২০১৯ সালে কেমন হবে সাইবার নিরাপত্তা পরিস্থিতি

গোলাপ মুনীর

বড় বড় করপোরেশন ও ওয়েবসাইটে সাইবার হ্যাকিং ২০১৮ সালেও অব্যাহত ছিল। আর অপরিহার্যভাবে ২০১৯ সালেও সাইবার নিরাপত্তার ক্ষেত্রেও সাইবার হ্যাকিং একটি অংশ হয়ে থাকবে। সদ্য শুরু হওয়া বছরটি আসতে না আসতেই বড় বড় ধরনের সাইবার সিকিউরিটি ও প্রাইভেসি প্রবণতার প্রচুর পরিমাণ আভাস-ইঙ্গিত আমরা পেতে পারি বিগত ১২ মাসের ঘটনাবলি থেকে। আজকের এই সময়ের পরিচিত ধরনের সাইবার হামলাগুলোর মধ্যে বড় বড় করপোরেশন ও ওয়েবসাইটে ২০১৮ সালে ঘটা সাইবার হ্যাক ২০১৯ সালেও অপরিহার্যভাবে চলতে থাকবে, সে কথা অনেক সাইবার সিকিউরিটি বিশ্লেষকই জোর দিয়ে বলছেন। বিশ্বব্যাপী অনেক সুপরিচিত সংগঠন ২০১৮ সালে উল্লেখযোগ্য পরিমাণে সাইবার হামলার শিকার হয়। সদ্য বিগত বছরটিতে সবচেয়ে বড় একক সম্ভাবনাময় ডাটালিঙ্ক মার্কেটিংয়ের ওপর ব্যাপক বিরূপ প্রভাব ফেলেছিল এবং ডাটা অ্যাগ্রেশন ফার্ম Exactis-এর ডাটাবেজেরও ক্ষতিসাধন করেছিল। এই ডাটাবেজে ছিল প্রায় ৩৪ কোটি পার্সোন্যাল ইনফরমেশন রেকর্ড।

সব সাধারণ সাইবার হামলার বাইরে ২০১৮ সালে সংঘটিত করপোরেট হামলা বিভিন্ন ধরনের টার্গেটে হামলার হুমকি এখন আরো বাড়িয়ে তুলেছে। সেই সাথে বাড়িয়েছে হামলার শিকারের সংখ্যা। সোশ্যাল নেটওয়ার্কিং জগতে ফেসবুক হিসাব দিয়েছে, হ্যাকারেরা গত বছর প্রায় ৩ কোটি লোকের ইনফরমেশন চুরি করেছে। ক্রমবর্ধমান সংখ্যায় জাতি-রাষ্ট্রগুলো সাইবার তদন্ত ও হামলা ব্যবহার করেছে করপোরেটের গোপন তথ্য থেকে শুরু করে স্পর্শকাতর সরকারি ও অবকাঠামো ব্যবস্থায় ঢুকে পড়তে। ব্যক্তিগত পর্যায়ে হেলথ ট্র্যাকার অ্যাকাউন্ট Under Armour's MyFitnessPal-এ ঢুকে পড়ে ১৫ কোটি লোকের ব্যক্তিগত তথ্য চুরি করে নেওয়া হয়। অতএব নতুন বছরে কী ধরনের সাইবার হামলার কথা আমরা চিন্তা করতে পারি? নিচে সে ধরনের কিছু সাইবার হামলার সম্ভাব্য প্রবণতা ও কর্মকান্ডের কথাই উপস্থাপন করা হচ্ছে, যেগুলো বিভিন্ন ধরনের সংগঠন, সরকার ও ব্যক্তির বেলায় ঘটতে পারে ২০১৯ সালে কিংবা তারও পরবর্তী সময়ে।

