সাইবার হামলা ও হানিপট

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

হানিপট বিষয়টি অনেকটা ফাঁদের মতো। সাইবার নিরাপত্তায় এর ব্যবহার বেশ কার্যকর। হানিপট সাধারণত মূল সিস্টেমের রেপ্লিকা তৈরি করে করা হয়। যদি কোনো সময় কোনো হ্যাকার সিস্টেমের নিরাপত্তা বেষ্টনী ভেঙে ঢুকে পড়ে, তবে তাকে ধোঁকা দেয়ার জন্য সাধারণত মূল সিস্টেমের মতো করে অন্য একটি সিস্টেম তৈরি করে রাখা হয়, যাতে সে বুঝতে না পারে যে সে আসলে নকল সিস্টেমে ঢুকেছে। এভাবে মূল সিস্টেমের নিরাপত্তা নিশ্চিত করা হয়।

ইন্টারনেটে মন ভোলানো ডিজিটাল ফাঁদ তৈরি করে শনাক্ত করা হয় সাইবার হামলা। এরপর সেগুলো ইন্টারনেটে সরাসরি প্রদর্শন করা হচ্ছে 'সিকিউরিটি-ও-মিটার' নামের এক ব্যবস্থা ব্যবহার করে। জার্মানির ডয়চে টেলিকম তৈরি করেছে এই ব্যবস্থা। কমপিউটারে ভাইরাস আক্রান্তের কথা খুব কম মানুষই সাথে সাথে বুঝতে পারে। বেশিরভাগ ক্ষেত্রেই এসব ভাইরাস ছড়ায় ই-মেইলের মাধ্যমে। সাধারণত এ ধরনের মেইল খুবই মজাদার বা কৌতূহলোদ্দীপক হয়। আর ই-মেইলের অ্যাটাচমেন্টে ক্লিক করলেই 'ছিঁচকে চোরের' মতো গোপনে কমপিউটারে ঢুকে যায় ভাইরাস। এরপর এই ভাইরাস কমপিউটারে থাকা বিভিন্ন তথ্য সংগ্রহ করতে থাকে। আর কমপিউটারটি যদি কোনো নেটওয়ার্কের সাথে যুক্ত থাকে, তাহলে সেই নেটওয়ার্কেও ছড়িয়ে পড়ে। এভাবে প্রতিদিন দুই লাখের বেশি নতুন ভাইরাস, ট্রোজান ও ওয়ার্ম ইন্টারনেটে ছড়াচ্ছে। সাধারণত ব্যক্তিগত কমপিউটার ও স্মার্টফোন, বিশেষ করে যেসব কমপিউটারে উইন্ডোজ অপারেটিং সিস্টেম ও স্মার্টফোনে অ্যান্ড্রয়িড অপারেটিং সিস্টেম ব্যবহার করা হয়, সেগুলো সাইবার হামলার শিকার হচ্ছে সবচেয়ে বেশি। তবে হ্যাকারদের আগ্রহ থাকে বিভিন্ন কর্তৃপক্ষ ও বড় ধরনের প্রতিষ্ঠানে হামলা চালানোর। যেসব কমপিউটারে উইন্ডোজ আর স্মার্টফোনে অ্যান্ড্রয়িড অপারেটিং সিস্টেম ব্যবহার হয়, সেগুলো সাইবার হামলার শিকার হচ্ছে সবচেয়ে বেশি।

জার্মান টেলিকমিউনিকেশন কোম্পানি ডয়চে টেলিকম সাইবার হামলা শনাক্ত ও প্রতিরোধে এক ভিন্ন ধরনের উদ্যোগ নিয়েছে। প্রতিষ্ঠানটি আইনি কাঠামোর মধ্যে থেকে একটি 'সিকিউরিটি-ও-মিটার' পদ্ধতি তৈরি করেছে, যা ব্যবহার করে বিভিন্ন ধরনের সাইবার হামলা সম্পর্কে তাৎক্ষণিক তথ্য সংগ্রহ করা সম্ভব হচ্ছে। সাইবার হামলা সম্পর্কিত এসব তথ্য সংগ্রহের সাথে সাথে জিশারহাইটসটাকো ডটইইউ ওয়েবসাইটে সেসবের বিস্তারিত প্রকাশ করছে ডয়চে টেলিকম। এভাবে বিভিন্ন নিরাপত্তা সংস্থার কাছে সাইবার হামলা সম্পর্কিত তথ্যও পৌঁছে দিচ্ছে কোম্পানিটি।

সম্ভাব্য সাইবার হামলা শনাক্তে হ্যাকারদের জন্য লোভনীয় ইলেকট্রনিক ফাঁদ তৈরি করেছে ডয়চে টেলিকম। এই ফাঁদ হ্যাকারেরা গিললেই টের পেয়ে যায় টেলিকম। এরপর প্রতিষ্ঠানটির তৈরি অনলাইন ব্যবস্থা সাইবার হামলার ধরন পর্যালোচনা করে ও প্রয়োজনীয় তথ্য জিশারহাইটসটাকো ডটইইউ ওয়েবসাইটে থাকা বিশ্ব মানচিত্রে প্রদর্শন করে। সেখানে হামলার উৎপত্তিস্থল সম্পর্কে সম্ভাব্য তথ্যও যোগ করা হয়।

ডয়চে টেলিকমের এই ব্যবস্থা থেকে প্রাপ্ত তথ্য পর্যালোচনা করে দেখা গেছে, বিশ্বের মধ্যে সবচেয়ে বেশি সাইবার হামলার উৎপত্তিস্থল রাশিয়া। শুধু ফেব্রুয়ারি মাসে সে দেশে সাইবার হামলার সংখ্যা ছিল ২৪ লাখ। এই তালিকায় দ্বিতীয় অবস্থানে রয়েছে তাইওয়ান, হামলার সংখ্যা ৯ লাখ। আর তৃতীয় অবস্থানে জার্মানি, সংখ্যা ৭ লাখ ৮০ হাজার।

