ম্যালিসাস ভাইরাস থেকে ম্যাকের রক্ষাকবচ

তাসনীম মাহ্‌মুদ

কম্পিউটার জগৎ-এর নিয়মিত বিভাগ ব্যবহারকারীর পাতায় যেসব বিষয় উপস্থাপন করা হয়, তার বেশিরভাগই পিসিসংশ্লি-ষ্ট। কিন্তু সবাই যে পিসি ব্যবহার করেন, তা নয়। এ দেশে অ্যাপল ডিভাইস ব্যবহারকারী মোটেও কম নয়। এ সংখ্যা দিন দিন বাড়ছে। এর প্রধান কারণ হলো অ্যাপলের আকর্ষণীয় ডিজাইন ও সহজ ব্যবহারযোগ্যতা। এ ছাড়া রয়েছে অ্যাপল কমপিউটার কখনই ভাইরাসে আক্রান্ত হয় না এমন বদ্ধমূল ধারণা।

অ্যাপল ডিভাইস ভাইরাসমুক্ত এমন ধারণা দীর্ঘদিন ধরে সত্য হিসেবে বিবেচিত হলেও, তা এখন ভুল হিসেবে প্রমাণিত। সম্প্রতি হাজার হাজার অ্যাপল ডিভাইসকে ভাইরাস আক্রান্ত হতে দেখা যাচ্ছে। এ লেখায় ব্যবহারকারীদের উদ্দেশে ব্যাখ্যা করে দেখানো হয়েছে ম্যাক কমপিউটারকে রক্ষা করার জন্য সফটওয়্যার প্যাচ, অ্যান্টিভাইরাস স্ক্যানিং টুল কীভাবে কাজ করে।

ব্যবহারকারীর উচিত তাদের ম্যাক পিসির সুরক্ষার জন্য সিকিউরিটি সেটিং চেক করা। গত কয়েক বছর ধরে অ্যাপলের জনপ্রিয়তা খুবই দ্রুত বেড়ে চলেছে। বিশেষ কর অ্যাপলের জন্য আইফোন এবং আইপ্যাড মোবাইল বিশ্বের এক বিরাট অংশ কর্তৃত্ব করছে। সম্প্রতি ম্যাক ব্র্যান্ডের রেঞ্জের ডেস্কটপ এবং ল্যাপটপ কমপিউটারে বেশ কিছু গুরুত্বপূর্ণ বহিরাক্রমণের লক্ষণ দেখা যায়, যা আগে শুধু বিবেচনা করা হতো মাইক্রোসফট উইন্ডোজচালিত পিসি'র ক্ষেত্রে। অথচ এর আগে আরো কয়েক বছর ধরে অ্যাপলপ্রেমীদের সংযত করা হয়েছিল এ ধারণা দিয়ে যে, অ্যাপলের সব পণ্য সব ধরনের ভাইরাস এবং ক্ষতিকর সফটওয়্যার সংক্রমণ থেকে নিরাপদ, যা উইন্ডোজ কমপিউটারের মতো সংক্রমণপ্রবণ নয়। এমনটি বলার যৌক্তিক কারণ হলো অ্যাপল তার প্রতিটি পণ্যের সর্বশেষ উপাদানকে নিয়ন্ত্রণ করে। অর্থাৎ তার সব পণ্যের হার্ডওয়্যার কম্পোনেন্ট থেকে শুরু করে অপারেটিং সিস্টেম পর্যন্ত সবকিছু নিয়ন্ত্রণ করে। তাই সিস্টেমের ভেতরে ভাইরাস বা ক্ষতিকর কোনো প্রোগ্রামের অ্যাক্সেস করা বেশ কঠিন হয়ে পড়ে। তবে সম্প্রতি লাখ লাখ অ্যাপল ম্যাক কমপিউটার নোংরা ভাইরাসে আক্রান্ত হয়, যেগুলো ব্যবহারকারীর কার্যকলাপ লক্ষ রাখতে থাকে। সুতরাং আপনি যদি বিশ্বাস করেন অ্যাপল ম্যাক, আইফোন বা আইপ্যাড অভেদ্য বা ইনভালনারেবল, তাহলে বর্তমান প্রেক্ষাপটে বলা যায়, এ বিষয়ে আপনাকে নতুন করে ভাবতে হবে।