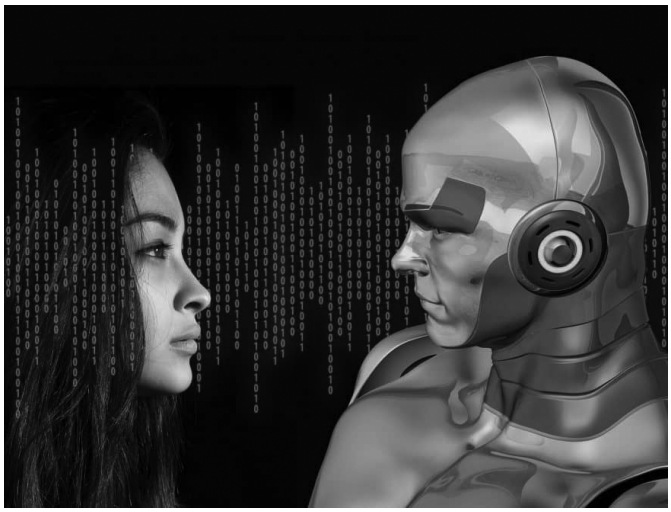
সাইবার হামলা ও কৃত্রিম বুদ্ধিমত্তা

সাইবার হামলাকারীরা কৃত্রিম বুদ্ধিমত্তা তথা আর্টিফিসিয়্যাল ইন্টেলিজেন্স (এআই) সিস্টেমসকে কাজে লাগাবে। এরা এআই ব্যবহার করবে হামলায় সহায়তা করার জন্য। এআইয়ের দীর্ঘ প্রতীক্ষিত বাণিজ্যিক প্রতিশ্রুতি বাস্তবায়ন শুরু হয়েছে সাম্প্রতিক বছরগুলোতে। বিজনেস অপারেশনের অনেক ক্ষেত্রে এআই-পাওয়ার্ড সিস্টেমের ব্যবহার ইতোমধ্যেই শুরু হয়ে গেছে। এমনকি এসব এআই সিস্টেম ম্যানুয়াল কাজ কেউ প্রত্যাশিত মাত্রায় স্বয়ংক্রিয় করে তুলছে। সেই সাথে সিদ্ধান্ত গ্রহণ প্রক্রিয়াসহ মানুষের অন্যান্য কাজকেও জোরদার করে তুলছে। একইভাবে এসব সিস্টেম প্রতিশ্রুতিশীল হয়ে উঠছে সাইবার হামলার জন্যও। কারণ, অনেক এআই সিস্টেম হচ্ছে বিপুল পরিমাণ ডাটারও হোম।

অধিকন্তু গবেষকেরা ক্রমবর্ধমান হারে এই সিস্টেম সম্পর্কে ক্ষতিকর ইনপুটের ব্যাপারে সংশয়েরও জন্ম দিয়েছেন, যা তাদের লজিককে করাপ্ট করতে পারে এবং তাদের অপারেশনের ওপর বিরূপ প্রভাব ফেলতে পারে। কিছু এআই টেকনোলজির ভঙ্গুরতা ২০১৯ সালের জন্য হবে কম বর্ধমান উদ্বেগের কারণ। কিছু কিছু উপায়ে টার্গেটে হামলার জন্য জটিল এআই সিস্টেমের উদ্ভব ঘটতে শুরু করেছিল ২০ বছর আগের ইন্টারনেটে। আর তা দ্রুত মনোযোগ কাড়ে সাইবার অপরাধী ও হামলাকারীদের, বিশেষ করে ইন্টারনেটভিত্তিক ই-কমার্সের বিস্ফোরণ শুরু হওয়ার পর।

ভবিষ্যতে সাইবার হামলাকারীরা শুধু এআই সিস্টেমকেই এর টার্গেটে পরিণত করবে না। এরা এদের নিজস্ব অপরাধ কর্মকান্ডকে অতি জোরালো করে তোলার জন্য এদের হামলার তালিকায় রাখবে এআই টেকনিকগুলোকেও। এআই পরিচালিত স্বয়ংক্রিয় সিস্টেমগুলো ব্যবহার করা যাবে অনুদঘাটিত ভঙ্গুরতাগুলো খুঁজে বের করার কাজে। চরমভাবে ▸

