकणारा एक अत्यंत उपयुक्त प्रोग्राम 'झेरॉक्स' ने तयार केला. हा प्रोग्राम स्वतःच 'नेटवर्क' मार्गे निरनिराळ्या संगणकांमध्ये जाई आणि 'टेंपररी' फाईल्स काढून साफसफाई करण्याचे काम करी. ही व्यवस्था खरोखरीच सोयीस्कर, वेळ वाचवणारी आणि स्वयंचलित अशी होती. पुढे कुणीतरी ह्या प्रोग्राममध्ये काहीतरी 'गडबड'

केली. ह्या गडबडीमुळे तो प्रोग्राम टेंपररी फाईल्सबरोबर इतर डेटाही गाळून टाकू लागला. ही पडझड महाभयानक होती. यामुळे 'झेरॉक्स कॉर्पोरेशन' कंपनी हादरली. 'भीक नको, पण कुत्रा आवर' असं म्हणण्याची पाळी त्यांच्यावर आली. ह्या प्रोग्रामच्या कचाट्यातून सुटण्यासाठी मग 'झेरॉक्स'ने स्वत:चा आणि स्वत:साठी एक अँटी-व्हायरस प्रोग्रामच तयार केला. असे उपायात्मक जे काही पहिले सुरुवातीचे अँटी-व्हायरस प्रोग्राम्स तयार झाले त्यात हा 'झेरॉक्स' चा १९८२ चा प्रोग्रामही समाविष्ट आहे.

मी हा 'झेरॉक्स' कंपनीतला किस्सा तुम्हाला अशासाठी सांगितला की 'वॉर्म' म्हणजे काय ते तुमच्या नीट लक्षात यावे 'व्हायरस' आणि 'वॉर्म' यात काही ठळक फरक आहे. पण बहुतेक लोक आजही 'व्हायरस' आणि 'वॉर्म' हे एकच समजतात. 'झेरॉक्स' कंपनीतला 'टेंपररी' फाईल गाळणारा हा एक प्रकारचा 'वॉर्म' होता. जोपर्यंत तो केवळ 'टेंपररी' फाईल्स (त्या नकोशाच असत) गाळत होता तोपर्यंत तो उपयुक्त होता. पुढे त्याने नको ते उपद्व्याप केले तेव्हा त्यावर उपाय योजावा लागला.

'व्हायरस' हा प्रोग्राम एका संगणकावर स्वत:च्या अनेक प्रती तयार करीत पसरतो. दुसऱ्या संगणकाशी त्याचा संपर्क येण्यासाठी काहीतरी गोष्ट घडावी लागते. म्हणजे उदाहरणार्थ व्हायरस लागलेली फ्लॉपी ह्या संगणकाकडून त्या संगणकाकडे जावी लागते. तेव्हाच एकाचा इन्फेक्टेड बूट रेकॉर्ड दुसरीकडे जाणार. किंवा, एखादी फाईल 'ई मेल' वा तत्सम मार्गाने दुसऱ्या संगणकात जाऊन तेथे ती कुणीतरी उघडली तरच व्हायरस पसरु शकतो. तसच बरेचदा व्हायरस हा दुसऱ्या एखाद्या EXE किंवा Com प्रकारच्या फाईलमध्ये लपतो. जेव्हा ही EXE किंवा Com फाईल आपण उघडतो तेव्हा व्हायरसही कार्यरत होतो. अशा अनेक EXE फाईल्समध्ये एकाच व्हायरसची त्याने तयार केलेली एकेक प्रत (कॉपी) असू शकते. कारण व्हायरस स्वत:च्या अनेक प्रती स्वत:च तयार करुन काम करतो.

पण 'वॉर्म' चा स्वभाव थोडा वेगळा आहे. 'वॉर्म' हा एके ठिकाणी थांबून कारवाई करण्यापेक्षा वेगवेगळ्या संगणकांमध्ये स्वत:हूनच भ्रमण करीत 'बारा गावचं' पाणी पित जाणे पसंत करतो. त्यामुळे 'नेटवर्क' आणि 'इंटरनेट' हे त्याच्यासाठी भ्रमणाचे 'हाय वे' आहेत. 'वॉर्म' कुणाला

पसरवावा लागत नाही. तो स्वतःच पसरतो. स्वतःच भ्रमण करतो 'इंटरनेट' व 'नेटवर्क' यांचा वेग प्रचंड आहे. एका फ्लॉपीतून दुसऱ्या फ्लॉपीत व्हायरस पसरायला खूप वेळ लागेल. पण 'नेट' च्या भ्रमणातून विद्युत वेगाने 'वॉर्म' पसरु शकतो. 'वॉर्म' हा स्वतंत्र प्रोग्राम 'डेटा'चा विध्वंस करु शकतो. किंवा तो डेटा बदलूही शकतो.

थोडक्यात, 'वॉर्म' हा एक 'सेल्फ कंटेंड' म्हणावा असा प्रोग्राम आहे. तो स्वतःच्या स्वतंत्र प्रती सामान्यतः नेटवर्क मार्गे अन्य संगणकांमध्ये नेऊन सोडतो. 'व्हायरस' ला एखाद्या अन्य प्रोग्राममध्ये जाऊन घुसावे लागते. 'वॉर्म' ला त्याची गरज नसते. तो स्वतंत्रच राहतो. मुख्यत्वे दोन प्रकारचे 'वॉर्म' असतात. पहिला प्रकार म्हणजे 'होस्ट कॉंप्युटर वॉर्म' आणि दुसरा प्रकार आहे 'नेटवर्क वॉर्म.'

'होस्ट कॉंप्युटर वॉर्म' हा पूर्णपणे एकाच संगणकात राहतो आणि 'नेटवर्क' च्या कनेक्शनचा उपयोग करुन अन्य संगणकांमध्ये शिरतो. जेव्हा तो एका नेटवर्कमधल्या दुसऱ्या संगणकात जातो तेव्हा त्याचा पहिला अवतार समाप्त होतो. म्हणजेच 'होस्ट कॉंप्युटर वॉर्म' हा एक नेटवर्कवर एकटाच इकडून तिकडे फिरतो. काही जण ह्या प्रकारच्या वॉर्मला 'रॅबिट' असेही म्हणतात. 'रॅबीट,' अर्थात इकडून तिकडे उड्या मारीत फिरणारा ससा. 'होस्ट कॉंप्युटर वॉर्म'चा स्वभाव त्या सशासारखाच आहे.

दुसरा प्रकार 'नेटवर्क वॉर्म' चा तोही स्वतंत्र प्रोग्रामच. स्वतःहून स्वतंत्रपणे चालणाराच. पण त्याचे आपापले विभाग असतात. ह्या विभागांना 'सेगमेंट' असं म्हंटलं जातं. हे सेगमेंट 'नेटवर्क' मधल्या वेगवेगळ्या मशीनवर एकाच वेळी काम करीत असतात. प्रत्येक विभाग हा वेगवेगळ्या प्रकारची कृती करीत असणं शक्य असतं. काही वेळा एकाच नेटवर्कवरच्या दोन निरनिराळ्या कॉंप्युटरमध्ये असलेल्या वेगवेगळ्या सेगमेंटमध्ये आपापसात सहकार्य असते. ते एकमेकांच्या हातात हात घालून आपली कारवाई करु शकतात. ह्या प्रकारांना काही वेळा 'ऑक्टोपस' असही म्हंटलं जातं.

कल्पना करा की एका 'वॉर्म' ने बँकेच्या कॉंप्युटरमध्ये शिरुन एक छुपे अकाऊंट उघडले व त्या अकाऊंटमध्ये काही रक्कम ट्रान्स्फर करुन घेतली. बँकेच्या लक्षात आले की संगणकात अमुक अमुक वॉर्म आहे. तो 'वॉर्म' शोधून गाळून टाकला गेला. 'वॉर्म' चे अस्तित्व तेथे संपले. पण त्याने

तयार करुन ठेवलेले ते बोगस अकाऊंट! त्याचे काय? ते तसेच राहणार. त्या अकाऊंटमध्ये अमुक-तमुक रक्कम नियमित ट्रान्स्फर करण्याची 'वॉर्म'ची सूचना तशीच राहून गेली असेल तर त्या बोगस अकाऊंटमध्ये ट्रान्स्फर्स चालूच राहणार. थोडक्यात, एक प्रकारे 'वॉर्म' चा मृत्यू झाला व अस्तित्व संपले तरी त्याचे भूतच जणू शिल्लक असते.

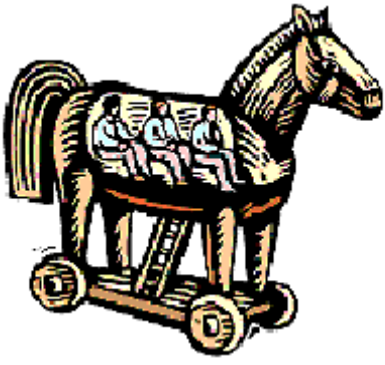
'वॉर्म' आणि 'व्हायरस' यांच्यात वैद्यकीय किंवा डॉक्टरी भाषेत स्पष्ट करुन फरक सांगायचा तर 'वॉर्म' हा साधे ट्युमर आहे (benign tumor) आणि 'व्हायरस' हे कॅन्सरचे ट्युमर (malignant tumor) आहे. अर्थात दोन्ही ट्युमर्स ही अनिष्टच. फक्त साधे ट्युमर ऑपरेशन करून काढून टाकले की संपते. पण कॅन्सरचे ट्युमर एका ठिकाणाहून ऑपरेशनने काढले तरी दुसरीकडे उद्भवू शकते. कारण कॅन्सर हा शरीरभर पसरलेला असतो.

सुप्रसिध्द 'मेलिसा' व्हायरस किंवा, 'एक्स्प्लोअररझीप' किंवा 'लव्ह लेटर' हे सारे 'वॉर्मस' होते. त्यांनी अधिक अधिक संख्येने संगणकात प्रवेश करण्याचा प्रयत्न केला. १९८७ साली 'ख्रिसमस' नावाचा वॉर्म आला होता. तो मॉनिटरवर 'ख्रिसमस ट्री'चे चित्र दाखवित असे. १९८८ चा 'मॉरिस इंटरनेट वॉर्म' हाही धूमाकूळ माजवून गेल्याची नोंद आहे.

जानेवारी २००१ साली जगात ३० कोटी लोक इटंरनेट वापरीत आहेत असा अंदाज व्यक्त केला जातो. जर हे सारे एकाच प्रकारचे सॉफ्टवेअर आणि सिस्टम्स वापरीत असतील तर एक वॉर्म त्या प्रत्येकाकडे पोहोचू शकतो. ''व्हायरस नियंत्रणाच्या पांरपारिक पध्दती 'वॉर्म' च्या बाबतीत कामी येत नाही. त्यासाठी 'अँटी-व्हायरस' कंपन्यांनी अधिक विचार केला पाहिजे'' असे उद्गार 'नार्टन' कंपनीचे रिसर्च डायरेक्टर स्टीफन ट्रीलींग यांनी नुकतेच एका व्याख्यानात काढले.

ट्रोजन हॉर्सेस

'ट्रोजन हॉर्स' ची ऐतिहासिक कथा तुम्ही नक्कीच वाचली असेल. 'ट्रॉय' शहराच्या प्रवेशद्वाराशी एक भला मोठा लाकडी घोडा येऊन उभा राहिला. तो एखाद्या इमारतीसारखा अजस्त्र होता. ट्रोजन लोकांसाठी ही एक मित्रत्वाची भेट आहे असे त्यांना वाटल्यामुळे त्या घोड्याला ट्रोजन



लोकांनी आपल्या ट्रॉय शहरात प्रवेश दिला. हा चाकांचा लाकडी घोडा शहरात शिरला आणि त्यातून शेकडो ग्रीस सैनिक शस्त्रास्त्रे घेऊन अचानक बाहेर पडले आणि त्यांनी ट्रॉय शहराचा पाडाव केला अशी ती गोष्ट आहे. ह्या गोष्टीशी अतिशय साम्य असल्यानेच त्या विशिष्ट घातक प्रोग्राम्सना 'ट्रोजन हॉर्सेस' असे म्हंटले जाते. खरं तर 'ट्रोजन हॉर्स' हा एक विश्वासघात आहे. प्रत्यक्षात एक उपयुक्त सॉफ्टवेअर आहे असा आभास तयार करुन 'ते डाऊनलोड करून वापरावे' असा सल्ला 'ट्रोजन हॉर्स' देतो. कधी तो एखादा गेम असल्याचे सांगतो किंवा एखादी युटीलिटी.

'इनर सर्क्ल क्लब' नावाचा एक हॅकर ग्रुप आहे. त्याने एक चेस (बुध्दीबळाचा) प्रोग्राम तयार केला. कॅनडातील एका मेनफ्रेम काँप्युटरच्या ऑपरेटरशी ही हॅकर मंडळी ह्या प्रोग्रामवर बुध्दीबळ खेळायची. 'बुध्दीबळ खेळल्याने काय होणार आहे?' असा भोळसट विचार त्या ऑपरेटरने केला. पण हा 'चेस प्रोग्रम' म्हणजे एक ट्रोजन होता. चेस खेळता खेळता ही हॅकर मंडळी त्या मेनफ्रेम काँप्युटरमध्ये कधी घुसली हे त्या ऑपरेटरला कळले सुध्दा नाही. बिचारा सगळ्या बाजूंनी चेकमेट होऊन गेला.

'बुलेटीन बोर्ड सर्व्हिस' (बी.बी.एस.) हा एकेकाळी खूपच लोकप्रिय प्रकार होता. तेथे लोकांना एखादा आकर्षक 'ग्राफीक्स' प्रोग्राम द्यायचा आणि तो प्रोग्राम म्हणजे 'ट्रोजन हॉर्स' आहे हे कळेपर्यंत जो विध्वंस करायचा तो करुन द्यायचा असे प्रकार घडलेले आहेत.

थोडक्यात, 'ट्रोजन हॉर्स' च्या आतमध्ये काहीही असू शकते. व्हायरस

ही असू शकतो, किंवा 'वॉर्म' ही असू शकतो किंवा दोन्हीही असू शकतात. मात्र व्हायरसप्रमाणे 'ट्रोजन हॉर्स' स्वत:च्या अनेक प्रती तयार करीत नाही, किंवा आपोआप पसरत नाही. मात्र एकदा का त्याने आपले दरवाजे उघडले की तो कसलीही दयामाया न दाखवता आपला उद्योग करुन मोकळा होतो.

बँकेतील काँप्युटरमध्ये शिरुन तेथील प्रत्येक अकाऊंटमधून अगदी दोन पाच रुपयांएवढी नगण्य रक्कम काढून ती एका बोगस अकाऊंटमध्ये जमा करायची आणि नंतर त्या बोगस अकाऊंट मध्ये जमलेली रक्कम काढून घ्यायची हा गुन्हाही एका 'ट्रोजन हॉर्स' वर आधारलेला आहे. ह्या गुन्ह्याला 'Salami Slicing' असे म्हणतात.

लॉजिक बॉम्ब

'लॉजिक बॉम्ब' आणि 'ट्रोजन हॉर्स' यात बरेच साम्य आणि एक महत्वाचा फरक आहे. दोघेही महाभयंकर विध्वंस करण्यासाठी प्रसिध्द आहेत. 'ट्रोजन हॉर्स' च्या आत विघातक 'व्हायरस' वा 'वॉर्म' लपलेले असतील. पण 'लॉजिक बॉम्ब' हा एखाद्या प्रोग्रामध्ये किंवा 'डेटा' मध्येही लपलेला असू शकतो. महत्वाचा फरक हा की 'लॉजिक बॉम्ब' हा एखाद्या 'टाईम बॉम्ब' प्रमाणे विशिष्ट वेळी किंवा विशिष्ट कृतीनंतर फुटतो आणि धुमाकूळ घालतो.

बरेचदा 'लॉजिक बॉम्ब' चा वापर सूड घेण्यासाठीही केला जातो. त्याची अनेक उदाहरणे आहेत. एका कर्मचाऱ्याला कामावरुन काढून टाकण्यांत आले. ह्या कर्मचाऱ्याकडून कंपनीने पुरेसे काम करुन घेतले होते आणि वेतन मात्र अपुरे दिलेले होते. कंपनीने आपल्याकडून जे काम अन्यायाने करुन घेतले आहे त्याचा सूड त्याला घ्यायचा होता. त्याने एक 'लॉजिक बॉम्ब' त्याने काँप्युटरवर केलेल्या कामातच पेरुन ठेवला. त्यात व्यवस्था अशी होती की कंपनी ज्या क्षणी त्याला कामावरुन काढून टाकील आणि ज्या क्षणी त्याचे नाव कर्मचाऱ्यांच्या यादीतून काँप्युटरवरुन डीलीट करील तत्क्षणी हा 'लॉजिक बॉम्ब' फुटेल. 'लॉजिक बॉम्ब' फुटेल म्हणजे एखाद्या भयानक व्हायरस आत शिरेल किंवा चक्क सारी सिस्टम व डेटाच पुसला जाईल 'लॉजिक बॉम्ब' हा दहा वर्षांनीही फुटू शकतो. त्याला काळा-वेळाची मर्यादा नाही. म्हणजेच कित्येक वर्षे तो आत गुपचुप राहूही शकतो.

कुणालाही कसलाही संशय येत नाही.

बरेचदा 'लॉजिक बॉम्ब'चा वापर ब्लॅकमेलींगसाठीही केला जातो. कुणीतरी तुमच्या कॉंप्युटरमध्ये 'लॉजिक बॉम्ब' ठेवला आहे. अमुक एक रक्कम द्या, तर तो बॉम्ब कसा निकामी करायचा ते सांगू'' अशा प्रकारचे ब्लॅक-मेलींग करु शकतो. काही वेळा 'लॉजिक बॉम्ब'चा वापर 'इन्शुरन्स' म्हणूनही वेगला जातो. खूपदा कन्सल्टंट वा सप्लायर एखाद्या कंपनीला संपूर्ण प्रोग्राम तयार करुन देतो, वा कॉंप्युटर्स सेट-अप करुन देतो. त्याचे पैसे जर त्याने विशिष्ट अवधीत दिले नाहीत तर 'लॉजिक बॉम्ब' फुटतो आणि सारा डेटा नाहीसा होतो. बिलेवसुलीसाठी असा बॉम्ब पेरुन ठेवणारे लोक आणि संस्था जगात आजही आहेत. ऑस्ट्रेलियातील मेरीलँड लायब्ररीने एका सिस्टमचे बिल ती सिस्टम नीट चालत नाही म्हणून द्यायचे नाकारले. मात्र सुदैवाने लायब्ररीला तो 'लॉजिक बॉम्ब' अगोदरच मिळाला आणि पुढला अनर्थ टळला. 'लॉजिक बॉम्ब'ही 'ट्रोजन हॉर्स' प्रमाणे स्वत:च्या प्रती तयार करीत नाही.