সিকিউরিটি বেসিক

ব্যবহারকারীরাই হলেন কমপিউটারের নিরাপত্তার ক্ষেত্রে সবচেয়ে দুর্বলতম লিঙ্ক। আর এ ক্ষেত্রেই উইন্ডোজচালিত কমপিউটার অ্যাপল ডেস্কটপ এবং ল্যাপটপ কমপিউটারের চেয়ে চিহ্নিতভাবে এগিয়ে আছে। অ্যাপলের ডেস্কটপ অপারেটিং সিস্টেম ম্যাক ওএসএক্সের লুক ও ফিল অনেকটাই উইন্ডোজের মতো, তবে ম্যাকের পাসওয়ার্ডের জটিল সিস্টেম এবং 'permission' চেক করে দেখে ম্যাক কমপিউটারে সবচেয়ে গুরুত্বপূর্ণ ফাইলে কে এবং কী অ্যাক্সেস করতে পারবে, যা মূলত সিস্টেমকে অনেক বছর ধরে হুমকিমুক্ত রেখেছিল। এ কারণে ম্যাক সমর্থকরা বিশ্বাস করতেন উইন্ডোজ ব্যবহারকারীদের উচিত ম্যাকে সুইচ করা।

সহজ ভাষায় বলা যায়, ম্যাক ওএসএক্সের মূল অংশ সমতুল্য উইন্ডোজের বিভিন্ন ভার্সনের তুলনায় অনেক বেশি সুরক্ষিত। কেননা ম্যাক ওএস অপারেটিং সিস্টেমের সবচেয়ে গুরুত্বপূর্ণ অংশে অ্যাক্সেস করা ভাইরাস রচয়িতার পক্ষে অনেক কঠিন।

আরেকটি অবশ্যম্ভাবী সত্য হলো দীর্ঘদিন ধরে অ্যাপলের পণ্য ভাইরাস রচয়িতাদের আকৃষ্ট করার জন্য তেমন জনপ্রিয় ছিল না। যেহেতু অ্যাপল ব্যবহারকারীর সংখ্যা উইন্ডোজ পিসি ব্যবহারকারীর তুলনায় অনেক কম, তাই স্বাভাবিকভাবে ভাইরাস রচয়িতারা অ্যাপলকে

চিত্র-১ : ফ্ল্যাশব্যাক ম্যালওয়্যার টুল অপসারণ করা

টার্গেট না করে বিশাল ব্যবহারকারীর ক্ষেত্র উইন্ডোজকে টার্গেট করেন, অর্থাৎ উইন্ডোজ পিসি স্বত্বাধিকারীদেরকে টার্গেট করেন। সবচেয়ে উদ্বেগের বিষয় ক্ষতিকর কোডের দরকার বিপুলসংখ্যক ব্যবহারকারীর সম্পৃক্ততা।

ত্রুটি দূর করা

অ্যাপল ম্যাক কমপিউটার ২০১২ সালে ক্র্যাক হওয়ায় আমাদেরকে একটু পেছনে ফিরে যেতে হচ্ছে। এ বছরের শুরুতে একটি ট্রোজান বিস্তার লাভ করে, যা আপাতদৃষ্টিতে প্রয়োজনীয় অ্যাপ্লি-কেশন হিসেবে মনে হলেও এটি আসলে ধারণ করে কিছু গোপন অমঙ্গলকারী কোড, যা নিজে নিজেই ইনস্টল হয় প্রায় পাঁচ লাখের বেশি ম্যাকে।

