হার্ডডিস্কে স্বয়ংক্রিয় ম্যালওয়্যার ছড়ানো

সোহেল রানা

মার্কিন যুক্তরাষ্ট্রের একটি গোয়েন্দা সংস্থা বাংলাদেশসহ ৩০টিরও বেশি দেশের কমপিউটারের হার্ডডিস্কে গোপন সফটওয়্যার ব্যবহারের মাধ্যমে নজরদারি চালাচ্ছে। রাশিয়া থেকে অ্যান্টিভাইরাস নির্মাতা প্রতিষ্ঠান ক্যাসপারস্কি সম্প্রতি এই তথ্য জানিয়েছে। আর সম্পূর্ণ প্রতিবেদনটি 'ইকুয়েশন গ্রুপ : কোয়েশ্চনস অ্যান্ড আনসারস' নামে প্রকাশও করেছে প্রতিষ্ঠানটি।

প্রতিবেদন থেকে জানা গেছে, গোপন সফটওয়্যারটির মাধ্যমে সার্বক্ষণিক নজরদারিতে থাকছেন একজন ব্যবহারকারী। আর জনপ্রিয় সব ব্র্যান্ডের হার্ডডিস্কেই রয়েছে এই গোপন সফটওয়্যার। তোশিবা, স্যামসাং, ম্যাক্সটর, সিগেট কিংবা ওয়েস্টার্ন ডিজিটাল, বাদ পড়েনি কোনো ব্র্যান্ডই।

ক্যাসপারস্কির তথ্যানুযায়ী, গোয়েন্দারা এমন একটি প্রযুক্তি উদ্ভাবন করে তা কাজে লাগাচ্ছে, যাতে অস্পষ্ট কোডের ক্ষতিকর সফটওয়্যার বা ফার্মওয়্যার প্রতিবার কমপিউটার চালুর সময় সক্রিয় হয়ে ওঠে। ডিস্ক ড্রাইভে এ ধরনের ফার্মওয়্যারকে গোয়েন্দা ও সাইবার নিরাপত্তা বিশেষজ্ঞেরা পিসি হ্যাকারের জন্য গুরুত্বপূর্ণ সম্পদ বলেই মনে করেন। বায়োস কোডে স্বয়ংক্রিয় সফটওয়্যার ইনস্টলের পরেই ফার্মওয়্যারকে গুরুত্বপূর্ণ বলে ধরা হয়।

ক্যাসপারস্কির গবেষক কোস্টিন রায়ু বলেছেন, এই হার্ডওয়্যারের কারণে কমপিউটার বারবার আক্রান্ত হতে থাকে। এই ম্যালওয়্যার যারা ছড়ানোর কাজ করেন, তারা শত শত পিসিকে নিয়ন্ত্রণ করতে পারেন এবং সেখান থেকে ফাইল সরানো বা নজরদারির সব কাজ সারতে পারেন দূরে বসেই। কিন্তু তারা সব কমপিউটারে এ ধরনের কাজ করেন না। বেশিরভাগ ক্ষেত্রে যারা তাদের লক্ষ্যবস্তু হিসেবে পরিণত হন, তাদেরই শুধু আক্রমণ চালানো হয়। এখন পর্যন্ত ৩০ দেশে ৫০০ ভুক্তভোগীর সন্ধান পেয়েছে ক্যাসপারস্কি।

ক্যাসপারস্কি দাবি করেছে, যাদের হাতে সোর্স কোড থাকে শুধু তারাই এ ধরনের ম্যালওয়্যার ঢোকাতে পারেন। সাধারণ মানুষের পিসির তথ্য ব্যবহার করে সোর্স কোড ছাড়া হার্ডড্রাইভের অপারেটিং সিস্টেম রিরাইট করা সম্ভব নয়। এনএসএ কীভাবে সোর্স কোড পেয়েছে সে বিষয়টিও পরিষ্কার নয়। ক্যাসপারস্কির মতে, নজরদারিতে থাকা দেশগুলোর মধ্যে রয়েছে রাশিয়া, ভারত, পাকিস্তান, চীন, সিরিয়া, মালি, ইরান, যুক্তরাজ্য, জার্মানি, তুরস্কসহ প্রভৃতি দেশ। এসব দেশের বিভিন্ন খাতের প্রতিষ্ঠানে হার্ডডিস্কের এই গোপন সফটওয়্যারের মাধ্যমে নজরদারি চালিয়ে যাচ্ছে গোয়েন্দা সংস্থা। এর মধ্যে আছে সরকারি প্রতিষ্ঠান, আর্থিক প্রতিষ্ঠান, স্বাস্থ্য খাতের প্রতিষ্ঠান, দূতাবাস, সামরিক সংস্থা, টেলিযোগাযোগ সংস্থা, শিক্ষাপ্রতিষ্ঠান, সংবাদমাধ্যম প্রভৃতি।