ह्या 'वॉर्म', 'ट्रोजन' आणि 'लॉजिक बॉम्ब' च्या प्रकरणाचा सारांश काय? अनिष्ट आणि विघातक अशा प्रोग्राम्समधील विविधता ते दर्शवितात. संगणकाच्या 'मेमरी' चे कार्य मंदगतीला आणणे, 'संगणका'च्या एकूणच कामकाजात अडथळे आणणे, त्यावर ताण आणणे, विविध डेटा संकटात पाडणे किंवा उखडून टाकणे हे सारे 'व्हायरस' चे कर्तृत्व ह्या प्रकारांमध्येही आहे. थोडक्यात, जसे व्हायरसेस पासून सावध रहायला हवे, तसे यांच्यापासूनही सावधान असायलाच हवे. 'ट्रोजन' आणि 'लॉजिक बॉम्ब' हे वॉर्म आणि व्हायरसच्या तुलनेत खूपच कमी दिसून येतात. म्हणून बरेचदा त्यांचा विचार केला जात नाही मात्र याचा अर्थ त्यांचा धोका कमी आहे असं मात्र अजिबात नाही.

'व्हायरस' चे प्रकार

आजमितीस सुमारे ५५००० व्हायरस येऊन गेलेले आहेत. त्यांच्या अनेक तऱ्हा आहेत. ते काँप्युटरच्या बूट सेक्टरमध्ये राहणारे होते की एखाद्या फाईलबरोबर येणारे होते, स्वत:चे अस्तित्व पूर्णपणे लपवून राहणारे होते की आपले कोड क्षणोक्षणी बदलून ओळखू न येणारे, उपाय काढता येऊ न देणारे होते, मेमरीत लपणारे, विंडोज प्रोग्रामसाठी तयार झालेले अशा शेकडो प्रकारात व्हायरसेसना विभागता येईल. प्रत्येक जण आपापल्या परीने असे 'व्हारायहीभरे' वर्गीकरण करील. पण ढोबळमानाने म्हणा किंवा व्हारायटीभरे मुख्य प्रकार सांगायचे झाले तर ते खालील प्रमाणे:

ज्या गोष्टींना व्हायरसेसची लागण होते तो निकष धरुन व्हायरसेसचे खालील प्रकार पहा:

१. सिस्टम सेक्टर व्हायरसेस: खुद्द डिस्कच्या नियंत्रणासाठी असलेल्या माहितीलाच हे व्हायरस बाधा आणतात. 'डॉस' चा बूट सेक्टर व डिस्कचे पार्टीशन सेक्टर ताब्यात घेणारे व्हायरस यात मोडतात.

२. फाईल व्हायरसेस: Com व EXE तसेच BAT ह्या प्रकारच्या फाईल्स आपल्याला प्रोग्राम फाईल्स म्हणून माहीत आहेत. ह्या प्रोग्राममध्ये जायचे व तो प्रोग्राम उघडला गेला की आपली कारवाई चालू करायची हा प्रकार हे व्हायरस करतात.

३. मॅक्रो व्हायरसेस: 'मॅक्रो' हे मायक्रोसॉफ्ट ऑफिसमुळे विशेष लोकप्रिय

झाले. तेही एक प्रकारचे प्रोग्रामच. त्यामुळे व्हायरसे च्या दृष्टीने ते एक 'संधीच' असतात.

४. कंपॅनियन व्हायरसेस: अस्तित्वात असलेल्या EXE फाईलच्या जागी Com प्रकारची व्हायरस फाईल तयार करायची व 'डॉस' च्या नियमाप्रमाणे EXE फाईलच्या अगोदर Com फाईल चालत असल्याने आपोआपच व्हायरसभरी Com फाईल चालवून गोंधळ घालायचा असा ह्या 'कंपॅनियन' चा स्वभाव आहे.

५. क्लस्टर व्हायरसेस: आपली हार्ड डिस्क असो की फ्लॉपी डिस्क. ती वेगवेगळ्या भागात विभागलेली असते. त्यांना आपण क्लस्टर म्हणतो. वेगवेगळ्या क्लस्टर्समध्ये वेगवेगळ्या डिरेक्टरीज असतात. उदाहरणार्थ जर आपण मायक्रोसॉफ्ट वर्ड प्रोग्राम वापरत असलो तर मायक्रोसॉफ्ट वर्डची डिरेक्टरी आणि त्या डिरेक्टरीतल्या फाईल्स कुठल्या तरी क्लस्टर मध्ये डिस्कवर असतात. जेव्हा आपण 'वर्ड' प्रोग्राम चालू करतो तेव्हा ह्या डिरेक्टरीतल्या EXE किंवा Com फाईल्स चालतात. कारण तशी सूचना PATH मध्ये असते. मात्र ह्या व्हायरसमुळे तुम्ही त्या प्रोग्रामची EXE फाईल न चालवता व्हायरसचे कोड कार्यान्वित करता. कारण ह्या प्रकारातला व्हायरस तशा प्रकारे डॉस इन्फर्मेशन बदलत असतो. थोडक्यात, फार गोंधळून न जाता इतकच लक्षात घ्या की हा डिरेक्टरी व्हायरस आहे.

६. बॅच फाईल व्हायरसेस: autoexec.bat नावाची फाईल तुम्ही ऐकलीच असणार. ज्या फाईल्सचे extention 'BAT' असते त्यांना बॅच फाईल म्हणतात. ह्या एक प्रकारच्या प्रोग्राम फाईल्स असतात. उदाहरणार्थ autoexec.bat मध्ये काँप्युटर सुरु झाल्यानंतर काय काय प्रोग्राम वा कृती व्हावी याच्या सुचना असतात. त्याप्रमाणे तुमचा काँप्युटर सुरु होतो. पुढे जाऊन आणखी उदाहरण द्यायचे तर तुमची सूचना असेल की काँप्युटर सुरु झाल्याबराबेर पेजमेकर प्रोग्रामही सुरु व्हावा तर तशी सूचना autoexec.bat फाईलमध्ये देता येते. तर अशा बॅच किंवा bat फाईलना लागण लावणारा व्हायरस हा 'बॅच फाईल व्हायरस' म्हंटला जातो.

७. सोर्स कोड व्हायरसेस: प्रत्यक्ष एखाद्या प्रोग्रामच्या कोडमध्ये हा व्हायरस आपले कोडही मिसळतो, आणि कार्यभाग साधतो.

व्हायरसेसची लागण करण्याची जी पध्दत आहे त्या पध्दतीप्रमाणेही व्हायरसेसचे प्रकार पाडता येतात. त्यातील मुख्य आणि महत्वाचे प्रकार असे:

१. पॉलीमॉर्फिक व्हायरसेस: हा 'व्हायरस' आपले गुणधर्म स्वरुप बदलते ठेवतो.

२ स्टील्थ व्हायरसेस: अँटी-व्हायरस प्रोग्रामच्या दृष्टीसही आपण पडू नये अशी काळजी घेऊन लपण्याची जागा निश्चित करीत वस्ती करणारा व्हायरस म्हणजे स्टील्थ व्हायरस.

३. फास्ट अँड स्लो इनफेक्टर्स: अँटी व्हायरस प्रोग्रामच्याच पाठीवर बसून फाईल्सना लागण लावीत जाणे हे यांचे वैशिष्टय. अँटी व्हायरस जेव्हा एक एक फाईल स्कॅन करण्यासाठी उघडतो तेव्हा हा व्हायरस अशा प्रत्येक फाईलला आपली लागण करतो. जसजसा अँटी व्हायरस पुढे पुढे जातो तसतसा हाही ती प्रत्येक फाईल इनफेक्ट करीत करीत शेवटी संपूर्ण डिस्कच व्हायरसमय करुन टाकतो. याला 'फास्ट इनफेक्टींग' म्हणतात. स्लो इनफेक्टर व्हायरस मात्र प्रोग्राम उघडून चालल्यानंतरच ती फाईल इनफेक्ट करीत असतो.

४. स्पार्स इनफेक्टर: अँटी-व्हायरस प्रोग्रामला पकडता येऊ नये यासाठी प्रयत्न करीत आलेले हे व्हायरसेस असतात. यांच्या तऱ्हा त्यामुळे वेगळ्याच असतात. उदाहरणार्थ एखादी फाईल किंवा प्रोग्राम २० वेळा उघडल्यानंतर हा व्हायरस कार्यान्वित होईल; किंवा ज्या फाईल्सच्या नावाची सुरुवात अमुक-तमुक आद्याक्षरांनी होत असेल. तेवढ्याच फाईल्स इनफेक्ट होतील. किंवा ज्या फाईलची साईझ अमुक तमुक इतक्या प्रमाणात असेल, त्यांनाच हा व्हायरस लागण करील. अशा अनेक पध्दती ह्या प्रकारात येतात.

५. आर्मर्ड व्हायरसेस: 'आर्मर्ड' याचा शब्द कोशातला अर्थ 'चिलखत घातलेला' असा आहे. ह्या प्रकारातले व्हायरस निष्प्रभ करणे किंवा खालसा करणे अवघड असते. यात अँटी-व्हायरस बनविणाराला दाद लागू नये यासाठी खूप आटापिटा केलेला असतो. ह्या प्रयत्नात बरेचदा हे व्हायरस आकाराने मोठे होतात.

६. मल्टीपार्टाइट व्हायरसेस: वर जे जे विविध प्रकार आपण पाहिले

त्यातल्या एकापेक्षा जास्त प्रकारात मोडणारे व्हायरस म्हणजे 'मल्टीपार्टाइट' व्हायरस. म्हणजे तो 'स्टील्थ' ही असेल, म्हणजे लपून बसणाराही असेल आणि 'आर्मर्ड' ही असेल. असे अनेक गुणधर्म धारण करणारे व्हायरस बरेचदा आणखी तापदायक असतात. बरेचदा तो केवळ 'बूट सेक्टर' इनफेक्ट करणारा आहे असं वाटतं. पण त्याने 'बूट' सेक्टरबरोबरच मेमरी, प्रोग्राम फाईल वगैरेवरही हल्ला केलेला असतो.

७. कॅव्हिटी (स्पेसफीलर) व्हायरसेस : लागण लागल्यानंतरी त्या फाईलची साईज पूर्वीइतकीच रहावी, व बदल लक्षात येऊ नये असा ह्या व्हायरसचा प्रयत्न असतो. अर्थात हे फार अवघड असल्याने अशा प्रकारचे व्हायरसेस खूपच कमी आहेत.

८. टनेलींग व्हायरसेस: अँटी-व्हायरस प्रोग्राम संगणकात सतत घडणाऱ्या बदलांवर लक्ष ठेवून असतात. त्यामुळे एखादा व्हायरस घुसतो आहे की काय इकडे त्यांचं लक्ष बारकाईने असतं. अशा अँटी-व्हायरस प्रोग्राम्सचं लक्ष चुकवून हा व्हायरस थेट 'डॉस' व 'बायोस' मध्ये जाऊन सर्वांत खाली राहून लपून बसतो. याला 'टनेलींग' तंत्र म्हणतात. काही अँटी-व्हायरस प्रोग्राम्सही व्हायरस शोधण्यासाठी हे तंत्र वापरतात.

९. कॅमोफ्लेज व्हायरसेस: वर वर दिसायला एक साधे सॉफ्टवेअर वाटेल पण जो आतून व्हायरस असेल असा प्रकार कॅमोफ्लेज व्हायरस. अगदी पूर्वी जेव्हा अँटी-व्हायरस प्रोग्राम्स पुरेसे प्रगत नव्हते तेव्हा हे व्हायरस त्यांना फसवू शकत. पण आता असे व्हायरस प्रोग्राम्स तयार करणे अशक्यप्राय आहे, कारण आताचे अँटी-व्हायरस प्रोग्राम्स खूपच प्रगत आहेत. त्यामुळे ह्यापुढे भविष्यात ह्या प्रकारचे व्हायरसेस कधीच दिसणार नाहीत. असे व्हायरस तयार करण्यासाठी खूपच कष्ट पडतात हेही एक कारण त्यांच्या दुर्मिळतेमागे आहे.

१०. व्हायरस ड्रॉपर: हा प्रकार म्हणजे व्हायरस म्हणता येणार नाही. तो ट्रोजनसारखा प्रकार आहे. व्हायरस ड्रॉपर हा एक स्वतंत्र प्रोग्राम असतो. जेव्हा हा प्रोग्राम उघडून चालवला जातो तेव्हा त्यातून व्हायरस बाहेर पडतो, म्हणजे व्हायरस 'ड्रॉप' केला जातो. म्हणून त्याचे नाव 'व्हायरस ड्रॉपर' असे आहे. 'अँटी व्हायरस' स्कॅनिंगमध्ये बरेचदा ह्या प्रोग्रामच्या आतल्या व्हायरसचे विषारी कोड लक्षात येत नाही. परंतु 'ड्रॉप'

झाल्यानंतर ते लक्षात येते. थोडक्यात, 'ट्रोजन' चाच हा एक मिनी अवतार आहे असं म्हंटल्यास वावगं होणार नाही. 'व्हायरसेस'चे हे झाले प्रमुख प्रकार. छोटे छोटे आणखी निकष धरुन काही जण आणखी काही प्रकार सांगू शकतील. पण कमी-अधिक प्रमाणात हे ह्या वरील प्रकारात बसणारेच असणार. त्यामुळे ती यादी येथे न लांबवता आपण वळू या पुढल्या प्रकरणाकडे ...

व्हायरसचे जन्मदाते

डॉ. ओल (OWL) कडे कसलीही डॉक्टरेट नाही. तो वैद्यकीय डॉक्टरही नाही. तो असच नावामागे डॉक्टर लावतो. खरं तर सध्या तो बेकार आहे. काम शोधतोय. पूर्वी त्याने सेल्समनची नोकरी केलेली आहे. आज तो २१ वर्षांचा आहे. आईबरोबर तो सरकारी भाड्याच्या घरात राहतो. मध्यमवर्गीय जेमतेम म्हणावी अशी त्याची परिस्थिती आहे. डॉ. ओल वयाच्या १२ व्या वर्षापासून व्हायरस लिहितोय. तो उद्योग आजही चालू आहे. एवढ्या वर्षात त्याने २० व्हायरसेस तयार केले. त्याला फोटोग्राफीचा छंद आहे. बागकाम, विशेषतः फळ झाडे लावणे त्याला आवडते. आपल्या निसर्ग छायाचित्रांचा संग्रह त्याला पुढल्या वर्षी प्रसिध्द करायचा आहे. एकूण, डॉ. ओल सध्या तरी दिशाहीन आहे. फक्त व्हायरस तयार करणे ह्या व्यतिरिक्त त्याच्या आयुष्यात निश्चित असं काहीच नाही. डॉ. ओलला व्हायरस लिहावेसे का वाटतात? नेमकं असं काय आहे की हे अनिष्ट, निरुपयोगी काम तो करतो? 'पीसी वर्ल्ड' मासिकाने 'आय.सी.क्यू' म्हणजे ऑनलाईन चॅटच्या माध्यामातून डॉ. ओलची नुकतीच मुलाखत घेतली. 'आय.सी.क्यू' माध्यमातून बोलणारा जगातून नेमका कुठून बोलतोय हे कळणं अशक्य असते. त्यामुळे हॅकर्स किंवा व्हायरसकर्ते ह्या माध्यमातून निर्धास्तपणे मुलाखती देत असतात. डॉ. ओल हा 'फेदर्ड सर्पंट' ह्या गटाचा सदस्य आहे. ह्या गटाचे नाव 'फेदर्ड सर्पंट' म्हणजे पिसे असलेला साप. नावापासूनच विकृती सुरु झाली. ह्या 'फेदर्ड सर्पंट'चे एकूण सात सदस्य आहेत. ते ऑस्ट्रेलिया, अमेरिका व युरोपमधील देशांतले आहेत.

'पीसी वर्ल्ड' मासिकाची डॉ. ओल ह्याच्याशी झालेली ही बातचीत पहा:

- **ह्या व्हायरसशी तुझा संबंध आला कसा? तू लिहिलेला पहिला व्हायरस कोणता?**

डॉ.ओल: एकदा माझ्या फ्लॉपीवर 'स्टोन्ड व्हायरस' आढळला. हा कॉमन असा बूट सेक्टर व्हायरस आहे. कुणीतरी तो न्युझीलंडमध्ये लिहिलाय. मग मी काही पुस्तके वाचली आणि जाणून घेण्याचा प्रयत्न केला की हा व्हायरस कसं काम करतो. नंतर मलाच व्हायरस लिहायला आवडू लागला. पुढे हे पाहण्याचा छंदच जडला की आपण कसे काम (व्हायरस लिहिण्याचे) करतोय आणि इतर कसे काम करताहेत.

- **पण, पहिला व्हायरस तू कोणता आणि कधी लिहिलास?**

डॉ. ओल: पहिला व्हायरस मी लिहिला त्याचे नाव Facade. तो खरं म्हणजे मी माझ्या मित्रासाठी लिहिला. त्याला तो हवा होता. त्याच्या वाढदिवसाच्या दिवशी म्हणजे २७ फेब्रुवारी रोजी हार्ड डिस्कचा विध्वंस करणारा हा व्हायरस होता. त्याला तो मोठ्या कंपन्यांच्या मॅनेजर्ससाठी हवा होता. मॅनेजर्सना कामगारांची बिल्कुल कदर नसते असा त्याचा रोष होता. मी तयार केलेला हा व्हायरस 'स्टील्थ' प्रकारचा होता. माझ्या मित्राने तो कधी वापरला का नाही हे माहीत नाही. पण वर्ष-दोन वर्षांनी तो अमेरिकेतल्या एका विद्यापीठात गेला तेथे तो शांतपणे काढून टाकला गेला. तेथे तो कुणी पसरवला हे मला माहीत नाही.