এফ-সিকিউর (F-Secure)-এর প্রধান গবেষণা কর্মকর্তা মিকো হাইপোনেন (Mikko Hypponen) মনে করেন, অ্যাপলের সব পণ্যের শতকরা একভাগ ব্যবহারকারী সম্ভবত ভাইরাস আক্রান্ত। অন্যদিকে রাশিয়ায় অ্যান্টিভাইরাস গবেষণা প্রতিষ্ঠানের তথ্যে দেখা গেছে যুক্তরাজ্যের মোট ম্যাক ব্যবহারকারীর শতকরা ১২ ভাগ ভাইরাস আক্রান্ত।

Backdoor.Flashback নামের ট্রোজান সংক্রমিত পিসির প্রতিটি কি প্রেসের লগ করে এবং যারা এটি তৈরি করেছেন তাদের কাছে এর রিপোর্ট পাঠায়। তাই যেকোনো একক দিনের লগিংয়ে ক্যাপচার হতে পারে আপনার ক্রেডিট কার্ড নম্বর, ব্যাংক অ্যাকাউন্ট লগইন ডিটেইলস ইত্যাদি। এসব তথ্য ডিজিটাল গোল্ড ডাস্ট হিসেবে বিবেচিত ট্রোজান সৃষ্টিকারীদের কাছে। কেননা তাদের কাছে এমন সফটওয়্যার আছে, যা এসব ডিজিটাল ডাস্ট থেকে গুরুত্বপূর্ণ তথ্য বের করে আনতে পারে। তাই ব্যবহারকারীদের উচিত তাদের কমপিউটার রক্ষার জন্য নিয়মিতভাবে সিকিউরিটি সেটিং চেক করা।

ফ্ল্যাশব্যাকের আবির্ভাব ঘটে ম্যাকে আক্রমণ করার জন্য। কোড সংবলিত সামাজিক নেটওয়ার্ক যেমন টুইটার বা ফেসবুক ওয়েবসাইটের লিঙ্কে ক্লিক করলে সংক্রমিত হওয়ার সম্ভাবনা থাকে বেশি জাভার ম্যাক এডিশনের সিকিউরিটি হোলের মাধ্যমে। এই ক্রস প-াটফরম ল্যাঙ্গুয়েজ ব্যবহার হয় সাইটকে অধিকতর ইন্টারেক্টিভ করার জন্য এবং সেইসব অ্যাপ্লি-কেশন রান করানোর জন্য, যা বিশেষভাবে আপনার কমপিউটারের জন্য ডেভেলপ করা হয়নি।

অবশ্য জাভা অ্যাপলের জন্য নয়। সুতরাং অনেকেই যুক্তি দেখাতে পারেন, এ ধরনের ফাটল বা চিড় ধরার জন্য অ্যাপলকে খুব সামান্যই দায়ী করা হয়। আসলে অ্যাপল মেইনটেইন করে জাভার জন্য এর নিজস্ব ভার্সন। যদিও ফ্ল্যাশব্যাক ট্রোজানের রিপোর্ট প্রকাশিত হয় ফেব্রুয়ারি ২০১২-তে এবং তা দৃঢ়ভাবে থাকে ৩ এপ্রিল পর্যন্ত ম্যাক ওএসএক্স আপডেট ভার্সন অবমুক্ত হওয়ার আগ পর্যন্ত। ওরাকল ডেভেলপ করে জাভার উইন্ডোজ ভার্সন, যা প্রবর্তন করে পিসি ব্যবহারকারীদের জন্য এক ফিক্স।

এখানে সবচেয়ে মারাত্মক বিষয় হলো অ্যাপলের ডেভেলপ করা প্যাচ অ্যাপ-াই করা যায় শুধু অ্যাপল অপারেটিং সিস্টেমের সর্বশেষ দুই ভার্সনে, যেমন স্নো লিওপার্ড (Snow Leopard) এবং লায়ন (Lion) অপারেটিং সিস্টেমে। যার অর্থ হচ্ছে এখনো যারা আগে থেকে ম্যাকের পুরনো ভার্সন ব্যবহার করছেন, তাদের উচিত হবে জাভাকে ডিজ্যাবল করে সাফারি চালু করা। এ জন্য সাফারি মেনু ওপেন করে Preferences ▸