বাস্তবভিত্তিক ভিডিও ও অডিও তৈরি করে অথবা ওয়েল-ক্র্যাফটেড ই-মেইল ডিজাইন করে টার্গেটেড ব্যক্তিদের বোকা বানানোর কাজে কৃত্রিম বুদ্ধিমত্তাকে আরো অভিজাত উপায়ে ব্যবহার করা যাবে ফিশিং ও অন্যান্য সোশ্যাল ইঞ্জিনিয়ারিং অ্যাটাকে। তা ছাড়া কৃত্রিম বুদ্ধিমত্তাকে আরো ব্যবহার করা যাবে রিয়েলিস্টিক ডিজাইন ফরমেশন ক্যাম্পেইনের কাজে। যেমন- কল্পনা করুন একটি ফেইক এআই-ক্রিয়েটেড রিয়েলিস্টিক ভিডিওতে একটি কোম্পানির সিইও ঘোষণা করছেন, একটি বড় ধরনের আর্থিক ক্ষতির কথা, একটি বড় ধরনের নিরাপত্তা ভঙ্গের কথা কিংবা বড় ধরনের অন্য কোনো খবরের কথা। সত্য ঘটনাটি জানা-বোঝার আগেই এ ধরনের ফেইক ভিডিওর ব্যাপক ছড়িয়ে দেয়ার ফলে কোম্পানির ওপর বড় ধরনের ক্ষতিকর প্রভাব পড়তে পারে। অপরদিকে আমরা সবাই দেখছি, অনলাইনের মাধ্যমে অ্যাটাক-টুলকিটগুলো সহজেই বেচাকেনা হচ্ছে। এর ফলে



অ্যাটাকারেরা তুলনামূলকভাবে সহজ সুযোগ পেয়ে যাচ্ছে নতুন নতুন হুমকি সৃষ্টির। আমরা নিশ্চিত দেখতে পাচ্ছি, এআই-পাওয়ারড অ্যাটাক-টুলস হামলাকারীদেরকে নতুন নতুন অভিজাত টার্গেটে হামলা করায় আরো বেশি সক্ষম করে তুলবে। এ ধরনের টুল দিয়ে অতিমাত্রিক পারসোন্যালাইজড অ্যাটাককে আরো স্বয়ংক্রিয় করে তোলা হবে। অতীতে এসব সাইবার হামলা ছিল অধিকতর কষ্টসাধ্য ও ব্যয়বহুল। এ ধরনের এআই-পাওয়ার্ড টুলকিটগুলো ক্র্যাফটিংয়ের প্রান্তিক ব্যয় ও প্রতিটি অতিরিক্ত লক্ষিত হামলার ব্যয় অপরিহার্যভাবে নেমে যাবে শূন্যের কোটায়।

প্রতি হামলা ও কৃত্রিম বুদ্ধিমত্তা

এআই সিকিউরিটি স্টোরির একটি উজ্জ্বল দিকও রয়েছে। থ্রেট আইডেন্টিফিকেশন সিস্টেম নতুন নতুন থ্রেট চিহ্নিত করার কাজে ইতোমধ্যেই ব্যবহার করছে মেশিন লার্নিংয়ের নানা টেকনিক। আর এটি শুধু হামলাকারীরাই ভঙ্গুরতা খোলার জন্য ব্যবহার করছে না, প্রতিরোধকারীরাও তা ব্যবহার করছে হামলাকারীদের প্রতিরোধ ঠেকানোর পরিবেশ শক্তিশালী করে তোলার কাজে। যেমন- এআই-পাওয়ারড সিস্টেম একটি এন্টারপ্রাইজ নেটওয়ার্কের ওপর পরিচালনা করতে পারে ধারাবাহিকভাবে সিমুলেটেড অ্যাটাক। খুব শিগগিরই এআই ও অন্যান্য টেকনোলজিস একজনকে সহায়তা করবে আরো ভালোভাবে তার ব্যক্তিগত ডিজিটাল সিকিউরিটি ও প্রাইভেসি রক্ষায়। এআই এমবেডেড করা যেতে পারে একটি মোবাইল ফোনে, যা ব্যবহারকারীকে সতর্ক করে দেবে সুনির্দিষ্ট কিছু ঝুঁকির ব্যাপারে। যেমন- যখন আপনি আপনার মোবাইল ফোনে নতুন একটি ই-মেইল অ্যাকাউন্ট সেটআপ করেন, তখন আপনার মোবাইল ফোন স্বয়ংক্রিয়ভাবে সতর্ক করে দেবে টু-ফ্যাক্টর অথেন্টিকেশন সেটআপ করার জন্য। এক সময় এ ধরনের সিকিউরিটি-বেজড এআই মানুষকে সহায়তা করতে পারে ভালো বোঝাপড়ায়, যখন তারা ব্যক্তিগত ইনফরমেশন দেয় কোনো অ্যাপ্লিকেশন ব্যবহারের বিনিময়ে।