- **तुझ्या मित्राचा हेतू तो त्याच्या कंपनीत पसरवण्याचा होता?**

डॉ. ओल: मला माहीत नाही. त्याच्या वाढदिवसाला त्याला काहीतरी वेगळं आणि चांगलं हवं होतं. बसं.

- **आता पर्यंत तू असे किती व्हायरसेस पसरवले आहेस?**

डॉ. ओल: मी स्वतः एकही नाही. मला जर व्हायरस पसरवायचा असता तर त्यासाठी खूप काम करावं लागलं असतं. छोटे व्हायरस चटकन तयार होतात. अर्ध्या क्षणात ते मरतात. ते काहीच करु शकत नाहीत. काहीतरी जबरदस्त करणारा आणि आपली छाप दीर्घकाळ ठेवून जाणारा व्हायरस

मला तयार करावा लागला असता. पण मला इतर कामे होती म्हणून हे करता आलं नाही. मी केलेला व्हायरस चटकन संपून विसरला गेला असता तर मला वाईट वाटलं असतं.

- **तू म्हणतोस की चटकन संपून विसरला असता तर तुला वाईट वाटलं असतं. तुला नेमकं काय म्हणायचय?**

डॉ. ओल: 'व्हायरस'चे डिझाईन तयार करताना खूप विचार करावा लागतो. एखाद्या छोट्या मुलाला शिकवल्याप्रमाणे त्याच्याकडे पहावं लागतं. मग तुम्ही त्याच्यात गुंतून जाता. जर तो व्हायरस सगळीकडे पसरला आणि त्याची चर्चा जगभर झाली तर तुम्हाला अभिमान वाटतो. कष्टाचं चीज झाल्यासारखं वाटतं. जर तो अल्पायुषी ठरला आणि मच्छरासारखा मेला तर तुम्हाला दु:ख होतं. जर त्याला जिवंत पकडून 'झू' मध्ये प्रदर्शनार्थ ठेवलं गेलं तर फारच वाईट.

- **जर तू स्वत: व्हायरस पसरवत नाहीस म्हणतोस, तर मग ते तू लिहितोस कशासाठी?**

डॉ. ओल: मी व्हायरस लिहितो याचे कारण तंत्रज्ञानातील ते प्रत्येक प्रगतीचे पाऊल असते. त्याचा मला अभिमान वाटतो. तो जर डिटेक्ट न होता पसरत राहिला तर त्याचा अर्थ तुम्ही खूपच प्रगती साधलेली आहे असा होतो. असे तंत्रज्ञान तुम्ही विकूही शकता.

- **तुझं नाव 'ओल' म्हणजे घुबड असं आहे. ते नाव तू का घेतलस. घुबड तर कुरुप आणि अभद्र असतं.**

डॉ. ओल: छे छे. घुबडं खूप क्यूट असतात. घुबडं खूनशीही असतात. पण तो तर निसर्गाचाच न्याय आहे. पण घुबडं ही बुध्दीमत्तेचं प्रतीक असतात हे लक्षात घ्या.

- **बरं. दुसरी गोष्ट. तू असुरी समाधानासाठी व्हायरस लिहितोस असं म्हंटल तर?**

डॉ. ओल: हे बघा मी ओरडून सांगितलं की मी हुशार प्रोग्रामर आहे. मी बुध्दीमान आहे. मला काम द्या. तर कोणी देईल! म्हणतील, असे हजारो पडलेत. पण मी म्हंटलं की 'फेकेड' व्हायरस तयार करणारा तो मीच.

तर लोक आदराने पाहतील. माझ्याकडून तंत्रज्ञान विकत घेतील. मला प्रश्न विचारायला घाबरतील. नाहीतर इंटरव्यूमध्ये प्रश्न विचारून विचारुन माझा कचरा करतील. जेवढा व्हायरस मोठा, तेवढा माणूस मोठा.

- **पण तुला असं वाटत नाही का की तुमच्या व्हायरसेसमुळे निरपराध लोकांना त्रास होतो. त्यांचा काहीही दोष नसताना त्यांचे नुकसान होते, आणि त्याला जबाबदार तुम्ही लोक असता?**

डॉ. ओल: मी असं कुठे म्हणालो की नुकसानीसाठी मी व्हायरस बनवतो? मी एवढच म्हणालो की माझा व्हायरस हा प्रदीर्घकाळ जगावा आणि त्याची चर्चा व्हावी. व्हायरसमुळे स्वत:चं नुकसान करुन घेणारे लोक स्वत:च त्याला जबाबदार असतात. हे म्हणजे मायक्रोसॉफ्टने तुम्हाला 'फॉर्म्याट' कमांड दिली आहे. ती तुम्ही अपघाताने वापरुन स्वत:ची हार्ड डिस्क पुसून टाकलीत तर त्याला काय मायक्रोसॉफ्टला जबाबदार धरणार? मी व्हायरस बनवला. पण इतरांनी तो पसरवला. त्यांना जबाबदार धरा.

- **पण 'फेकेड' सारख्या व्हायरसमुळे ज्याचं नुकसान झालं, ज्याला त्रास झाला, त्याबद्दल तुला सहानुभूती नाही वाटत?**

डॉ. ओल: सहानुभूती? येस, वाटते. पण जबाबदारी नाही घेणार त्याची. हं जर मी व्हायरस तयार केला; तुमच्या कॉंप्युटरमध्ये मी स्वत: तो पसरवला आणि तुमचे नुकसान केले तर ती माझी जबाबदारी राहील. त्याला मी जबाबदार. काड्यापेटीतील काडीने तुम्ही घर पेटवलेत तर काड्यापेट्यांची कंपनी कशी काय जबाबदारी घेईल?

डॉ. ओल ह्या २१ वर्षीय व्हायरस निर्मात्याचे तत्वज्ञान पाहिलेत? तुम्हाला बुध्दीमत्ता आणि दिशाहीनता हातात हात घालून जाताना दिसतील. हा तरुण त्याची बुध्दीमत्ता चुकीच्या दिशेला वळवून चाललाय. दूध बालकाच्या मुखात पडायला हवं. पण हे लोक ते गटारात ओतत आहेत. त्याचे काहीतरी तत्वज्ञान सांगताहेत असा प्रकार आहे.

आय.बी.एम. कंपनीने व्हायरसच्या अशा जन्मदात्यांची मनोधारणा जाणून घेण्यासाठी बरेच संशोधन केले आहे. त्यांचेसाठी संशोधन करणारे सारा गॉर्डन आणि थॉमस वॅटसन हे दोन संशोधक म्हणतात, ''कुठेतरी

असंतुष्टता राहिलेले हे अल्पवयीन बुध्दीमान तरुण असतात. कुणाच्या आयुष्यात निरर्थकता असते, किंवा कोणाला गर्लफ्रेंड नसते, कुणी कुरुप असतो. वगैरे.'' सारा गॉर्डन हिने आजपर्यंत १०० पेक्षा जास्त व्हायरस रायटर्सच्या मुलाखती घेतल्या आहेत. त्यांचे मानसशास्त्र समजावून घेण्याचा प्रयत्न तिने जेवढा केलाय तेवढा अन्य कुणी क्वचितच केला असेल. एका व्हायरस रायटरने तर आपली सर्वनिर्मिती (सर्व व्हायरसेस) तिला समर्पित केले आहेत. ती म्हणते की ''खूप व्हायरस रायटर्स असे असतात की जे केवळ थ्रील म्हणून असे कोडस् लिहितात. त्या दूरगामी परिणामांची त्यांना नीट कल्पनाही नसते बरेचदा.''

''आता बरेच तरुण व टीनेजर्स हॅकींगकडे वळले आहेत, आणि ते 'व्हायरस लिहिणे' हे कमी प्रतीचे मानू लागले आहेत'' असे सांगून सारा गॉर्डन म्हणते की '' आता व्हायरस लिहिणे म्हणजे बहुधा पूर्वीचे व्हायरस सुधारुन किंवा त्यात आणखी भर घालून ते सोडणे. आता फार थोडी ओरिजिनॅलिटी व्हायरस रायटींगमध्ये उरली आहे. ह्या उलट हॅकींगमध्ये भरपूर हुशारी, बुध्दी आणि चातुर्य पणाला लागते. बुध्दीमान किशोर व तरुण वयीन व्यक्तींना ते अधिक आकर्षित करते. बऱ्याच मुलीही व्हायरस लिहिणाऱ्या आहेत.''

आणखी एक महत्वाचा मुद्दा सारा गॉर्डन सांगते. ती म्हणते की ''हॅकींग हा नियंत्रणाचा भाग आहे. यश मिळाल्यानंतर तुमच्या हातात नियंत्रण येते त्यात सत्तेचे समाधान असते. पण ह्या उलट व्हायरस बनला की तो तुमच्या ताब्यातून दूर जातो. त्याच्या पसरण्यावर वा यश-अपयशावर तुमचे कसलेही नियंत्रण रहात नाही.''

''एके काळी व्हायरस रायटर्सचे वय १४ ते १७ हे असे. आता ते २५ ते ३२ आहे.'' असे गॉर्डन म्हणते. 'मेलिसा' व्हायरस लिहिल्याचा आरोपी डेव्हिड स्मिथ हा ३० वर्षांचा आहे.''

'इंटरनेट'मुळे व 'ई मेल' सुविधेमुळे व्हायरस कोडींग एकमेकांना पाठवणे, त्यावर चॅटमधून चर्चा करणे सोपे झाले आहे. बऱ्याच जणांनी व्हायरस बनविण्याची ट्युटोरियल्स आपल्या वेबसाईटस्वर ठेवली आहेत. काहींनी तर व्हायरस तयार करण्याचे सोपे व तयार प्रोग्रामचं वेबसाईटवर डाऊनलोड

करण्यासाठी ठेवले आहेत. ॲना कॉर्निकोवा हा २००१ च्या फेब्रुवारीत आलेला 'ई मेल ॲटॅचमेंट' मधून पसरणारा व्हायरस अशाच तयार टूलचा वापर करुन जगात पसरवला होता. त्यामुळे आता हा एक पोरखेळ बनून गेल्यासारखा वाटतो.

''काही मुली आपल्या बॉयफ्रेंडस्ना खूष करण्यासाठी मेहनत घेऊन व्हायरस बनवितात. यामुळे त्या बॉयफ्रेंडच्या सर्कलमध्ये ती सामावली जाईल अशी तिची समजूत असते'' असेही सारा गॉर्डन हिने म्हंटले आहे. ''मात्र बरेच व्हायरसेस हे इतके ढिसाळपणे कोड केलेले असतात आणि त्यात इतके दोष असतात की त्यांच्यात पसरण्याची ताकदच नसते.'' हे आपले निरीक्षण सारा गॉर्डनने नोंदवले आहे.

इव्हल नावाच्या एका व्हायरस रायटरची कथा सारा गॉर्डनने सांगितली आहे. ह्या इव्हलने बरेच व्हायरस बनवले आणि सोडले. एकदा मात्र तो स्वत:च अशा एका व्हायरसचा बळी ठरला. इव्हलचाच खूप डेटा पुसला गेला. इव्हलने त्या डेटासाठी खूप परिश्रम केलेले होते. इव्हल म्हणतो '' तो प्रकार घडल्यानंतर माझ्या डोक्यात धोंडा पडल्याप्रमाणे झाले. मी स्वत:लाच विचारले की तास न तास मेहनत करुन जमा केलेला डेटा पुसण्याचा काय अधिकार आहे कोणाला? माझ्या व्हायरसेसनीही अशीच कुणाची तरी मेहनत पाण्यात घालवली असणार. ह्या प्रकारानंतर मी व्हायरस लिहिणे सोडले.''

व्हायरसचे जन्मदाते आणि त्यांचे मन व त्यामधील गुंतागुंत ही अशी आहे. किशोरवयातल्या कृष्णाच्या गोष्टी आपण पाहतो, वाचतो. दूरदर्शनवरही त्या दिसतात. वृष्ण झाडावर बसलेला असतो. बरोबर मित्र असतात. एकीकडे नदीवरुन पाणी भरुन गवळणी मातीचे घडे डोक्यावर ठेवून चाललेल्या असतात. ह्या गवळणींनी मेहनतीने पाणी भरलेले असते. पदरचे चवल टाकून घडे खरेदी केलेले असतात. पण कृष्ण झाडावरुन त्या भरलेल्या घड्यांवर खडे मारतो. घडा फुटतो. पाणी सांडते. गवळणीची मेहनत पाण्यात जाते. कृष्ण आणि त्याचे सहकारी हसू लागतात. त्यांना यात मौज वाटते. कृष्ण आणि त्याचे सहकारी आणि हे अल्पवयीन व्हायरस रायटर यांच्यात काही साम्य तुम्हाला दिसते का?

हा मूळ मानवी स्वभाव जर पुराणकाळापासून चालत आला आहे तर

तो कसा थांबणार? काल व्हायरस धुमाकूळ घालत होते, आज हॅकर्स धुमाकूळ घालताहेत. उद्या?? उद्याही असाच काहीतरी नवा प्रकार दिसेल. शेवटी 'माणूस' हा चार अंगुळे वर उरतच असतो. त्यावर माणसाचा काय इलाज चालणार?

फॉल्स अलार्मस्

व्हायरस म्हणजे नेमकं काय, 'व्हायरस' लागल्याची लक्षणे कोणती, किती प्रकारचे व्हायरस प्रचारात आहेत वगैरे माहिती आपण पूर्वीच्या प्रकरणांतून पाहिली आहे. व्हायरस कसा आत येतो, कोणत्या मार्गाने येतो, नेमकं कसं काम करतो आणि मूळातच तो येऊ नये यासाठी काय करावं हेही आपण काही प्रकरणांमध्ये वाचलेलं आहे. 'व्हायरस' हे तयार होतच राहणार आणि त्यावर प्रत्येक वेळी नीट तपासूनच उपाय शोधावा लागणार हेही आता आपल्याला माहीत आहे. आपल्याला आता चार प्रमुख गोष्टी हव्या आहेत:

१) मूळातच ज्या क्षणी प्रचलित व्हायरस प्रवेश करण्याचा प्रयत्न करील त्याच क्षणी त्याला दारातच अडवून त्याचा प्रवेश होत आहे असा पूर्वसंदेश आपल्याला मिळायला हवा.

२) नीट काळजी घेऊनही किंवा अनवधानाने झालेल्या चुकीमुळे वगैरे समजा एखादा प्रचलित व्हायरस आत शिरलाच तर त्याची बकोट पकडून त्याला मूळासकट बाहेर फेकून देणारी यंत्रणा आपल्याला हवी आहे.

३) अगदी नवे, नव्या प्रकारचे म्हणजे अज्ञात असे व्हायरस आले तर त्याचीही पूर्वसुचना मिळायला हवी.

४) ज्या व्हायरसवर उपाय सापडलेला नाही, किंवा त्याला बकोट पकडून बाहेर काढता येणे अशक्य आहे अशा बहुधा नव्या किंवा अज्ञात व्हायरसला आपल्याच काँप्युटरवर एका रिंगणात कोंडून त्याची विघातक

शक्ती आणि प्रवृत्ती आपल्याला बंदिस्त करता यायला हवी.

आपल्या ह्या चार मागण्या आजचे प्रसिध्द 'अँटी व्हायरस प्रोग्राम्स' बऱ्याच प्रमाणात पूर्ण करीत आहेत. मी मुद्दाम 'बऱ्याच प्रमाणात' असा शब्दप्रयोग करतो आहे; आणि त्याचे कारण म्हणजे कोणताही 'अँटी व्हायरस प्रोग्राम' हा पूर्ण आणि बिनचूक असू शकतच नाही. कारण सरळ आहे, व्हायरसचा धोका क्षणोक्षणी आहे, आणि व्हायरसचे स्वरुप कोणत्या क्षणी बदलेल हे कुणीच सांगू शकत नाही. म्हणजेच कोणताही अँटी व्हायरस प्रोग्राम हा आपण १०० टक्के परफेक्ट आहोत असं स्वत:बद्दल म्हणू शकत नाही. अर्थात, जाहिरात करताना त्यांना तसं म्हणावं लागेल ही गोष्ट वेगळी. जाहिरातीतले दिसणे आणि प्रत्यक्षातले असणे यात खूपदा फरक असतो हे आपण लहानपणापासून जाणून असतो.

तर, मुद्दा हा की आपल्या उपरोल्लेखित चार मागण्या पूर्ण करणारे 'नॉर्टन अँटीव्हायरस', 'एफ. प्रॉट', मॅक फी अँटीव्हायरस वगैरेंसारखे अँटी व्हायरस प्रोग्राम खूप नावाजलेले असले, खूप लोकप्रिय असले आणि खूप प्रमाणात आपल्याला ते संरक्षण देत असले तरी त्यांच्या देखत एखादा व्हायरस आपल्या काँप्युटरच्या पाठीत खंजीर खूपसू शकतो. म्हणजेच साधं उदाहरण देऊन सांगायचं तर अगदी ब्लॅक कॅट कमांडो असले आणि अगदी झेड प्लस सुरक्षा असली तरी अनपेक्षितपणे नेत्यावर खूनी हल्ला होऊ शकतो. किंवा वॉचमन असूनही चोरी होऊ शकते. असे होते म्हणून कुणी वॉचमनला काढून टाकत नाहीत. किंवा ''झेड-प्लस' संरक्षणाचा उपयोग नाही'' असं म्हणत नाही. इमारतीला वॉचमन असला तरी आपल्या घराला कुलूप लावून आपण आणखी काळजी घेतच असतो.