বেছে নিতে হবে। এবার Security-তে ক্লিক করে Enable Java বক্স থেকে টিক অপসারণ করার জন্য ক্লিক করতে হবে।

এর বিকল্প হিসেবে সিমেনটেকের ফ্ল্যাশব্যাক-রিমোভাল টুল ডাউনলোড করে রান করতে পারেন। ম্যাকে ট্রোজান চেক করার জন্য ব্যবহার করা হয় ম্যাকে টেক্সটভিত্তিক অ্যান্টারপাইনিং টুল। এই টুল যদি কিছু শনাক্ত করতে পারে তাহলে তা অপসারণ করুন।

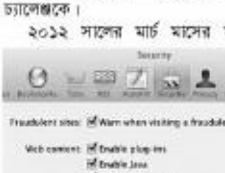
যদি আপনি স্নো লিওপার্ড বা লায়ন ব্যবহার করেন, তাহলে মেনুবারের আইকনের পরিবর্তে Apples own fix (or path) অ্যাপ-ই করুন। এরপর Software Update সিলেক্ট করে Install-এ ক্লিক করুন আপডেট প্রয়োগ করার জন্য।

ম্যাককে নিরাপদ রাখা

যদি পরিচিত কোনো সমস্যা সমাধান করতে অ্যাপল দীর্ঘ সময় নেয় এবং পুরনো মেশিনকে অনিরাপদভাবে রেখে দেয়া হয়, তাহলে আপনাকে নিরাপত্তার জন্য এখন থেকেই ভাবতে হবে। গত কয়েক যুগ ধরে উইন্ডোজ ব্যবহারকারীরা সিস্টেমের নিরাপত্তার জন্য যেভাবে অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করে আসছেন, ম্যাক ব্যবহারকারীকেও সে ধরনের অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করতে হবে কি না?

ম্যাকের জনপ্রিয়তা বাড়ার সাথে সাথে এ ক্ষেত্রে হ্যাকারদের সংখ্যাও বাড়ছে, কেননা হ্যাকার বা ক্ষতিকর ভাইরাস রচয়িতাদের টার্গেট বিপুলসংখ্যক ব্যবহারকারী। তাই কেউ কেউ এই জনপ্রিয় কমপিউটিং প্ল্যাটফরমকে কাজে লাগিয়ে উপভোগ করছেন নতুন এই চ্যালেঞ্জকে।

২০১২ সালের মার্চ মাসের মাঝামাঝিতে



চিত্র-২ : সিকিউরিটি প্রিফস

ট্রেন্ড মাইক্রোর থ্রেড রিসার্চ ম্যানেজার ইভান ম্যাকলিন্টাল মাইক্রোসফট ওয়ার্ড ডকুমেন্ট অ্যাটাচমেন্টসহ এক সিরিজ ই-মেইলের বিবরণ পেশ করেন, যেখানে দাবি করা হয় তিব্বতের মানবাধিকারের সমর্থনের কথা। আসলে এটি ছিল ওএসএক্সের জন্য মাইক্রোসফট ওয়ার্ডের দুর্বলতাকে কাজে লাগানো। এর দু'সপ্তাহ পর এমন ঘটনার আবার আবির্ভাব ঘটে। এ সময় সামান্য টোয়েক হয়। তবে ওএসএক্সে তা মাইক্রোসফট অফিসের সাথে থেকে যায়। এপ্রিলের মাঝামাঝিতে অ্যান্টিভাইরাস বিশ্লেষক ক্যাসপারস্কির সিকিউর লিস্ট সার্ভিস প্রকাশ করে সাবপাব (SabPub), যা ম্যাকে জাভার আরেকটি হুমকি। এটি ছিল স্পষ্ট ফ্ল্যাশব্যাক, যা শুধু একবারই ঘটেনি। সুতরাং এখন প্রশ্ন দেখা দিয়েছে, ম্যাকের নিরাপত্তার জন্য আমরা কী করতে পারি? এর সহজতম উপায় হলো সফটওয়্যার প্যাচ দিয়ে সবসময় আপডেট থাকা। অ্যাপল তার নিজের অর্থাৎ ইন-হাউস অ্যাপি-কেশনের জন্য ফিক্স অবমুক্ত করে নিয়মিতভাবে। এর সাথে সম্পৃক্ত থাকে আইওয়ার্ক, আইলাইফ এবং ওএসএক্স। বাইডিফল্ট সপ্তাহে একবার এগুলো চেক করার জন্য ম্যাকে সেট করা থাকে।