অবাক করার মতো বিষয় হচ্ছে, ডয়চে টেলিকমের তালিকায় চীনের অবস্থান ১২তম। অথচ সাম্প্রতিক সময়ে মার্কিন বিভিন্ন গণমাধ্যম ও প্রতিষ্ঠানে সাইবার হামলার জন্য চীনের দিকেই আঙুল তুলেছেন অনেকে। তবে হামলার উৎপত্তিস্থলে হামলাকারী হ্যাকার অবস্থান করছে, এমনটা ভেবে নেয়াটা ঠিক নয়। সাধারণত সেখানে আক্রান্ত কমপিউটারটি থাকে। হ্যাকারেরা চায় যতগুলো সম্ভব ততগুলো কমপিউটারের নিয়ন্ত্রণ নিজেদের হাতে নিতে। এরপর তারা আক্রান্ত কমপিউটারগুলো নিজেদের মতো করে কাজে লাগায়।

হ্যাকারদের আক্রমণের শিকার বেশিরভাগ কমপিউটারই পুরনো কিংবা সেগুলোতে থাকা অপারেটিং সিস্টেম হালনাগাদ করা হয়নি। পুরনো অ্যান্টিভাইরাস ব্যবহার করা হয় এমন কমপিউটারও সহজে হ্যাকারদের আক্রমণের শিকার হয়ে থাকে। এসব কমপিউটার ব্যবহারকারীরা হয়তো অবসরে রয়েছেন। তারা নিয়মিত উইন্ডোজ আপডেট করেন না। অ্যান্টিভাইরাসের দিকে খেয়াল রাখেন না।

ডয়চে টেলিকমও এ ধরনের কমপিউটারকে ফাঁদ হিসেবে কাজে লাগাচ্ছে। একজন টিপিক্যাল উইন্ডোজ ব্যবহারকারীর মতো ভান করেন। যিনি কি না ইন্টারনেট ভালোভাবে ব্যবহার করেন না। তিনি সবকিছুতে ক্লিক করেন। সব অ্যাটাচমেন্ট খুলে দেখেন, আর ইন্টারনেট নিরাপত্তা সংক্রান্ত কোনো নিয়মনীতির তোয়াক্কা করেন না। বেশিরভাগ হামলা স্বয়ংক্রিয়। প্রাপ্ত তথ্য বিশ্লেষণ করে আমরা বলতে পারি, এ ধরনের হামলাকারীরা ইন্টারনেটে দুর্বল নিরাপত্তা ব্যবস্থাসম্পন্ন কমপিউটার খুঁজে বেড়ায়।

কিন্তু এসব হামলাই হ্যাকারদের একমাত্র কাজ নয়। তারা বড় বড় প্রতিষ্ঠানের নেটওয়ার্কে হামলা করে সুনির্দিষ্ট লক্ষ্য নিয়ে। তাদের উদ্দেশ্য থাকে বিভিন্ন ব্যক্তির মাস্টার কার্ড, ব্যাংক তথ্যসহ ই-মেইলের পাসওয়ার্ডের মতো গুরুত্বপূর্ণ তথ্য সংগ্রহ করা। এজন্য বিভিন্ন ধরনের 'ফিশিং' ই-মেইল ছড়িয়ে দেয় হ্যাকারেরা। এ ছাড়া স্টাক্সনেট, ফ্লেম কিংবা রেড অক্টোবরের মতো বড় সাইবার হামলা চালানো হয়েছে গোপনীয় ভূরাজনৈতিক ও সামরিক তথ্য সংগ্রহের জন্য। এসব হামলার পেছনে রয়েছেন চৌকস প্রোগ্রামারেরা। এসব হামলা স্বয়ংক্রিয় নয়। তারা পুরনো কমপিউটারের নিরাপত্তা ফাঁক খুঁজে বের করে এরকম হামলা চালান না।

ফলে ডয়চে টেলিকমের তৈরি করা মধুর ফাঁদে এরকম বড় ধরনের বিপজ্জনক সাইবার হামলা ধরা পড়বে না। আর এসব হামলা প্রতিরোধের জন্য এই পদ্ধতি তৈরি করাও হয়নি। তারা আসলে আগাম সতর্ক ব্যবস্থা হিসেবে 'সিকিউরিটি-ও-মিটার' তৈরি করেছে। তবে তারা এই ব্যবস্থা থেকে প্রাপ্ত তথ্য ব্যবহার করে আরও মজবুত নিরাপত্তা ব্যবস্থা তৈরি করতে চায়।

বিশ্বের আরও অনেক নামকরা কোম্পানি এরকম হানিপট তৈরি করে সেসব নেটওয়ার্কে বিভিন্ন অ্যাটাকের তথ্য পাবলিকলি শেয়ার করছে। এতে সবাই সেই ধরনের অ্যাটাক সম্পর্কে জানছেন ও সতর্ক হতে পারছেন। এ ছাড়া বিভিন্ন কোম্পানি তাদের নিজস্ব নেটওয়ার্কের ভেতরেও হানিপট কনফিগার করে রাখছে, যাতে হ্যাকারদের ধোঁকা দেয়া যায় বা তাদের অ্যাটাক সম্পর্কে আরও বিস্তারিত জানা যায়। অনেক ধরনের হানিপট তৈরি করা যায়, যেমন– পিউর হানিপট, হাই ইন্টারেকশন হানিপট ও লো ইন্টারেকশন হানিপট কজ

ফিডব্যাক : jabedmorshed@yahoo.com