तात्पर्य,'अँटी व्हायरस प्रोग्राम' सारखा एक वॉचमन एक 'झेड-प्लस' सारखी यंत्रणा प्रत्येक संगणकाला असायलाच हवी. ती खूपच उपयुक्त आहे. पण हे 'अँटी व्हायरस प्रोग्राम्स' नेमक्या कोणत्या प्रकारच्या चुका करतात? ते संदेश देताना चुकतात. याला 'फॉल्स अलार्मस्' असं म्हंटलं जातं. ह्या चुका दोन प्रकारच्या असतात.

दोन प्रकारच्या चुका

१) पहिल्या प्रकाराला म्हणतात 'फॉल्स पॉझीटीव्ह' (False Positive).

आपण मराठीत त्याला 'चुकीचा भितीयुक्त इशारा' असे म्हणू या. ह्या प्रकारात तुम्ही 'अँटी व्हायरस प्रोग्राम' वापरुन व्हायरस आहे का याची चाचणी (स्कॅनिंग) करता आणि चाचणी पूर्ण करुन तो सांगतो की 'अमुक तमुक' प्रकारचा व्हायरस शिरलेला आहे. ह्या इशाऱ्यात भिती असते. पण प्रत्यक्षात तसे नसते. काहीतरी वेगळ्याच गोष्टीला तो व्हायरस समजलेला असतो. आणि आपल्याला चुकीचा भितीयुक्त इशारा देत असतो.

२) दुसरी चूक म्हणजे 'फॉल्स निगेटीव्ह' (False negative). आपण मराठीत म्हणू या 'चुकीच्या निश्चिंतीचा इशारा' किंवा 'चुकीचा हिरवा सिग्नल'. तुमच्या एव्हाना लक्षात आलच असेल की 'अँटी व्हायरस प्रोग्राम' ने जिथे रेड सिग्नल देऊन 'व्हायरस' चा इशारा द्यायला हवा होता तिथे तो न देता सारे 'आलबेल' असल्याची चुकीची माहिती त्याने देणे म्हणजे फॉल्स निगेटिव्ह.

वरील दोन्ही प्रकारात 'फॉल्स निगेटीव्ह' ही चूक फार महागात पडणारी असते. एखाद्या फाईलमध्ये व्हायरस नाही हे कळल्यानंतर आपण ती उघडली आणि त्यातून महाभयंकर व्हायरस बाहेर पडून त्याने कॉंप्युटरचा डेटा गिळून टाकला की सारेच संपले. चुकीचा हिरवा सिग्नल देणारा 'अँटी व्हायरस प्रोग्राम' सुध्दा तो गिळून टाकू शकतो (अर्थात 'डिलीट' करतो किंवा 'करप्ट' करतो).

'फॉल्स पॉझीटीव्ह' हा पहिला प्रकार त्या मानाने कमी तापदायक आहे. कारण तो आपल्याला अस्वस्थ करीत असला आणि गोंधळून टाकत असला तरी प्रत्यक्षात नुकसान काहीच करीत नसतो. 'दगडापेक्षा वीट मऊ' म्हणता येईल एवढाच काय तो फरक दोघांमध्ये आहे.

डॉ. फ्रेड कोहेनचा संदेश

डॉ. फ्रेड कोहेन हे कॉंप्युटर व्हायरस रिसर्चच्या क्षेत्रातील एक फार मोठे नाव आहे. डॉ कोहेन यांनीच १९८३ मध्ये 'व्हायरस' हे नाव अशा प्रोग्राम्सना प्रथम दिले आणि ते नंतर प्रचारात येऊन रुढ झाले एवढे सांगितले तरी त्यांच्या संशोधनाचे मोल आपल्या लक्षात येईल. डॉ. कोहेन यांनी ह्याच विषयावर आपली Ph.D. मिळवली आहे. ते म्हणतात ''प्रत्येक 'व्हायरस डिटेक्शन प्रोग्राम' मध्ये अगणित 'फॉल्स पॉझीटीव्ह'

आणि अगणित 'फॉल्स निगेटीव्ह' हे असणारच.''

आजकाल जे सुधारित 'व्हायरस स्कॅनिंग प्रोग्राम' आहेत त्यात 'फॉल्स पॉझीटीव्ह' असण्याची शक्यता खूप कमी असते. 'स्कॅनर प्रोग्राम' जेव्हा 'बूट सेक्टर' किंवा 'फाईल्स' वगैरे स्कॅन करुन व्हायरस आहे का हे तपासत असतो तेव्हा तो त्याला माहीत असलेले विशिष्ट व्हायरसेसचे कोडस् शोधत असतो. जर तशाच प्रकारचे कोडस् जर एखाद्या साध्या फाईलमध्ये असतील तर त्याला वाटेल की तिथे व्हायरस आहे. त्यामुळे व्हायरस स्कॅनिंग (शोधण्याचे तंत्र) करताना तपासणीसाठी जे कोडस् ठरवले जातात ते महत्वाचे ठरतात. आजमितीस 'फॉल्स पीझीटीव्ह' ची शक्यता खूप कमी आहे एवढं सांगितलं तरी पुरे आहे. अर्थात त्यासाठी तुमचा अँटी व्हायरस प्रोग्राम हा आजच्या तारखेपर्यंत अद्ययावत हवा हे लक्षात घ्या.

आधुनिक काळातील 'अँटी व्हायरस प्रोग्राम्स' आणि 'व्हायरस' यांच्यात खरे तर रात्रंदिवस एक युध्दच चाललेले असते. नवा व्हायरस आला की काही क्षणात त्यावर उपाय देण्याची स्पर्धा असते. तर दुसरीकडे व्हायरस तयार करणारे प्रयत्न करीत असतात की अँटी-व्हायरस प्रोग्राम्सना त्यांनी सही सही चकवावे. ह्या प्रयत्नात हे 'फॉल्स अलार्मस्' येण्याची शक्यता असते.

काही पारिभाषिक शब्द व शब्दप्रयोग

कॉंप्युटर व्हायरस रायटींग ही प्रोग्रॅमिंगचीच एक शाखा म्हणावी लागेल. तिचा विकास होता होता काही विशिष्ट इंग्रजी शब्द व शब्दप्रयोग रुढ झाले. ह्या शब्दांना विशिष्ट अर्थ आणि पार्श्वभूमी असते ती धरुनच ते वापरले जातात. असे काही शब्द, शब्दप्रयोग आणि त्यांचे अर्थ इथे दिले आहेत:

Active X

Active X हे छोटे छोटे आणि स्वतंत्र प्रोग्राम्सच असतात. ते मायक्रोसॉफ्टच्या Component Object Model (COM) पध्दतीवर आधारलेले असतात. सॉफ्टवेअर्समध्ये हे छोटे तयार प्रोग्राम्स घातले की त्या सॉफ्टवेअरला ते सक्रियता (functionality) देतात आणि एका बाजूला तो त्या सॉफ्टवेअरचाच भाग वाटतो. इंटरनेटवर Active X हे वेब पेजेसवर टाकता येतात. जो ब्राऊझर Active X युक्त असतो तो वेब पेज उघडताच Active X क्रिया डाऊनलोड करुन एखाद्या प्रोग्रामप्रमाणे क्रिया घडवतो. Active X Control हा संपूर्ण सिस्टमवरही नियंत्रण मिळवू शकतो. मात्र क्वचित काही Active X Control हे अनिष्ट वा malicious असू शकतात. त्यांच्यापासून सावध रहायला हवे.

Algorithm

एखादा तार्किक क्रम वा गणित करण्यासाठी विशिष्ट क्रियांचा (steps) क्रम आवश्यक असतो. त्याला Algorithm म्हणतात. डिजिटल सीग्नेचर्स,

डेटा फाईल डिक्रीप्ट वा एनक्रीप्ट करण्यासाठी काही विशिष्ट क्रिप्टोग्राफीक अल्गोरीथम वापरले जातात.

Anti-antivirus virus

जो व्हायरस अँटी व्हायरस प्रोग्रामवर हल्ला करुन ते निष्प्रभ करण्याचा प्रयत्न करतो त्याला Anti-antivirus virus असे म्हणतात.

Attack

सिस्टम (संगणक) सिक्युरिटीला नामोहरम करण्याचा वा ती ओलांडण्याचा प्रयत्न. ॲटॅक हा ॲक्टीव्ह (सक्रिय) किंवा पॅसीव्ह (निष्क्रिय) असू शकतो. ॲक्टीव्ह ॲटॅक हा डेटा पुसून टाकतो वा त्याचा विध्वंस करतो. पॅसीव्ह ॲटॅक डेटा जराही न बदलता तो फक्त वाचतो. संगणकशास्त्रात वेगवेगळे 'ॲटॅक' सांगितले जातात. त्यात 'ब्रूट फोर्स ॲटॅक', 'पासवर्ड ॲटॅक', 'पासवर्ड स्नीफींग', 'डिनायल ऑफ सर्व्हिस' वगैरेंचा समावेश आहे.

Back Door

प्रोग्राम तयार करताना प्रोग्रामर हे त्यात स्वत:साठी काही विशेषाधिकाराचा दरवाजा ठेवतात. येथून फक्त प्रोगामरच आत जाऊ शकतो. इतरांना हा दरवाजा कळतही नाही. हा प्रवेश प्रोग्राममधील दोष वगैरे दूर करण्यासाठी असतो. मात्र जर हॅकर्सनी हा दरवाजा शोधला तर प्रकरण अवघड असते. येथून घुसून दोष दूर करण्याऐवजी दोष निर्माण करण्याची प्रक्रिया मग सुरु होऊ शकते.

Back Orifice

'बॅक ओरिफाईस' हा प्रोग्राम The Cult of the Dead Cow (cDc) ने तयार केला आहे. हा व्हायरस नव्हे. ते एक रिमोट ॲडमिनीस्ट्रेशन टूल आहे. दूर राहून संगणकावर ताबा ठेवण्यासाठीची ती लबाडी आहे. जर हॅकरने ते इन्स्टॉल केले तर त्याच्याकडे संपूर्ण संगणकाचा/नेटवर्कचा ताबा राहू शकतो. पासवर्डस् आणि गुप्त डेटा त्याला मिळू शकतो व हॅकरला तो गुपचुप विशिष्ट 'ई मेल' पत्त्यावर पाठवता येतो. 'बॅक ओरिफाईस' हा विस्तारक्षम प्रोग्राम आहे. इतर प्रोग्रामर तो वाढवू शकतात वा बदलू शकतात.

Background Scanning

काही अँटी व्हायरस प्रोग्राम्समध्ये याची सोय असते. एकीकडे फाईल उघडताना वा बंद होताना वा चालविली जाताना किंवा तिची निर्मिती होत असताना अँटी व्हायरस प्रोग्राम तिचेही व्हायरस तपासण्यासाठी स्कॅनिंग करु शकतो. हे स्कॅनिंग म्हणजे व्हायरस स्कॅनिंग. ज्या अँटी व्हायरस प्रोग्राम्सना अशी सोय नसते तिथे सर्व फाईल्स बंद केल्यानंतरच स्कॅनिंग करता येते.

Bimodal virus

दोन क्रियांचा व्हायरस. उदाहरणार्थ असा व्हायरस की जो बूट रेकॉर्डस् देखील बिघडवतो व फाईल्सनाही लागण करतो.

BIOS

Basic Input/Output System. ऑपरेटींग सिस्टमचा भाग. BIOS म्हणजे सूक्ष्म प्रोग्राम्सचा एक संचच असतो. काँप्युटर चालू होताना सिस्टम डिस्ककडे जाण्यापूर्वी तो ह्या संचाचा वापर करुन चालू होतो. BIOS हा 'रीड ओन्ली मेमरी' त असतो आणि तिथे त्याला अढळपद असते.

Brute Force Attack

पासवर्ड म्हणजे काय तर आपल्या की बोर्ड वरील बटणे दाबण्याचा एक क्रम. अशा सर्व बटणांचे सर्व संभाव्य क्रम तपासले तर कुठे ना कुठे पासवर्ड हा असणारच. असे सर्व क्रम एक एक करीत शोधून पासवर्ड मिळवणे याला Brute Force Attack म्हणतात.

Bug

एखाद्या सॉफ्टवेअर वा प्रोग्राममध्ये चुकून राहून गेलेला दोष. हा दोष अनवधानाने राहिलेला असतो, तो ठेवण्यामागे काही उद्देश नसतो.

Cavity Virus

व्हायरस ज्या फाईलमध्ये शिरतो त्या फाईलची सक्रियता न घालवता व तिच्या आकारमानात (Size) वाढ न करता तिथे जागा करुन तो राहतो. त्याला Cavity Virus म्हणतात. फाईलची साईज वाढल्यास तेथे व्हायरस

असल्याचे कळते. ते कळू नये म्हणून व्हायरस ही व्यवस्था करीत असतो.

Check Sum

फाईलच्या गुणधर्मावरुन तिचा एक क्रमांक ठरतो. फाईलमध्ये काकणभर जरी बदल झाला तरी तिचा Check Sum बदलतो. 'चेक सम' बदललेल्या फाईलमध्ये व्हायरस असण्याची शक्यता असते.

Cluster Virus

संगणकाच्या डिरेक्टरीतील टेबल एन्ट्रीज हा व्हायरस अशा प्रकारे बदलतो की त्या डिरेक्टरीतील इतर प्रोग्राम चालू होण्याच्या अगोदर व्हायरस आपला प्रोग्राम चालू करतो. व्हायरसचे कोड केवळ एकाच ठिकाणी असते. मात्र कोणत्याही प्रोग्रामवर क्लीक केले तरी व्हायरस प्रोग्रामच रन होतो. हा व्हायरस डिरेक्टरी टेबल बदलत असल्याने असे भासते की डिरेक्टरीतील प्रत्येक प्रोग्राममध्ये त्याची लागण झाली आहे.

Cold Boot

काँप्युटर पॉवर ऑफ करुन म्हणजे इलेक्ट्रीकचे बटण पूर्ण बंद करुन पुन्हा चालू करणे याला 'कोल्ड बूट' असे म्हणतात. बरेचदा 'कोल्ड बूट' करुन नंतर 'रेस्क्यू डिस्क' टाकून व्हायरस काढावा लागतो.

Warm Boot

काँप्युटरची पॉवर ऑफ न करता, केवळ Control+Alt+Delete ही बटणे दाबून काँप्युटर चालू करणे याला वॉर्म बूट म्हणतात.

Compromise

Authorisation (पासवर्ड व लॉगिन वापरुन प्रवेश) नसताना डेटा (माहिती) देणे-घेणे वा उघड करणे.

Cookie

काँप्युटरच्या हार्ड डिस्कवर एका फाईलमध्ये विशिष्ट टेक्स्ट मॅटर (शब्द) ठेवून ते वापरणे. वेब साईटस्‌च असे मॅटर ठेवतात आणि युजर जेव्हा पुन्हा त्या वेब साईटवर जातो तेव्हा ह्या मॅटरचा (कुकीचा) उपयोग करतात. उदाहरणार्थ विशिष्ट वेबसाईटवर जर 'लॉगिन नेम' टाईप करावे लागत

असेल तर वेब साईट स्वत:च ते कुकीतून घेते. मग युजरला ते टाईप करावे लागत नाही. 'शॉपिंग कार्ड' ची माहिती, 'युजर प्रेफरन्सेस' वगैरेसाठी तसेच वेब साईट कस्टमाईज करण्याच्या प्रक्रियेत कुकी भूमिका बजावत असते.

Denial of Service (DoS)

संगणकावर वा सिस्टमवर असा ॲटॅक की ज्यामुळे अधिकृत लॉगिन व पासवर्ड असणारांना त्यांचा अधिकार नाकारला जातो. सामान्यत: हॅकर्स सर्व्हर इतका ओव्हरलोड करतात की त्या गर्दीमुळे खरोखर वापरणारांना तिथे प्रवेश मिळत नाही, किंवा मिळायला विलंब होतो. काही वेळा सर्व्हरवरील डेटा बदलल्याने वा त्याचा विध्वंस केल्यानेही Denial of Service ची समस्या उद्‌भवू शकते.

Direct Action Virus

डायरेक्ट ॲक्शन व्हायरस हा स्वत: त्वरित मेमरीत जातो, तेथून अन्य फाईल्समध्ये शिरतो व शेवटी मेमरीतून बाहेर पडतो.

File Viruses

सामान्यत: Com व EXE ह्या दोन प्रकारच्या फाईल्सना फाईल व्हायरसेस लागण करतात. मात्र SYS, DRV, BIN, OVL आणि OVY ह्या प्रकारच्या फाईल्सनाही ते लागण करु शकतात.

Firewall

नेटवर्कमध्ये असणाऱ्या काँप्युटर्सबरोबर बाहेरील काँप्युटर्सचा थेट संपर्क होणे 'फायरवॉल' मुळे प्रतिबंधित होते. बाहेरील काँप्युटर्स व नेटवर्कवरील काँप्युटर यांच्यात संपर्क होताना फायरवॉल काटेरी तारांच्या कुंपणासारखे काम करते. येथूनच प्रवेश होताना द्यावयाची माहिती देऊन जावे लागते. फायरवॉल प्रोग्राम नेटवर्कमध्ये प्रवेश देताना तो काळजीपूर्वक तपासूनच देतो. अन्यथा प्रवेश नाकारतो. कोणाला कसा व कुठपर्यंत प्रवेश द्यायचा याचे नियम फायरवॉलला आखून दिले की ती त्यानुसार काम करते.

Hijacking

संगणकावर काम चाललेले असताना मध्येच येऊन व्यत्यय आणणे व

त्या चाललेल्या कामात हस्तक्षेप करणे याला हायजॅकींग म्हणतात. विधीवत संगणक वापरणारा कधी मध्येच संगणक असुरक्षित सोडून दुसरीकडे गेला तर त्याच्या अनुपस्थितीत 'हायजॅकींग' होऊ शकते. खेरीज इंटरनेटच्या माध्यमातूनही रिमोट हायजॅकींग शक्य असते.

Hole

आपण कायद्यात फट राहणे असे म्हणतो. तेव्हा जो अर्थ अपेक्षित असतो तसाच अर्थ प्रोग्राम वा सॉफ्टवेअरच्या सुरक्षेत राहिल्यास लावता येईल. 'Hole' हा शब्द सामान्यतः 'Security Hole' (सुरक्षिततेतील फट) ह्या अर्थानेच वापरला जातो.