চেক করে দেখুন এই অপশন ডিজ্যাবল করা হয়নি। এ জন্য মেনুবারে অ্যাপ আইকনে ক্লিক করুন এবং System Performances-এ ক্লিক করে Software Update-এ ক্লিক করান।

এবার নিশ্চিত হয়ে নিন যে 'Check for updates' এবং 'Download updates automatically' উভয় অপশনের বক্সের পাশে টিক করা আছে কি না। ফ্রিকোয়েন্সিকে Weekly to Daily-তে পরিবর্তন করার জন্য ঐচ্ছিকভাবে ড্রপডাউন মেনু ব্যবহার করতে পারেন। এবার এই স্ক্রিন থেকে Check Now অথবা অ্যাপল মেনু থেকে Software Update সিলেক্ট করতে পারেন ম্যানুয়াল চেক কার্যকর করার জন্য।

অ্যাপল ওএসএক্সের প্রত্যেক নতুন রিলিজের সাথে সাথে সিকিউরিটির শক্তি বাড়ানো হয়। সুতরাং যখনই অ্যাপ স্টোরে নতুন ভার্সন সম্পৃক্ত করা হয়, তখনই অ্যাপল আপগ্রেড করতে হয়। সবচেয়ে বিস্ময়কর বিষয় এসব আপগ্রেড দিন দিন সস্তা হচ্ছে। মাউন্টেন লায়ন, ওএসএক্স ১০.৮ যা অতিসম্প্রতি অবমুক্ত করা হয়, এতে সম্পৃক্ত করা হয় গেইটকিপার (Gatekeeper) নামে এক সিকিউরিটি ফিচার, যা এই টুলকে সহজতর করেছে অ্যাপি-কেশনগুলোকে আলাদা করার জন্য।

যদি আপনার ম্যাক সর্বশেষ অপারেটিং সিস্টেম রান করানোর জন্য অনেক পুরনো হয়ে থাকে, তাহলে আপনার হার্ডওয়্যারকে আপগ্রেড করে নিতে পারেন। নরটন অ্যান্টিভাইরাস ১২ ম্যাকের জন্য, এটি ই-মেইল এবং আইচ্যাট মেসেজ স্ক্যান করতে পারে, স্পাইওয়্যার শনাক্ত এবং সাইবার অপরাধ প্রতিহত করতে পারে, যা নন-অ্যাপল অ্যাপি-কেশন টুলের হোল ব্যবহার করে ম্যাকে অ্যাক্সেসের জন্য চেষ্টা করে। এর জন্য দরকার ইন্টেল কোর ২ ডুয়ো প্রসেসরসহ ম্যাক, ২ গি.বা. মেমরি এবং ম্যাক ওএসএক্স ১০.৭ বা তদূর্ধ্ব।

ম্যাক হোম এডিশনের জন্য সোফোস অ্যান্টিভাইরাস একটি ফ্রি বিকল্প টুল। এই টুল পাওয়ার পিসিভিত্তিক ম্যাকে রান করতে পারে, যা ম্যাক ওএসএক্স ১০.৪ বা তদূর্ধ্ব ভার্সনে রান করে। সুতরাং এই টুল পুরনো ম্যাক মেশিনেও রান করা যাবে। সোফোস অ্যান্টিভাইরাস এর ম্যাক হোম এডিশন টুলটির থ্রেডকে কোয়ারান্টাইন করে ক্ষতিকর ফাইলগুলোকে বিনা খরচে সরিয়ে নেয় এবং রিকোভার করে এরোনাস মিলিয়ে দেখে।