ক্যাসপারস্কির বিশেষজ্ঞ ইগর সোমেনকভ জানিয়েছেন, এই গোপন সফটওয়্যার থেকে সুরক্ষার কার্যকর উপায় হচ্ছে এ ধরনের হার্ডড্রাইভ পুরোপুরি নষ্ট করে ফেলা। কারণ, এ ধরনের সফটওয়্যার এমনভাবে হার্ডড্রাইভে লুকানো থাকে যাতে ড্রাইভ ফরম্যাট দিয়ে, নতুন করে ফ্ল্যাশ দিয়ে আবার ইনস্টল করলেও তা থেকে মুক্তি মেলে না। এই সফটওয়্যার দক্ষ সাইবার বিশেষজ্ঞ ছাড়া শনাক্ত করা সম্ভব নয়। যেকোনো উইন্ডোজচালিত পণ্য এবং উইন্ডোজ ছাড়াও অন্যান্য ওএস, হার্ডড্রাইভ ফার্মওয়্যার এমনকি ইউএসবি স্টিক ও সিডিতেও এ ধরনের ম্যালওয়্যার ছড়িয়ে দিতে পারে ইকুয়েশন গ্রুপটি।

ক্যাসপারস্কির গবেষকেরা আরও জানিয়েছেন, এই গোপন কৌশল বের করতে তারা দুই সপ্তাহের বেশি সময় নিয়ে বিস্তর গবেষণা করে একটিমাত্র ক্রিপটোগ্রাফিক উপাদান বের করতে সক্ষম হন।

গবেষকেরা বলছেন, এই বিষয়টি ব্যবহারকারী কীভাবে গ্রহণ করছেন তার ওপর নির্ভর করে। অন্যদিকে আক্রমণকারীরা কিন্তু তাদের সুনির্দিষ্ট লক্ষ্যে কাজ করে যাচ্ছে। কাকে কখন আক্রমণ করতে হবে, তা তাদের হাতের নাগালেই থাকে।

সম্প্রতি কানাডার ভ্যানকুভারে অনুষ্ঠিত ক্যানসেকওয়েস্ট সিকিউরিটি কনফারেন্সে কমপিউটার নিরাপত্তা বিশেষজ্ঞ জেনো কোভাহ এবং কোরে ক্যালেনবার্গ দেখিয়েছেন কীভাবে বায়োস চিপের মাধ্যমে হ্যাকিং হয়। বায়োস চিপ একটি কমপিউটারের মাদারবোর্ডে ফার্মওয়্যারের মাধ্যমে ধারণকারী মাইক্রোচিপ। বায়োস একটি কমপিউটার বুট করে এবং অপারেটিং সিস্টেম লোড করতে সাহায্য করে। এই মূল সফটওয়্যারে সংক্রমণ করে, যা কি না অ্যান্টিভাইরাস এবং অন্যান্য নিরাপত্তা পণ্যের নিচে পরিচালিত হয় এবং সাধারণত এগুলো স্ক্যান করে না অ্যান্টিভাইরাস। ফলে গুপ্তচরেরা খুব সহজেই এখানে ম্যালওয়্যার দিয়ে দিতে পারে এবং এই ম্যালওয়্যার কমপিউটারের অপারেটিং সিস্টেম মুছে ফেললে বা পুনরায় ইনস্টল করলেও থেকে যায়। পরবর্তী সময়ে হ্যাকিং আক্রমণ দূর থেকে ই-মেইলের মাধ্যমে অথবা সিস্টেমে ফিজিক্যাল ইন্টারডিসকাশনের মাধ্যমে করা যায়। উইয়ার্ড রিপোর্ট অনুযায়ী গবেষকেরা একে 'ইনকারশন ভলনারেবিলিটিস' বলেন, যে উপায়ে হ্যাকারেরা প্রায় সব কমপিউটারে প্রবেশ করতে পারে কজ