In the wild

प्राणी दोन प्रकारचे असतात. एक, प्राणी संग्रहालयातले किंवा 'झू'मधले आणि, दुसरे, जंगलात मुक्त असलेले. जे व्हायरस बाहेर पसरलेले आहेत त्यांना 'In the Wild' असा शब्दप्रयोग वापरला जातो. थोडक्यात प्रयोगशाळेच्या बाहेर पडून व्हायरसने लागण केली आहे हे सिध्द झाले की तो 'Wild List' मध्ये जातो.

Zoo

'व्हायरसेस' चा प्रयोगशाळेतील संग्रह. तो मुख्यत्वे संशोधकांसाठी असतो.

Zoo Virus

संशोधकांनी तयार केलेला हा व्हायरस केवळ अभ्यासासाठी असतो. तो संशोधन गृहाच्या बाहेर कधीही गेलेला नसतो, वा जगात कुठल्याही संगणकाला त्याची लागण कधीही झालेली नसते.

Key

'विंडोज' ह्या ऑपरेटींग सिस्टमचे व त्या अंतर्गत चालणाऱ्या प्रोग्राम्सचे नियंत्रण करण्यासाठी 'विंडोज'मध्ये 'रजिस्ट्री' नावाचा एक विभाग असतो. तिथे अनेक गोष्टींची नोंद असते. ह्या नोंदीनुसार 'विंडोज' व अन्य प्रोग्राम्स चालतात. जेव्हा नवा एखादा प्रोग्राम संगणकात टाकला जातो तेव्हा त्याच्या

नोंदी रजिस्ट्रीत होतात. ह्या नोंदीना Key असं म्हंटलं जातं. ह्या Key मध्ये जर व्हायरसने काही बदल केले तर त्याचे घातक परिणाम होतात.

Library File

'विंडोज' मधील सॉफ्टवेअर्स किंवा प्रोग्राम्स चालण्यासाठी आणि मुख्यत्वे विविध प्रोग्राम्समध्ये लागणारी तीच ती कोडस् सार्वजनिकरित्या वापरण्यासाठी Library File ची योजना असते. ह्या फाईल्सना DLL म्हणजे Dynamic Link Library Files असे म्हणतात. जेव्हा एखाद्या DLL फाईलला व्हायरसची लागण होते तेव्हा ती फाईल वापरणारे जेवढे प्रोग्राम्स आहेत त्या सर्वांवर त्याचा परिणाम होत असतो. कारण ती एक फाईल हे सगळेच प्रोग्राम्स मिळून वापरत असतात.

Mailbomb

हजारोच्या संख्येने एकाच वेळी ई मेल पाठवून सर्व्हर स्पेस भरुन टाकणे व इतर येणाऱ्या खऱ्या ई मेल्सना प्रतिबंध निर्माण करणे. हाच प्रकार आकाराने बरीच मोठी 'ई मेल' वा ॲटॅचमेंट पाठवूनही करता येतो.

Malicious Code

संगणकाचे नुकसान करण्याच्या दृष्टीने लिहिलेले प्रोग्रॅमिंग कोड.

Malware

व्हायरस, ट्रोजन हॉर्सेस, मॅलिशियस ॲक्टीव्ह कंटेटस् इत्यादिंसारख्या नुकसानकारक प्रोग्रॅम्सना Malware म्हणतात.

Master Boot Record (MBR)

संगणकाच्या मास्टर बूट सेक्टरमध्ये असलेला ३४० बाईटस्चा एक छोटा प्रोग्राम. हा प्रोग्राम डिस्कचे पार्टिशन टेबल वाचतो, कोणते पार्टिशन बुटींगसाठी वापरायचे ते ठरवतो आणि त्या पार्टिशनच्या पहिल्या सेक्टरला जाऊन तेथील प्रोग्रामकडे संगणकाचा ताबा सोपवतो. एका हार्ड डिस्कवर एकच मास्टर बूट रेकॉर्ड असतो.

MP3 file

Moving Picture Experts Group Audio Layer 3 File. तिला

MP3 म्हणून ओळखले जाते. ह्या फाईल्समध्ये अत्यंत कॉम्प्रेस्ड असे ऑडिओ ट्रॅक्स असतात. ते इंटरनेटवर अत्यंत लोकप्रिय आहेत. लक्षात घेण्यासारखी गोष्ट ही की MP3 फाईल्स म्हणजे प्रोग्राम्स नव्हेत. त्यामुळे त्यांना व्हायरसेसची लागण होऊ शकत नाही.

Not in the Wild

जे व्हायरसेस त्यांच्यातल्या दोषांमुळे यशस्वीपणे पसरु शकत नाहीत त्यांना 'Viruses not in the wild' असे म्हंटले जाते.

Payload

व्हायरसचा हल्ला झाल्यानंतर जो परिणाम दिसून येतो त्याला 'पे लोड' असं म्हंटलं जातं. 'ड्रॉपर' किंवा 'ट्रोजन हॉर्स'च्या मध्ये जे व्हायरसेस लपलेले असतात त्यांनाही 'पे लोड' असं संबोधतात.

Rogue Programme

प्रोगाम्स किंवा डेटाचे नुकसान करण्यासाठी किंवा संगणकाची सुरक्षा व्यवस्था तोडण्यासाठी वापरल्या जाणाऱ्या कोणत्याही प्रोग्रामला Rogue Programme म्हणतात. त्यात 'ट्रोजन हॉर्सेस', 'लॉजिक बॉम्ब', 'व्हायरस' अशांचा समावेश आहे.

Self-garbling Viruses

अँटी व्हायरस प्रोग्रामपासून वाचण्यासाठी स्वत:चे कोड घोळ घालून स्वत:च बदलणारा व्हायरस हा सेल्फ-गार्बलींग व्हायरस म्हणून ओळखला जातो. जेव्हा हे व्हायरस पसरतात तेव्हा ते आपले कोड बदलतात. त्यामुळे अँटी व्हायरस प्रोग्राम त्यांना ओळखू शकत नाही. ह्या व्हायरसमध्ये एक अत्यंत छोटा प्रोग्राम कोड असतो; हा छोटा कोड सारे कोड 'डी कोड' करुन टाकतो.

Signature

अँटी व्हायरस स्कॅनिंग करणारा प्रोग्राम एखादा विशिष्ट व्हायरस आहे की नाही हे तपासण्यासाठी काही विशिष्ट पध्दतीची अक्षररचना शोधत असतो. प्रत्येक व्हायरसची 'सीग्नेचर' (अक्षररचना) वेगवेगळी असते.

तशी अक्षररचना सापडली नाही तर तो व्हायरस संगणकात नाही असं अँटी व्हायरस प्रोग्राम जाहीर करतो.

Sparse Infector

स्पार्स इन्फेक्टर हा काही विशिष्ट परिस्थितीतच फाईल्सना लागण करतो. उदाहरणार्थ विशिष्ट फाईल १० व्यांदा जेव्हा उघडली जाईल तेव्हाच तो तिला लागण करील किंवा जी फाईल १२८ के.बी.पेक्षा लहान असेल तिलाच त्याची लागण होईल. हे व्हायरसेस सतत व वारंवार लागण करीत नसल्याने त्यांना शोधणे अवघड जाते.

String

सलग अशी अक्षरांची रचना म्हणजे 'स्ट्रींग'. उदाहरणार्थ: " afsHc*&@~" ही स्ट्रींग आहे. थोडक्यात अक्षरे, संख्या व खूणांची सलग मालिका म्हणजे 'स्ट्रींग'. अँटी व्हायरस प्रोग्राम्स हे व्हायरसच्या विशिष्ट स्ट्रींग्ज निवडून त्यांना 'सीग्नेचर' म्हणतात.

Timestamp

एखादी फाईल ज्या दिवशी तयार झाली, व ज्या तारखेस बदलली गेली ती तारीख एखाद्या फाईलवर वा एखाद्या डेटामध्ये नोंदली जाते. ज्यावेळी आपण एखाद्या फाईलच्या Properties पहातो तेव्हा हा टाईम स्टँप आपल्याला दिसतो.

TOM

Top of Memory. बहुसंख्य संगणकांमध्ये ही डिझाईन मर्यादा ६४० के.बी.ची असते. बूट रेकॉर्डला काही ही सगळी मेमरी लागत नाही. तो काही भाग व्यापून बराच भाग मोकळा सोडतो. ह्या मोकळ्या भागात लपण्याची युक्ती बरेच बूट व्हायरसेस करतात. ही टॉप ऑफ मेमरीची संख्या (Value) पाहिली व त्यात मोठा फरक दिसला तर व्हायरस असण्याची शक्यता दाट. मात्र अन्य कारणांमुळेही असा फरक दिसू शकतो हेही तेवढेच खरे आहे.

TSR

Terminate and Stay Resident. TSR प्रोग्राम हा चालू झाल्यानंतर

मेमरीत बसतो. ह्या प्रोग्राममधून त्या प्रोग्राममध्ये जाणे यामुळे शक्य होते. मात्र काही TSR प्रोग्राम हेच व्हायरसेस असतात. ते मेमरीत राहतात आणि अन्य फाईल्सना लागण करतात.

Tunnelling

अँटी व्हायरस प्रोग्राम्सना नीट काम करता येऊ नये ह्या दृष्टीने डिझाईन केलेले व्हायरसचे तंत्र. अँटी व्हायरस प्रोग्राम्स हे ऑपरेटींग सिस्टमचा ताबा अगोदर आणि शीघ्रतेने घेतात. त्यामुळे ऑपरेटींग सिस्टम व्हायरस प्रोग्राम चालवू शकत नाही. टनेलींग व्हायरसेस ह्या बाबतीत अँटी-व्हायरसशीच स्पर्धा करु पाहतात. ते अँटी-व्हायरसने ऑपरेटींग सिस्टमचा ताबा घेण्याच्या अगोदर ऑ. सिस्टमचा ताबा घेतात व व्हायरस प्रोग्राम चालवतात. आता मात्र नवे अँटी व्हायरसेस असे टनेलींग व्हायरसेस ओळखू लागले आहेत.

Vaccination

काही अँटी व्हायरस प्रोग्राम्स हे तंत्र वापरतात. संगणकातील फाईल्सची माहिती हे तंत्र नोंदवून ठेवते. ह्या माहितीच्या बाहेर त्यात काही बदल होत असेल तर त्याची माहिती ह्या तंत्राद्वारे युजरला दिली जाते. ह्या तंत्राला 'व्हॅक्सिनेशन' असे नाव आहे. व्हॅक्सिनेशन दोन प्रकारचे असते. 'इंटर्नल' व 'एक्सटर्नल'. 'इंटर्नल' ह्या प्रकारात त्या त्या फाईल मध्येच ही माहिती ठेवली जाते. तर 'एक्सटर्नल' ह्या प्रकारात स्वतंत्र फाईल मध्ये ती ठेवली जाते.

Variant

एखाद्या व्हायरसची सुधारित आवृत्ती म्हणजे Variant. व्हायरसचे कोड त्या व्हायरसच्या रायटरने अथवा अन्य कुणीतरी बदलून दुरुस्त करणे ही क्रिया त्यात अंतर्भूत आहे. जर मूळ व्हायरसमध्ये फार छोटे बदल असतील तर बहुतेक अँटी व्हायरस प्रोग्राम्स हे Variant ही ओळखतात. मात्र जर हे बदल फार मोठ्या प्रमाणावर असतील तर अँटी व्हायरस ते ओळखू शकत नाहीत.

VBS

व्हिज्युअल बेसिक स्क्रीप्ट. ती एक प्रोग्रामिंग भाषा आहे. युजरला न

कळता एखादा प्रोग्राम उघडणे, वापरणे व बंद करणे ह्या VBS प्रोग्रामिंगमध्ये शक्य असते. ही फाईल VBS ह्या एक्स्टेंशनची असते. VBS प्रोग्राम्स हे HTML फाईलमध्ये टाकता येऊ शकतात व वेब पेजद्वारे ते active content येऊ शकते.

'व्हायरस'च्या जगतातील काही निवडक पारिभाषिक शब्दच येथे आले आहेत. असे आणखीही कित्येक शब्द वा शब्दप्रयोग रुढ झालेले आहेत. एखाद्या अँटी व्हायरसच्या वेब साईटवर जाऊन त्यांची माहितीही घेता येईल. महत्वाच्या वेब साईटस्ची माहिती पुढील एका प्रकरणात आली आहे.

इनॉक्युलेट आय.टी. एक उत्तम उपाय

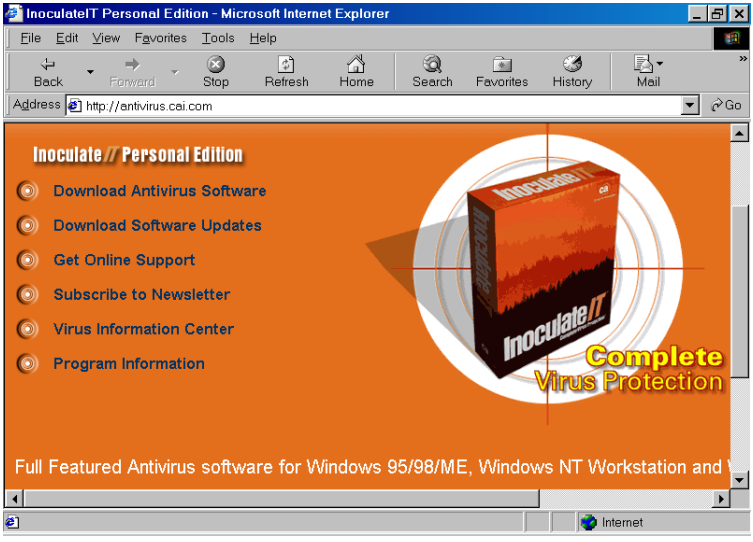
'व्हायरस'च्या समस्येला तोंड द्यायचं तर एखादा अँटी-व्हायरस प्रोग्राम आपल्या संगणकावर असायला हवा. आजकाल असे अनेक प्रोग्राम्स बाजारात आहेत. रु.५००/- पासून ते रु. १५,०००/- पर्यंत त्यांच्या किंमती आहेत. सामान्यतः ह्या इंटरनेटच्या मोफत जमान्यात आपण शोधत असतो 'चांगला आणि मोफत' प्रोग्राम. अँटी-व्हायरसचे अनेक प्रोग्राम्स इंटरनेटवर उपलब्ध आहेत. पण संपूर्ण विश्वासार्ह असे त्यातून शोधूनही सापडत नाहीत. मात्र 'इनॉक्युलेट आय.टी.' हा एकमेव प्रोग्राम माझ्या पाहण्यात असा आहे की जो मोफत तर आहेच, पण पूर्ण विश्वासार्हही आहे. त्याच्या ह्या गुणांमुळे आज तो जगातल्या पहिल्या चांगल्या पाच प्रोग्राम्समध्ये गणला जातो.

डाऊनलोड करा.

Inoculate IT इंटरनेटवरून मोफत डाऊनलोड करुन वापरता येतो. त्यासाठी तुम्हाला फक्त एक फॉर्म ऑनलाईन भरावा लागतो. ह्या फॉर्ममध्ये तुमचा 'ई मेल' पत्ता विचारला जातो. त्या ई मेल पत्त्यावर मग तुम्हाला तुमचा प्रोग्रामसाठीचा नंबर पाठविला जातो. प्रोग्राम इन्स्टॉल करताना तो नंबर टाईप करावा लागतो.

हा प्रोग्राम Computer Associates ह्या कंपनीने तयार केला असून तो त्यांच्या खालील वेब साईटवर डाऊनलोडींगसाठी उपलब्ध आहे:

http://antivirus.cai.com जर इथे डाऊनलोडींगसाठी काही अडचण येत असेल तर http://www.download.com वर जा. तेथील Utilities



वर गोलातील ठिकाणी क्लीक केल्यावर येणारा फॉर्म भरल्यानंतर डाऊनलोड सुरू होतो.

विभागातील Anti-Virus उपविभागात 'Inoculate IT' ची लिंक आढळेल त्यावर क्लीक करा. ह्या साईटवर फॉर्म भरावा लागत नाही हा एक फायदा आहे.

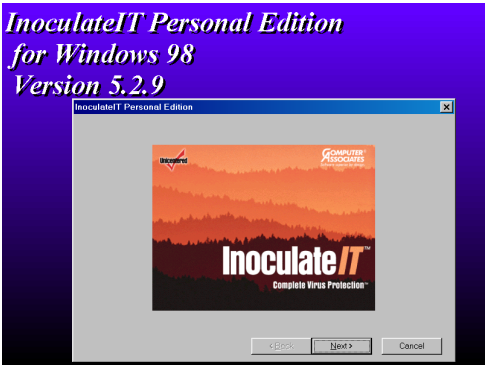
'इनॉक्युलेट' चे फायदे

बाजारात उपलब्ध असलेल्या लोकप्रिय McAfee Virus Scan व Norton Anti Virus च्या तुलनेत 'इनॉक्युलेट' अनेक लाभ युजरसाठी देतो. McAfee पेक्षा ६ टक्के कमी सिस्टम रिसॉर्सेस 'इनॉक्युलेट'ला लागतात. 'नॉर्टन'च्या तुलनेत 'इनॉक्युलेट' ला ६५ टक्के कमी हार्ड डिस्क स्पेस लागते. 'इनॉक्युलेट' ट्रोजन हॉर्सेस, वॉर्म्स, मॅक्रो, १ बूट वगैरेसह सर्व प्रकारचे व्हायरसेस शोधून ते काढून टाकू शकतो. 'व्हायरस'तपासण्यासाठी सिस्टम स्कॅन, व्हायरसयुक्त ई मेल मेसेजेसची सूचना देणे खेरीज 'विंडोज एक्स्प्लोअरर' मध्ये इंटेग्रेट होऊन माऊसने राईट क्लीक केल्यावर 'इनॉक्युलेट'चा मेनूही मिळता, व त्याद्वारे 'विंडोज

एक्स्प्लोअरर' मधील फाईल वा डिरेक्टरी किंवा संपूर्ण ड्राईव्ह देखील आपण स्कॅन करु शकतो.