ম্যাক সীমানা ছাড়িয়ে

অ্যাপল আইওএসকে আপাতদৃষ্টিতে নুলেট প্রুফ অপারেটিং সিস্টেম মনে করা হয় যা সাপোর্ট করে আইপ্যাড, আইফোন এবং আইপড টাচ। গত গ্রীষ্মকালে অ্যাপলের মোবাইল অপারেটিং সিস্টেমের একজন ডেভেলপার চার্লি মিলার আইওএসের এক মারাত্মক ত্রুটি দৃষ্টিগোচরে আনার পর অ্যাপল বাধ্য হয় তার মোবাইল অপারেটিং সিস্টেমের প্যাচ করতে।

আপাতদৃষ্টিতে লক হওয়া আইফোনে কিভাবে অ্যাপস ইনস্টল করতে হয়, তার টেকনিক্যাল সবকিছুই এটি অনুমোদন করে এবং রিট্রাইভ করতে পারে সম্ভাব্য ইউজার ফটো কন্টাক্ট ও ডাটা। অ্যাপল আইওএস ডেভেলপার প্রোগ্রাম থেকে মিলারকে বের করে দেয়

চিত্র-৩ : স্টোর হওয়া ওয়েবসাইট যা ব্রাউজারকে ট্র্যাক করবে

সম্পাদিত কাজের কৃতিত্ব প্রকাশ করার জন্য এবং ব্যবহারকারীকে অফার করে এক আপডেট। তবে পুরনো ডিভাইস যেমন প্রথম ও দ্বিতীয় প্রজন্মের আইপড টাচেস এবং মূল আইফোন ও আইফোন থ্রিজিতে এটি প্রয়োগ করা যায় না।

এমনকি সর্বাধুনিক হার্ডওয়্যার এবং সবচেয়ে আপ-টু-ডেট সফটওয়্যার প্যাচ আইওএস, ওএসএক্স এবং থার্ডপার্টি অ্যাপি-কেশন সবকিছুই সাইবার হামলার শিকার হতে পারে। সন্দেহাতীতভাবে বলা যায় সামাজিক নেটওয়ার্ক যেমন ফেসবুক, টুইটার প্রত্যেক ব্রডকাস্টারের মাধ্যমে ঝুকিপূর্ণ।

সুতরাং মনে রাখতে হবে, এখন অ্যাপল পণ্য আর বাইরের হুমকি থেকে সম্পূর্ণ নিরাপদ নয়। যেমন ফিশিং ওয়েবসাইট, অন্যান্য কমপিউটার বা ডিভাইস। সুতরাং অযাচিত ই-মেইল সংবলিত লিঙ্কে ক্লিক করা থেকে বিরত থাকা উচিত, বিশেষ করে যেগুলো অনলাইন ব্যাংক থেকে অবির্ভূত হয়।

শেষ কথা

দীর্ঘদিন ধরে ম্যাক ব্যবহারকারীরা উইন্ডোজ ব্যবহারকারীদের চেয়ে এগিয়ে ছিলেন নিরাপত্তার দৃষ্টিকোণ থেকে। তবে এখন পরিস্থিতি বদলাতে শুরু করেছে। ম্যাক ওএসের ডিজিটাল হুমকির মাত্রা দিন দিন বাড়ছে, তবে তা উইন্ডোজের তুলনায় কম। যদিও ফ্ল্যাশব্যাক এবং সাবপাব ট্রোজান সম্পূর্ণরূপে নিরাপদ হিসেবে দেখা যাচ্ছে না। তাই ম্যাককে আপটুডেট রাখা সম্ভব, যদি সাধারণ কিছু বোধ বা সেন্স প্রয়োগ করা যায়। একই বিষয় প্রযোজ্য আইওএসের ক্ষেত্রে। তবে সবারই উচিত ম্যাকভিত্তিক সিকিউরিটি টুল ইনস্টল করে ব্যবহার করা।

ফিডব্যাক : mahmood_sw@yahoo.com