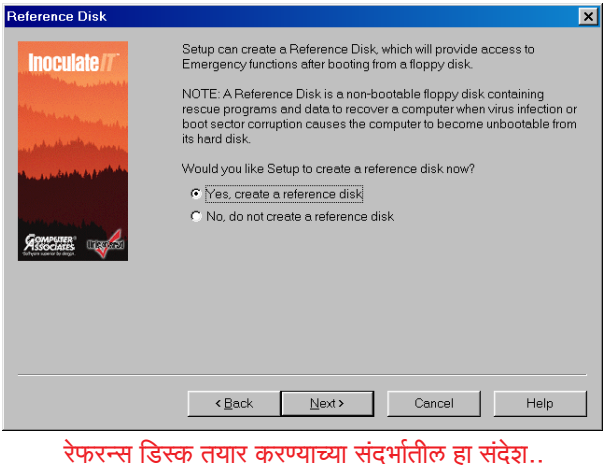
इन्स्टॉलेशन

'इनॉक्युलेट' प्रोग्राम इन्स्टॉल होताना एका फ्लॉपीची मागणी करतो. ही फ्लॉपी तो 'रेफरन्स डिस्क' म्हणून तयार करतो. अडचणीच्या वेळी सिस्टम रिबूट करण्यासाठी ही रेफरन्स डिस्क उपयोगी पडते.



इन्स्टॉलेशन सुरू झाल्यानंतर दिसणारा पहिला स्क्रीन..

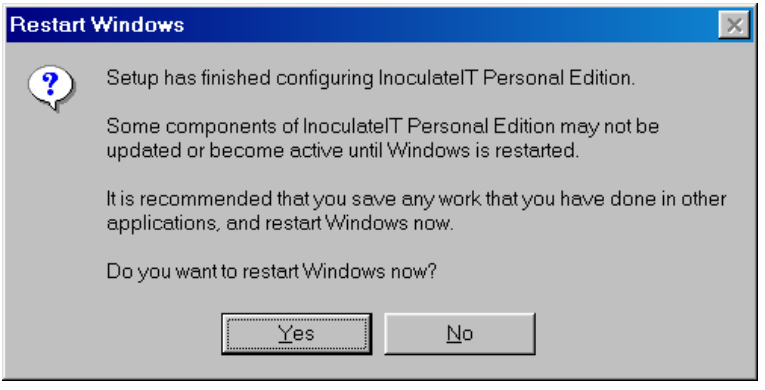
तुमच्या संगणकावर जर आणखी एखादा अँटी-व्हायरस प्रोग्राम असेल तर 'इनॉक्युलेट आय.टी.' तो काढून टाकायला सांगतो. तो काढल्याशिवाय



रेफरन्स डिस्क तयार करण्याच्या संदर्भातील हा संदेश..

'इनॉक्युलेट'चे इन्स्टॉलेशन होत नाही.

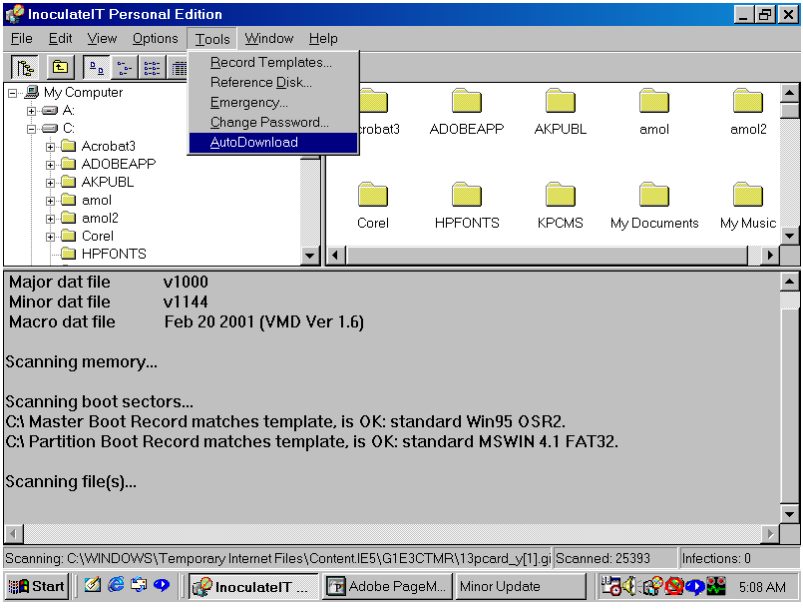
आता तुम्ही 'डाऊनलोड' करुन घेतलेली IPESetup.exe ह्या फाईलवर माऊसने डबल क्लीक करा. काही मिनिटांतच झपाट्याने इन्स्टॉलेशन संपते. मध्येच तो फ्लॉपीची मागणी करील तेव्हा फ्लॉपी टाकून Reference Disk तयार करण्यासाठी YES वर क्लीक करा. आता तुमच्याकडे संगणकावरील हार्ड डिस्कवर 'इनॉक्युलेट' लागलेले आहे, आणि हातात 'इनॉक्युलेट' ने तयार करुन दिलेली रेफरन्स डिस्क आहे. इन्स्टॉलेशन नंतर 'इनॉक्युलेट' लगेचच आणि स्वत:हून तुमचा संगणक स्कॅन करुन व्हायरसची तपासणी करतो. त्यानंतर तो तुम्हाला काँप्युटर बंद करुन पुन्हा चालू करायला म्हणजे 'रिबूट' करायला सांगतो. आता इन्स्टॉलेशन प्रक्रिया संपली आहे आणि तुम्ही 'इनॉक्युलेट आय.टी.' वापरायला मोकळे आहात.



इन्स्टॉलेशन संपल्यानंतर हा रिस्टार्ट विंडोजचा स्क्रीन येतो

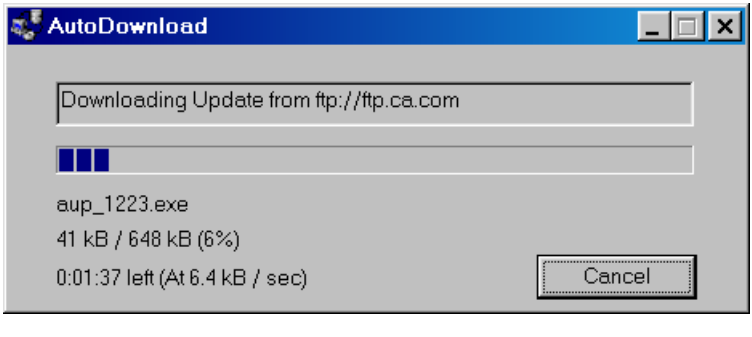
व्हायरस अपडेटस्

नवनवे व्हायरसेस येत असतात, आणि त्यावर नवनवे उपाय निघत असतात. ह्यासाठी अक्षरश: दैनंदिन स्तरावर आपले 'इनॉक्युलेट आय.टी' आपल्याला अपडेटेड ठेवणं आवश्यक आहे. Computer Associates कडून हे अपडेटस् देखील मोफत मिळतात. ह्यासाठी इंटरनेटवर ऑनलाईन असताना 'इनॉक्युलेट आय.टी' च्या TOOLS ह्या मेनूवर क्लीक करा, व



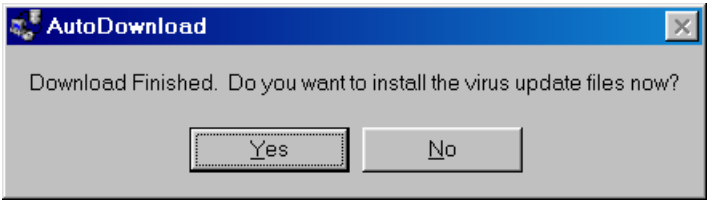
'AUTO DOWNLOAD' वर क्लीक करतानाची स्थिती

त्यानंतर AUTO DOWNLOAD वर क्लीक करा. AUTO DOWNLOAD याचा अर्थ नव्या व्हायरससाठी घ्यावयाचे अपडेटस् ऑटोमॅटिकली डाऊनलोड करुन घेणे. तुम्ही AUTO DOWNLOAD वर क्लीक केल्यानंतर एक फाईल डाऊनलोड होईल, नंतर ही फाईल



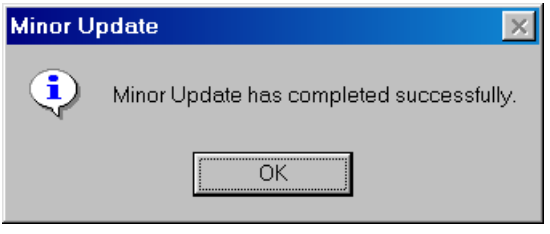
प्रत्यक्ष अपडेटची फाईल डाऊनलोड होतानाची स्थिती

इन्स्टॉल केल्यानंतर तुमचे 'इनॉक्युलेट आय.टी.'अपडेटेड राहील. अशा प्रकारे दोन-चार दिवसांनी अपडेटस् घेत राहिल्यास व्हायरस' ची समस्या



डाऊनलोड झाला. डाऊनलोड झालेली फाईल 'इन्स्टॉल' करायची का ?

. अर्थातच, करायची. YES वर क्लीक करा.

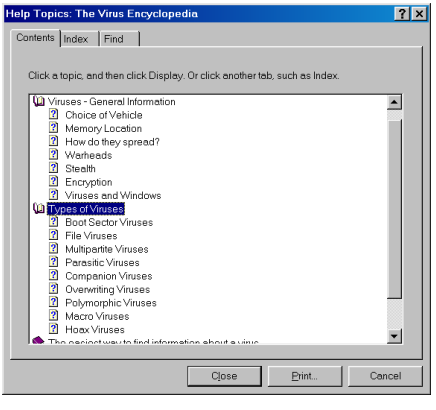


छोटा अपडेट आहे. पण कधी कधी मोठा अपडेटही मिळत असतो.

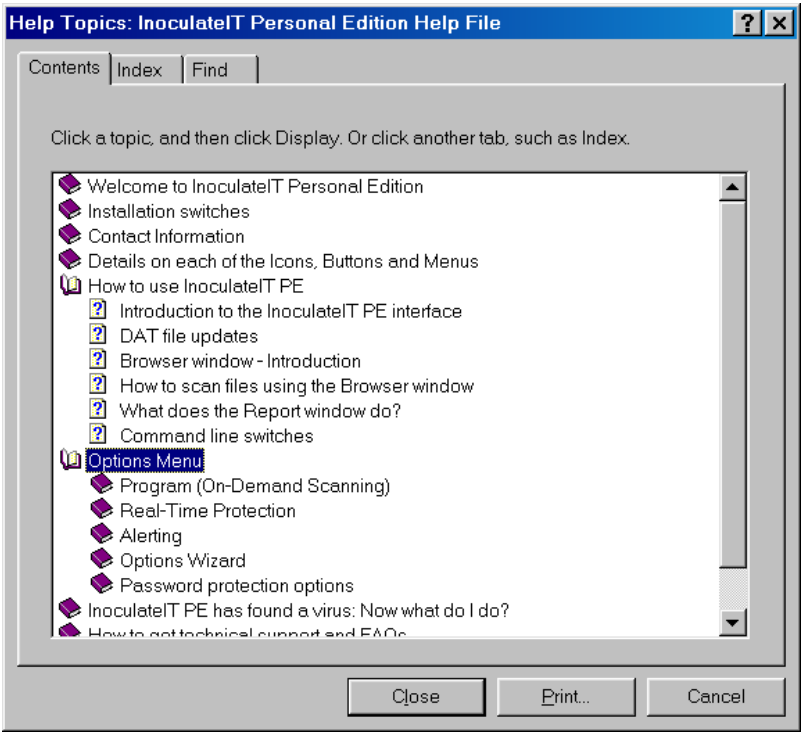
तुम्हाला भेडसावणं निव्वळ अशक्यच.

प्रशिक्षण, माहिती आणि मदत

'इनॉक्युलेट आय.टी.' बरोबर येणारी Help देखील खूप उपयुक्त



व्हायरस एनसायक्लोपेडिया. चांगली माहिती....

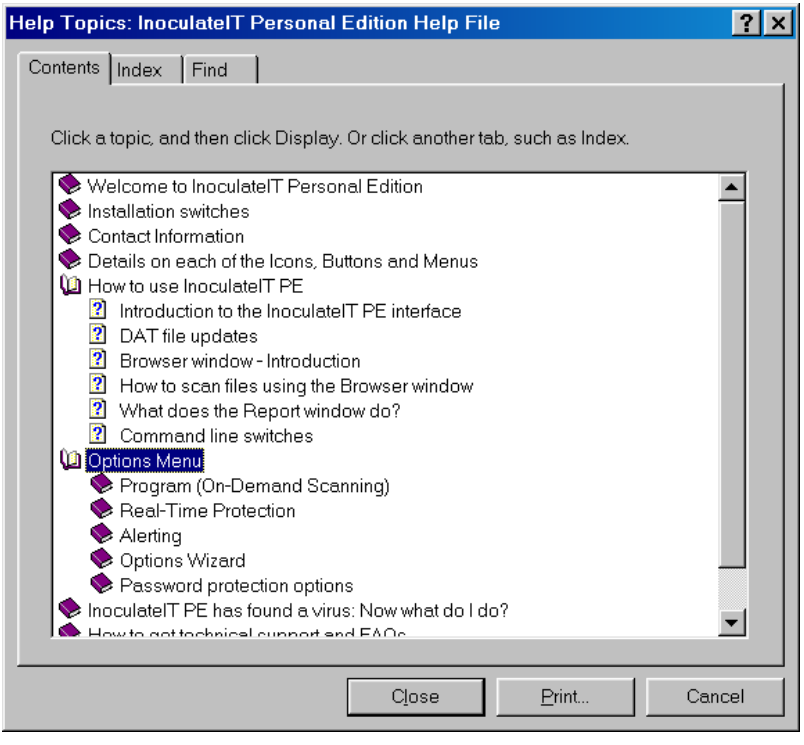


'इनॉक्युलेट आय.टी' वापरायला शिकवणारी हेल्प विंडो.

आहे. ह्याचे दोन भाग आहेत. एकात आहे Virus Encyclopedia. दुसऱ्यात आहेत Help Topics. जर सर्वसामान्यपणे व्हायरसबद्दल विशेष काही जाणून घ्यायचं असेल तर Encyclopedia पहा. ह्या भागात व्हायरसचे प्रकार, त्यात बूट सेक्टर व्हायरस, फाईल किंवा मल्टीपार्टाईट व्हायरसेस, मॅक्रो व्हायरसेस, होक्स व्हायरसेस अशी सविस्तर माहिती आहे. व्हायरस कसे पसरतात वगैरे मौलिक माहिती आहे. Help विभाग हा Innoculate IT हा प्रोग्राम कसा वापरावा, त्यातील मेनूमध्ये काय आहे, बटणांचा वगैरे उपयोग कसा करावा हे पध्दतशीरपणे सांगितले आहे.

ह्याखेरीज http://www.cai.com/virusinfo/encyclopedia/

ह्या वेबसाईटवर गेलात तर व्हायरसेसबद्दलची अगदी लेटेस्ट म्हणावी



'इनॉक्युलेट आय.टी' वापरायला शिकवणारी हेल्प विंडो.

अशी माहिती, व्हायरसेसची यादी वगैरे पहायला मिळेल . थोडक्यात, 'इनॉक्युलेट' कुठेही कमी पडत नाही. एवढं सगळं मोफत देणारा दुसरा कोणताही प्रोग्राम नाही. आणि म्हणूनच त्यावर ह्या पुस्तकांत संपूर्ण सचित्र आणि मुद्देसूद माहिती दिली आहे.

आज उपलब्ध असणारे काही इतर अँटी व्हायरस प्रोग्राम्स

'नॉर्टन अँटी व्हायरस २००१' बद्दल मागील एका प्रकरणात आपण माहिती घेतली. 'नॉर्टन अँटी व्हायरस' हा ट्रायल संपल्यानंतर विकत घ्यावा लागतो. त्याची आजची किंमत अदमासे रु. २५००/- आहे. ज्यांना मोफत व चांगला अँटी व्हायरस प्रोग्राम हवा आहे त्यांचेसाठी Inoculate IT हा उत्तम अँटी व्हायरस प्रोग्राम आहे. त्याची माहितीही आपण मागील प्रकरणात घेतलेली आहे. ह्या दोन अँटी व्हायरस प्रोग्राम्स व्यतिरिक्त खालील दिलेले प्रोग्राम्सही प्रसिध्द आणि कमी अधिक लोकप्रिय आहेत. त्या प्रोग्राम्सची नावे व त्यांच्या वेब साईटस्चे पत्ते येथे दिले आहेत. हे प्रोग्राम्स विकत घ्यावे लागत असले तरी त्यांच्या किंमती परवडण्याजोग्या आहेत.

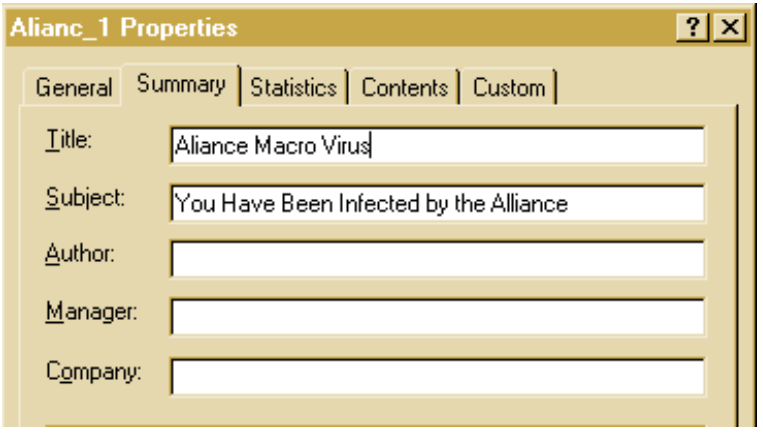
प्रोग्रामचे नाव	**डाऊनलोडींगसाठी वेब साईटचा पत्ता**
1. McAfee VirusScan 5.*	http://www.nai.com
2. Kaspersky Anti-Virus 3.5	http://www.avp.ch
3. F Prot 3.09	http://www.complex.is/f-prot/mirrors.html

4. Quick Heal 6	http://www.quickheal.com
5. Panda Anti Virus Platinum 6.3	http://pandasoftware.com
6. Antidote for PC Viruses (Personal Edition 2000)	http://www.antidote4pc.com
7. F-Secure Anti Virus 4.08	http://www.fsecure.com
8. Thunderbyte Anti Virus	http://www.thunderbyte.com
9. PC-cillin	http://www.antivirus.com
10. Command Anti Virus	http://Commandcom.com
11. AVG Anti Virus 6.0	http://www.grisoft.com
12. Sophos Anti Virus	http://www.sophos.com

'व्हायरस' चे दर्शनी स्वरुप

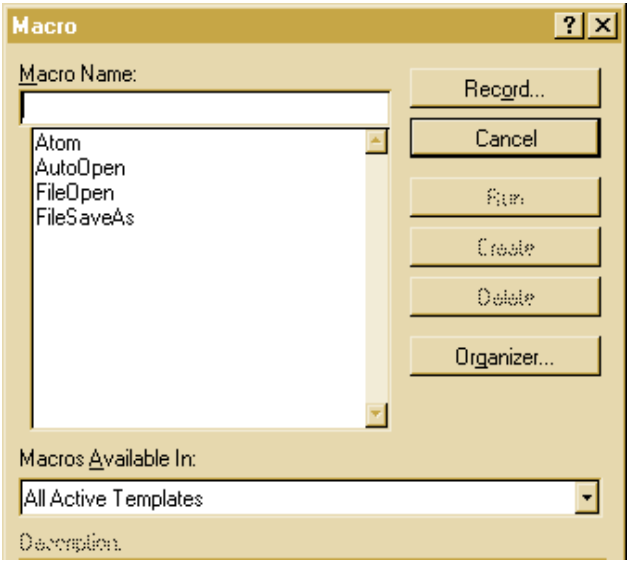
सामान्यतः व्हायरसेस हे परिणामाच्या स्वरुपातच आपण पाहतो. हार्ड डिस्क पुसली गेली आहे, संगणक मंद चालू लागला आहे, काहीतरी विचित्र अक्षरे दिसू लागली आहेत, काही प्रोग्राम्स उघडणं बंद झालेलं आहे. वगैरे वगैरे. व्हायरसेस सहसा स्वतःचा चित्रात्मक संदेश मागे ठेवीत नाहीत. यामागील महत्वाचे कारण म्हणजे चित्रामुळे 'व्हायरस'चा आकार (bytes) वाढतो. अशा फुगलेल्या आकाराचा व्हायरस लपवणे वा फ्लॉपीतून पसरवणे मग अवघड जाते. 'डॉस'च्या मागासलेल्या काळातले व्हायरस रायटर्स म्हणूनच चित्र वगैरेंच्या भानगडीत कधी पडले नाहीत. अगदी सुरुवातीच्या म्हणजे २८६ च्या काळात तर मोनोक्रोम मॉनिटर्स (कृष्ण-धवल) असत. त्यामुळे चित्राला तशाही मर्यादा होत्या. ह्या प्रकरणात काही 'व्हायरसेस'ची चित्रे दिली आहेत. अगदी अलीकडे आलेल्या 'नेकेड वाईफ' किंवा तत्सम वॉर्म्सनी 'फ्लॅश' चित्रांचा अवलंब केला. वॉर्म्स हे मुख्यत्वे ॲटॅच्ड फाईलच्या स्वरुपात गेल्याने 'साईज' वाढली म्हणून फारसे बिघडत नव्हते. त्यामुळे वॉर्म्समध्ये जेवढी चित्रे दिसतात तेवढी इतर व्हायरसेसमध्ये दिसत नाहीत. येथे काही अलिकडची तर काही जुन्या काळातील 'व्हायरसेस'ची चित्रे दिलेली पुढील पानांवर आहेतः

Alliance2, Macrovirus



Alliance ह्या मॅक्रो व्हायरसने मागे ठेवलेली विंडो.

Atom. Macrovirus

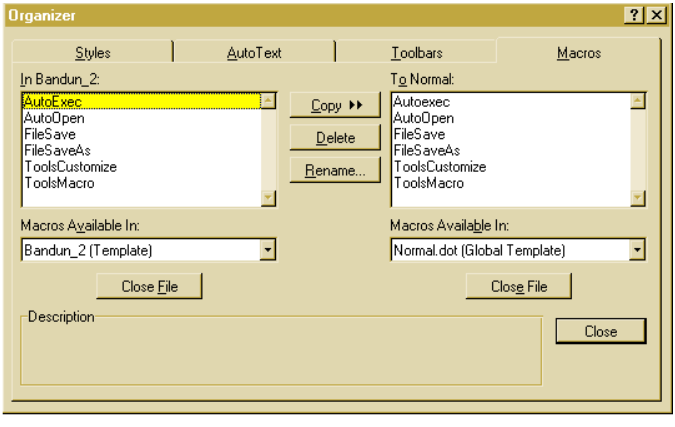


Atom ह्या मॅक्रो व्हायरसची प्रतिमा अशी होती...

Boza, first windows 95 virus

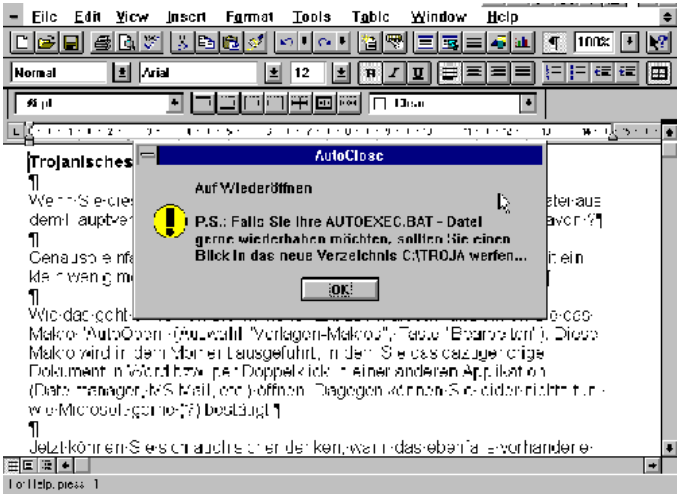
पहिला विंडोज ९५ व्हायरस बोझा असा दिसला.

Bandung.1.macrovirus



'बांडुंग' ह्या मॅक्रो व्हायरसचे दर्शन.

wiederhof.macrovirus

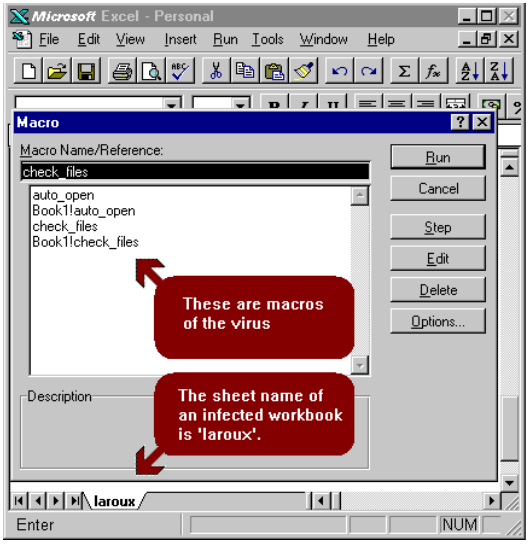


वाईड्रॉफ मॅक्रो व्हायरसची खूण

Olympic virus

आलिंपिक व्हायरसचा हा १९९४ चा अवतार

Larour Excel, Macro virus



लॅटर मॅक्रो व्हायरसची ही पिल्ले..

---

suicide virus

suicide व्हायरसने मागे ठेवलेले हे विकृत चित्र.

Flasher virus

'फ्लॅशर' व्हायरस गाजला नाही. पण ह्या चित्रावरुन
व्हायरस लिहिणाराचा बालिशपणा कळतो.

Leprosy virus

हे चित्र मागे ठेवून जाणारा 'लेप्रसी' व्हायरस Hellraiser अशी फुशारकी
मारत म्हणतो I will be back.

अगदी अलिकडील 'नेकेड वाईफ' ह्या
व्हायरसबरोबर आलेला फ्लॅश मुव्ही.

गाजलेल्या 'Love Letter ' ह्या व्हायरसची
अॅटॅच्ड फाईल अशी दिसत होती.

पुढे काय ?

एकूण आता व्हायरस हा प्रकार लक्षात आला. काँप्युटर व्हायरसला घाबरुन जाण्याची गरज नाही. तो फक्त काँप्युटरचे प्रोग्राम्स आणि डेटा यांना धोका पोहोचवू शकेल. हा डेटा आणि प्रोग्राम पुन्हा सहजपणे लावता येऊ शकतात. काँप्युटरच्या हार्डवेअरला त्यातून कसलेही नुकसान होत नसते. अचानक जाणारी वीज ही काँप्युटर व्हायरसपेक्षा भयानक असते. कारण व्होल्टेजच्या अचानक व शीघ्र वर खाली होण्याने काँप्युटरमधली एखादी चिप वा आय/सी खराब होऊ शकते. त्यातले नुकसान अधिक आहे. पण लोक व्हायरसला जास्त घाबरतात तेवढे ते वीजेच्या प्रवाहातील चढ-उताराला वा खंडित होण्याला घाबरत नाहीत. असं का होतं!

याचं मूळ माणसाच्या मनात आहे. व्हायरसेसना प्रसिध्दी इतकी मिळत गेली की ते आहेत त्यापेक्षा खूपच भयंकर वाटू लागले. काही कोटी रुपये नुकसान झाले वगैरे आकडे वाचनात आले की माणूस हबकतो. दुसरी गोष्ट म्हणजे भडक प्रसिध्दीबरोबर सतत प्रसिध्दी ही हातोड्यासारखे काम करते. हातोडा हा एकदा दगडावर आपटला तर दगड फुटत नाही. पण तो तीन चार वेळा घण घालून मारला तर दगड फुटतो. तसच ह्या व्हायरसच्या बाबतीत झालय. सतत तेच ते कानावर आल्याने व 'सावध रहा, सावध रहा' असा हाहाकारही खूप झाल्याने सावध राहिलेले सुध्दा घाबरुनच सावध राहतात. अज्ञानापोटी भिती, भितीपोटी निष्क्रियता आणि पुन्हा निष्क्रियतेपोटी अज्ञान असं काहीसं होतं. तुमच्याकडे जर 'बॅकप' करुन ठेवलेला असेल तर, डेटा जाण्याची भिती तुम्ही का बाळगावी ?

'उलट येऊ दे व्हायरस आल तर, आपण सामना करु या' असा बिनधास्त दृष्टीकोन फार कमी लोक ठेवतात. उगाचच घाबरण्याने व्हायरस रायटर्सचा इतका फायदा झालाय की काही विचारु नका.

आता साधी 'ई मेल' ची गोष्ट घ्या. 'ई मेल' बरोबर आलेली फाईल तपासल्याशिवाय उतरुन घेऊ नका' हा साधा नियम आहे. पण ह्या नियमाच्या बाबतीत आवश्यकता नसताना आपण निर्धास्त राहतो. ह्यावेळी कसलीही भिती आपल्या डोक्यात नसते. ती का? अति उत्साहात आपण ॲटॅचमेंट उघडतो. मग त्यातून व्हायरस शिरला की आपण गोंधळतो, घाबरतो, ''डेटा गेला डेटा गेलाऽऽ''असा टाहो फोडतो.

'पुढे काय' याचा विचार करीत असताना बातमी आलीय की 'नासा' ही अमेरिकन सरकारची खगोलशास्त्र संशोधन प्रयोगशाळा इ.स. २००३ मध्ये मंगळावरुन पृथ्वीवर ई मेल पाठविण्याची तयारी करतेय. याचे प्रपोजल तयार असून त्याला सरकारची मान्यता मिळताच वेगाने तयारी पूर्ण होईल. आता प्रश्न हा आहे की मंगळावरुन उद्या पहिली 'ई मेल' इथे येईल. परवा काही ॲटॅचमेंटस् देखील येतील. ह्या ॲटॅचमेंटस्ही तपासाव्या लागणार काय? पृथ्वीवरुन मंगळावर जाणारी 'ई मेल' 'मेलिसा' किंवा 'लव्ह लेटर' सारखा व्हायरस पाठवणार का? आणि मंगळावरही खळबळ उडणार का? याचं उत्तर आहे की आपले 'ई मेल' प्रोग्राम्स अंतर्बाह्य सुधारण्याची गरज आज आहे. ज्या 'ई मेल' मध्ये 'व्हायरस' आहे अशी 'ई मेल' आपोआप डिलीट होण्याची व्यवस्था त्या प्रोग्रामला करावी लागेल. किंवा ॲटॅचमेंटमधून व्हायरस काढून टाकून मगच ती पोहोचवण्याची क्षमता असणारे ई मेल प्रोग्राम्स येत्या काही वर्षात बनविणे आता आवश्यक झाले आहे.

हाताच्या बोटांचे ठसे मॉनिटरच्या काचेतून स्कॅन होऊन त्याचा उपयोग पासवर्ड म्हणून होऊ लागेल अशी दाट शक्यता एकूण संशोधन पाहता आज दिसते. आज आपण काही अक्षरे वा काही कीस्ट्रोक्सचा उपयोग पासवर्ड म्हणून करतो. हे पासवर्डस् ब्रूट फोर्स सॉफ्टवेअर वापरुन हॅक करणारी मंडळी जगात हजारो आहेत. त्यामुळे खूपदा लोकांना पासवर्ड आणि त्यावर आधारित 'ई मेल' व 'इंटरनेट' यांचेवर पूर्ण विश्वास ठेवताना अवघड जाते. एका बोटासारखे दुसरे बोट व ठसा नसतो. याचाच उपयोग

पासवर्डच्या जागी करुन सुरक्षा मूल्य वाढविण्याचा प्रयत्न उद्या होण्याची शक्यता आहे. अशा वेळी माणसाला बेशुध्द करुन व त्याच्या बोटाच्या ठशाचा वापर करुन जबरदस्ती होणे शक्य आहे काय? होय आहे. कारण हा मनुष्य स्वभाव आहे. मनुष्य एकीकडे प्रगती करीत राहणार आणि दुसरीकडे त्याची दैवगतीही अशा प्रवृत्तींना जन्म देत राहणार. हे होतच राहणार.

आजकाल बहुतेक व्हायरसेस हे इंटरनेटच्या माध्यमातून येतात. सॉफ्टवेअर्सच्या फाईल्स अनोळखी साईटवरुन डाऊनलोड करताना हे हमखास होते. अॅटॅचमेंट संशयास्पद वाटली तरी ती उघडण्यातूनच रामायण होते. 'ई मेल' द्वारा पसरलेले हे काही भयानक व्हायरस पहा. ह्या छोट्या छोट्या प्रोग्राम्सनी आपलाच संगणक वापरुन डाव साधलेला आहे. बहुतेक जण 'ई मेल' अॅटॅचमेंट उघडून नकळत ती इतरांना पाठवत गेले. त्या व्हायरसेसचा उपाय देखील येथे सांगितले आहेत. त्या त्या साईटवरुन ते डाऊनलोड करून घ्या.

Wscript. KakWorm

डिसेंबर १९९९ मध्ये प्रथम दिसून आला. मायक्रोसॉफ्टच्या आऊटलूक एक्सप्रेसचा उपयोग करुन 'ई मेल' अॅटॅचमेंटद्वारे तो पसरत जातो. आऊटलूक एक्सप्रेसमध्ये एक सुरक्षाविषयक दोष आहे. त्याचा वापर हा वॉर्म करतो. आता हा दोष दूर करण्यासाठी मायक्रोसॉफ्टने एक पॅच प्रोग्राम दिला आहे. तो खालील पत्त्यावरुन डाऊनलोड करता येईल.

http://www.microsoft.com/technet/ie/tools/scrpteye.asp

ह्यानंतर आलेला सुधारित Wscript. KakWorm.B हा वेगळा आहे. ' 'B' ची ह्यात भर पडली आहे. मूळच्या Wscript. KakWorm ची ही सुधारित आवृत्ती असली तरी तो काढण्यासाठी वेगळी पध्दत अवलंबावी लागते. त्याचा आकार फक्त ४११६ बाईटस् आहे. हा व्हायरस काढण्याची पध्दत व ह्या संदर्भातील सविस्तर माहितीसाठी खालील वेब साईटवर जा.

http://www.symantec.com/avcenter/venc/data/
wscript.kakworm.html

W95. MTX

ह्या व्हायरसची सविस्तर माहिती इथे घ्या.

http://www.symantec.com/avcenter/venc/data/w95.mtx.html

हा १७ ऑगस्ट २००० रोजी दिसून आला. तो काढून टाकणे अत्यंत अवघड आहे. मात्र वर दिलेल्या वेब पेजवर तो काढून टाकण्याचे मार्ग दिलेले आहेत.

W32. Navidad

हा एक मास मेलींग करणारा वॉर्म प्रोग्राम आहे. ३ नोव्हेंबर २००० रोजी दिसून आला. ३२७६८ बाईटस् हा त्याचा आकार आहे. वॉर्म काढून टाकण्याचा उपाय

http://www.symantec.com/avcenter/venc/data/w32.navidad.fix.html

येथे उपलब्ध आहे.

W32. Magistr

हा असा व्हायरस आहे की ज्याच्यात ई मेल Worm चे गुणधर्म ही आहेत. १३ मार्च २००१ रोजी आढळून आला. हा व्हायरस भयानक आहे. तो 'विंडोज' मधील CMOS व Flash BIOS डिलिट करतो. प्रत्येक पंचविसाव्या फाईलमधला डेटा पुसून त्या जागी YOUARESHIT अशी अक्षरे भरून टाकतो.

Happy 99.worm

२८ जानेवारी १९९९ रोजी दिसून आला. ई मेल अॅटॅचमेंटद्वारेच पसरतो. ही अॅटॅचमेंट happy99.exe किंवा happy.exe अशी नावाची असते.

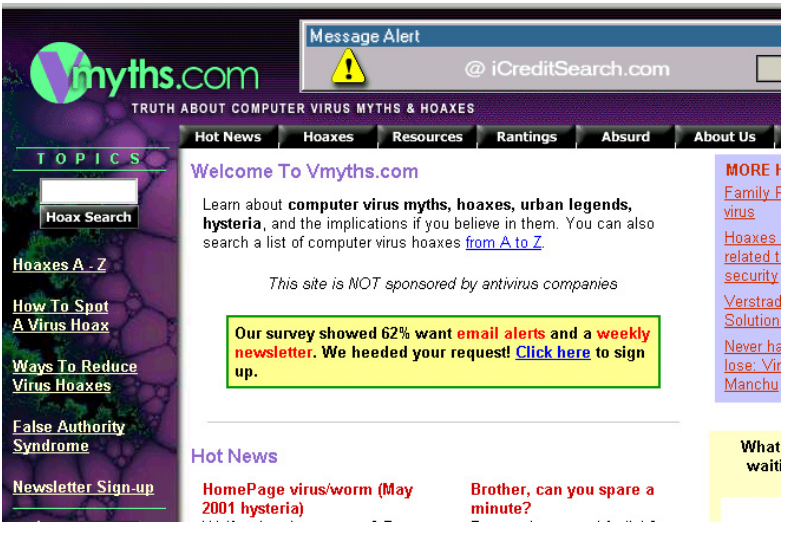
वरील व्हायरस पाहिले की वाटतं पुढे काय होणार आहे? लोक किती दिवस, किती महिने असे फसणार? लोक फसले नाहीत तर ई मेल व्हायरसेस किंवा वॉर्म्स यशस्वी होतील का? आता लोक फसत नाहीत, असे व्हायरस चालत नाहीत हे कळले की व्हायरस लिहिणारेही आपोआप नाउमेद होतील की नाही? यासाठीच इतरांशी संपर्क, काहीशी धडाडी, थोडेसे धैर्य वा धारिष्टय असायला हवं. आता सध्या फार थोडे नवे

व्हायरस येत असतात. येणारे हे जुनेच व्हायरस नव्या रुपात आहेत. वरील व्हायरस येथे मुद्दाम निवडून दिले. कारण यांच्याच शेकडो निरनिराळ्या आवृत्या बनलेल्या आहेत.

अँटी व्हायरस प्रोग्राम्स सध्या खूपच स्मार्ट झालेत. काट्याने काटा निघावा म्हणतात तसे 'व्हायरस' ह्या प्रोग्राम्सना 'अँटी व्हायरस' हा प्रोग्राम मारु पाहतो. अँटी व्हायरस अधिक स्मार्ट झाल्याने बरेच जण व्हायरसहीन होणार आहेत. बनणारा प्रत्येक व्हायरस मारण्याची ताकद एक दिवस आपण शोधणारच आहोत. पण तोपर्यंत ..? थोडा धीर धरावा, वाचावं, अभ्यास करावा आणि भयगंड टाकून द्यावा. यासाठी फार उच्च शिक्षणाची गरज नाही. थोडासा निश्चिय आणि तो तडीस न्यायला बरीचशी इच्छाशक्ती हवी असते.

'व्हायरस': काही महत्वाच्या वेबसाईटस्

'व्हायरस' चे जग मोठे आहे. दोन दशकांत ५०,००० व्हायरस येणं याचा अर्थ दररोज दरमहा सुमारे ३०० व्हायरसेस तयार होणं असा होतो. ह्या वेगाने व्हायरसेसची समस्या उभी राहिल्याने ह्या क्षेत्रात अनेक अभ्यासक आले, अनेक कंपन्या आल्या. अनेक संशोधन प्रयोगशाळा उभ्या राहिल्या. नंतर ही मंडळी इंटरनेटवरही आली. जगाला व्हायरसेसची माहिती पुरवू लागली. अशा काही हजार साईटस् आज इंटरनेटवर आहेत. त्यातील ह्या अगदी हाताच्या बोटावर मोजण्याएवढ्या साईटस् इथे पुढील पानांवर दिल्या आहेत:



http://www.vmyths.com

ही एक अत्यंत माहितीपूर्ण साईट आहे. व्हायरसविषयीच्या अफवांचा मागोवा घेऊन त्यात कितपत तथ्य आहे हे सांगणारी ही साईट. आत्तापर्यंतच्या अफवा आणि लोणकढ्या इथे पहा. अशा अफवा आणखी पुढे पसरु नयेत यासाठी काय काळजी घ्यावी याचे मार्गदर्शनही ही साईट देते. 'व्हायरस' नियंत्रणाशी थेट ह्या साईटचा संबंध नसला तरी निष्कारण गोंधळ उडून त्यातून काहीतरी नको ते घडणं टाळण्यासाठीच महत्वाची कामगीरी ही साईट करीत असते. यातील अफवा सविस्तर वाचणे हे एक मनोरंजनच आहे.

http://www.f-secure.com

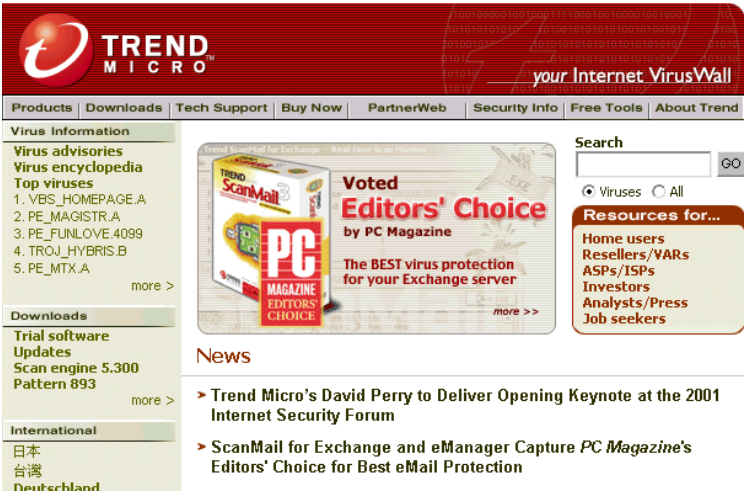
f-secure हे एक जुने अँटी-व्हायरस सॉफ्टवेअर आहे. १९८८ साली स्थापना झालेली f-secure ही कंपनी मूळ हेलसिंकी (फिनलंड) ची आहे. जगात सुमारे ९० देशांमध्ये तिचे वितरक असून १९९७ पर्यंत तिचे उत्पादन हे अत्यंत लोकप्रिय होते. अनेक पुरस्कारही तिने मिळवलेले होते. पामटॉप संगणकासाठी आता त्यांनी अँटी व्हायरस बनविलेला असून WAP साठी देखील FSAV हे अँटी-व्हायरस उत्पादन तयार केले आहे. आतापर्यंतच्या व्हायरसेसचे वर्णन ह्या साईटवर एका विभागात उपलब्ध आहे. ह्या खेरीज व्हायरसविषयक ताज्या बातम्या हे त्यांचे वैशिष्टय आहे.

http://www.symantec.com

सिमँटेक ही सुप्रसिध्द नॉर्टन अँटी व्हायरसची साईट. येथून तुम्ही नॉर्टन अँटी-व्हायरस २००१ वा आणखी अपडेटेड सॉफ्टवेअर डाऊनलोड करु शकता. आता 'सिमँटेक' ने काँप्युटर सिक्युरिटीमध्ये एक पाऊल पुढे टाकले आहे. 'नॉर्टन इंटरनेट सिक्युरिटी २००१' हे वेगळे सॉफ्टवेअर त्यांनी दिले आहे. सिमँटेकच्या ह्या साईटचे वैशिष्टय म्हणजे 'व्हायरसेस'चे सविस्तर तपशील व त्यावरील उपाय. आजमितीस नॉर्टन अँटी-व्हायरस हे सर्वांत प्रभावी अँटी-व्हायरस सॉफ्टवेअर मानले जाते. आकाराने ते खूप मोठे आहे. परंतु नव्या येणाऱ्या व्हायरसेसवरील उपाय, डेफीनीशन अपडेटस्, ऑनलाईन अपडेटस्, ह्या वैशिष्टयांनी लोक 'नॉर्टन' कडे आकर्षित होतात. 'पीटर नॉर्टन' यांनी 'सिमँटेक' ला आपली कंपनी विकल्यानंतर 'नॉर्टन' यांचे तेथील स्थान केव्हाच संपले आहे. केवळ नाव मात्र उरले आहे.

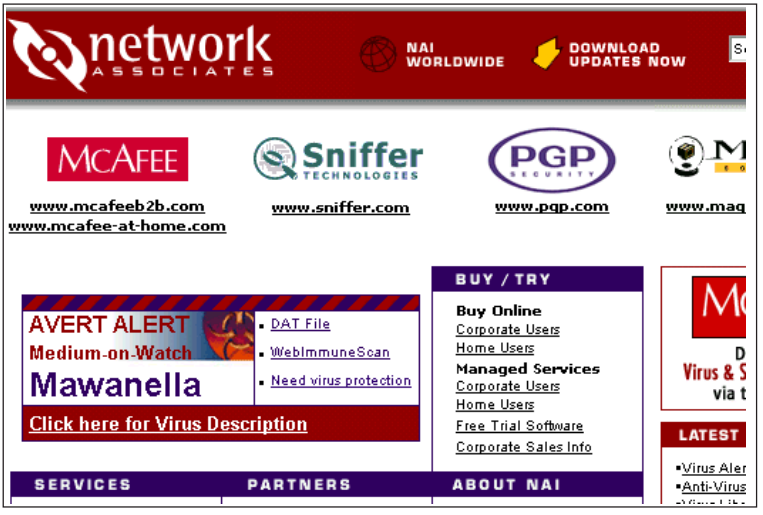
http://www.mcafee.com

ह्याच पुस्तकातील 'व्हायरसेस'चा मनोरंजक इतिहास हे प्रकरण पहा. तुम्हाला दिसेल की 'नेटवर्क ॲसोसिएट्सनी डॉ. सोलोमन हे व्हायरस सॉफ्टवेअरही विकत घेऊन टाकले. त्यामुळे 'मॅक फी' चा एकेकाळचा स्पर्धक जणू 'मॅक फी' च्याच घरात पाणी भरु लागला. आज 'मॅक फी' चे नाव मोठे आहे. मात्र 'सिमँटेक'ने एक पाऊल पुढे टाकले आहे. एकेकाळी व्हायरस स्कॅनिंग ही 'मॅक फी' ची मक्तेदारी होती हे सांगूनही खरे वाटणार नाही असा काळ सध्या आहे.



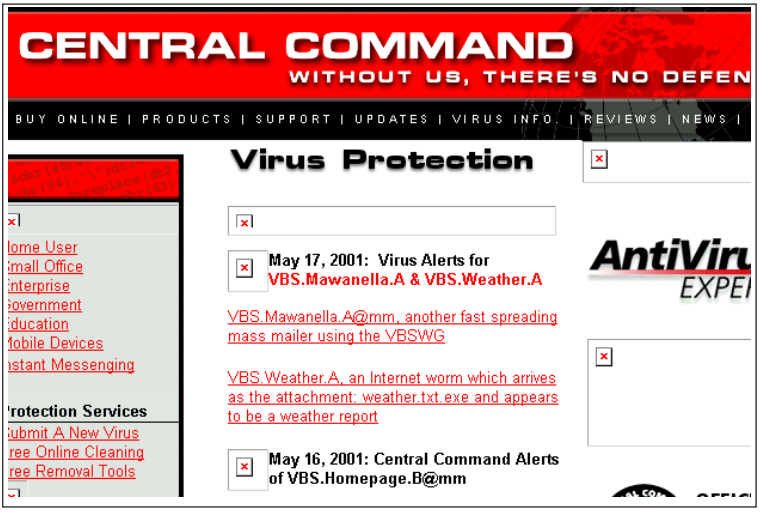
http://www.antivirus.com

'पीसीसिलिन' अँटी व्हायरस प्रोग्रामची ही वेब साईट. आजकाल जे प्रमुख अँटी-व्हायरस सॉफ्टवेअर निर्माते आहेत ते आपल्या वेबसाईटवर प्राथमिक माहिती, व्हायरसेसची वर्णने व त्यावरचे उपाय, तसेच अफवा, पारिभाषिक शब्द, नवे व्हायरस व त्यांच्या बातम्या ही सामुग्री देत असतात. पीसीसिलीनच्या 'ट्रेंड मायक्रो' कंपनीनेही ती दिली आहे. १९८९ साली सुरु झालेली ही कंपनी आता 'नॉर्टन' उत्पादनांसमोर स्पर्धेत बरीच मागे पडल्याचं दिसतय. Antivirus.com हे डोमेन नेम फार महत्वाचे आहे. असे नाव ह्या कंपनीने पटकावले कारण ह्या क्षेत्रातली ती एक जुनी खिलाडी आहे.



http://www.nai.com

'मॅक फी' च्या कंपनीचीच ही एक साईट

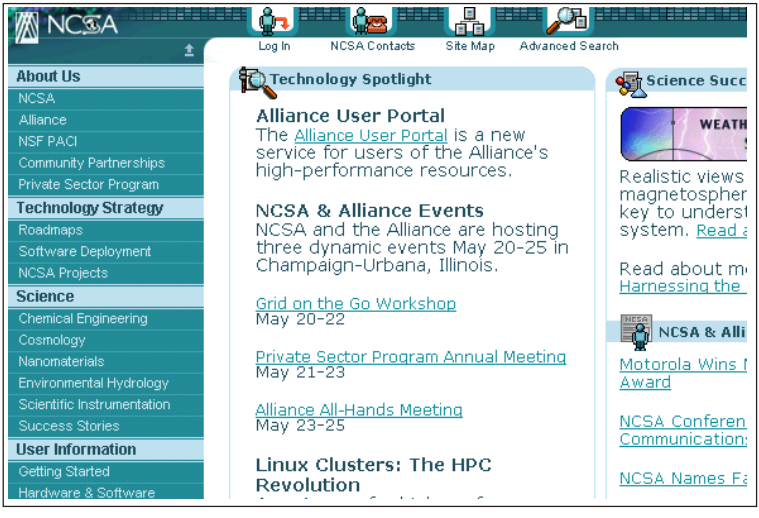


http://www.avp.com

'सेट्रंल कमांड' हे अँटी-व्हायरस सॉफ्टवेअर हळूहळू स्पर्धेत येत आहे.

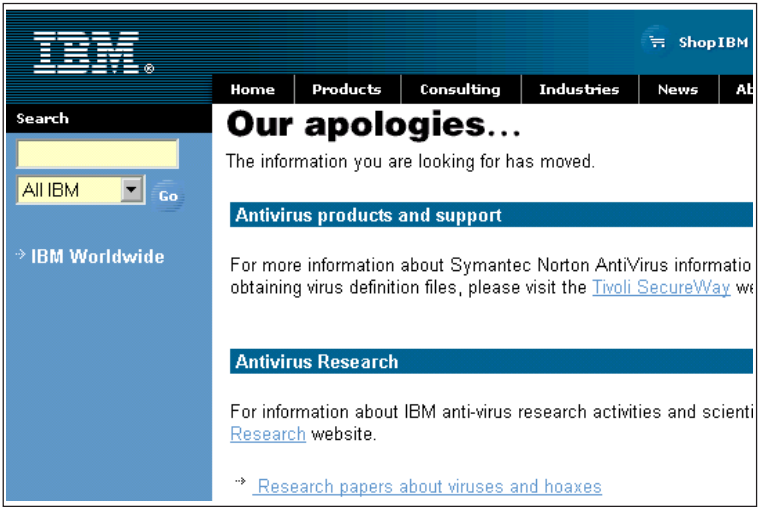
http://www.quickheal.com/default.htm

'क्वीक हील' हा एक लोकप्रिय भारतीय अँटी-व्हायरस प्रोग्राम



http://www.ncsa.uiuc.edu/

'नॅशनल कॉंप्युटर सेक्युरिटी ॲसोसिएशन'ची ही महत्वाची साईट



http://www.av.ibm.com

आय.बी.एम. पूर्वी अँटी व्हायरसला खूपच महत्व देत असे. आता त्यांना ते दिवस आठवावे लागतात.

http://www.cert.org

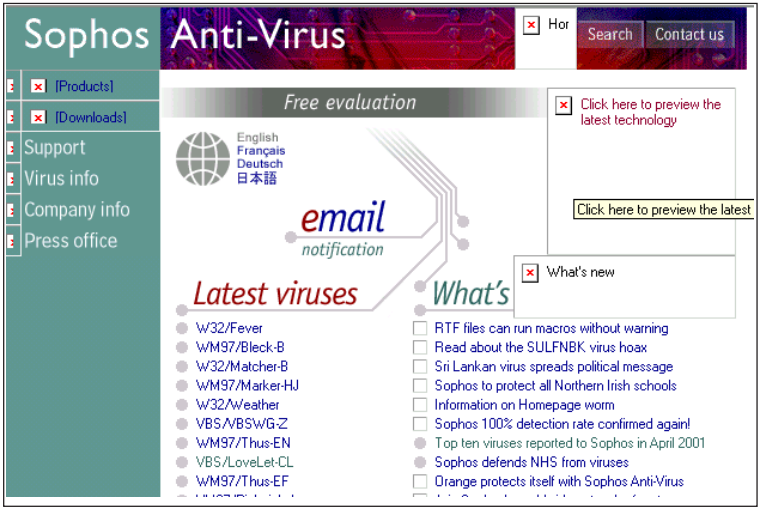
अमेरिकन सरकारची मदत घेऊन कॉंप्युटर सुरक्षेसाठी जनजागृती करणारी संस्था.

http://www.eicar.com

ह्या साईटवर एक साधी एका ओळीची फाईल आहे. ते कोड **malicious** आहे.
पण तो व्हायरस नव्हे त्याला **Test file** म्हणतात.

http://www.wildlist.org

एक महत्वाची संस्था. ही जगातील व्हायरसेसची यादी ठेवते



http://www.sophos.com

सोफोस ही एक चांगली व्हायरस साईट आहे. 'व्हायरस' हा विषय येथे सोप्या भाषेत समजावला गेला आहे.

http://www.grisoft.com

ए.व्ही.जी. अँटी व्हायरसची साईट. येथे मोफत डाऊनलोड उपलब्ध आहे.