ক্রমবর্ধমান ৫জি চালু

২০১৮ সালে বেশ কয়েকটি ৫জি নেটওয়ার্ক ইনফ্রাস্ট্রাকচার চালু করা হয়েছে। এটি অ্যাটাক সারফেস এরিয়ার সম্প্রসারণ ঘটাবে। ২০১৯ সালটি তৈরি হয়ে আছে ৫জি কর্মকান্ড ত্বরান্বিত করার জন্য। তবে ৫জি নেটওয়ার্কের ও ৫জি ক্যাপাবল ফোন ও অন্যান্য ডিভাইসের জন্য সময় লাগবে ব্যাপকভাবে চালু ৫জি নেটওয়ার্ক ইনফ্রাস্ট্রাকচারের প্রবৃদ্ধি দ্রুত বাড়াতে। উদাহরণ টেনে বলা যায়, আইডিজি (ইন্টারনেট ডেভেলপমেন্ট গ্রুপ) ২০১৯ সালকে অভিহিত করেছে ৫জি ফ্রন্টের একটি 'সেমিনাল ইয়ার' হিসেবে। তাছাড়া আইডিজির ভবিষ্যদ্বাণী হচ্ছে, ৫জি ও ৫জিসংশ্লিষ্ট নেটওয়ার্ক অবকাঠামোর বাজার ২০১৮ সালের ৫২ কোটি ৮০ লাখ ডলার থেকে বেড়ে ২০২২ সালে পৌঁছুবে ২৬০০ কোটি ডলারে। এর অপর অর্থ, এই সময়ে এই বাজারের চক্রবৃদ্ধি প্রবৃদ্ধি ঘটবে বছরে ১১৮ শতাংশ।

যদিও ৫জির মূল আলোকপাত হচ্ছে স্মার্টফোন, তবুও নতুন বছরে ৫জি-ক্যাপাবল স্মার্টফোনের ব্যবহার সীমিতই থেকে যাবে। ৫জি সেলুলার নেটওয়ার্ক ব্যাপকভিত্তিক করার একটি উল্লেখযোগ্য পদক্ষেপ হিসেবে কিছু ক্যারিয়ার বাসাবাড়িতে দেয়ার জন্য সুযোগ দিচ্ছে ফিক্সড ৫জি মোবাইল হটস্পট ও ৫জিসমৃদ্ধ রাউটার। ৫জি পিক ডাটা রেট হচ্ছে ১০ জিপিবিএস, যেখানে ৪জির ডাটা রেট হচ্ছে ১ জিপিবিএস। ৫জিতে উত্তরণ ক্যাটেলাইজ করবে নতুন অপারেশনাল মডেল, নতুন আর্কিটেকচার এবং শেষ পর্যন্ত নতুন ভালনারেবিলিটি বা ভঙ্গুরতা।

এক সময় আরো ৫জি আইওটি (ইন্টারনেট অব থিংস) ডিভাইস ওয়াই-ফাই রাউটারের বদলে বরং সরাসরি সংযুক্ত হবে ৫জি নেটওয়ার্কের সাথে। এই প্রবণতা এসব ডিভাইসকে সরাসরি আঘাতের জন্য আরো ভঙ্গুরতার দিকে ঠেলে দেবে। বাসাবাড়ির ব্যবহারকারীদের জন্য এটি সব আইওটি ডিভাইস মনিটর করা কাজকে আরো জটিল করে তুলবে। কারণ, এগুলো এড়িয়ে চলে সেন্ট্রাল রাউটারকে। আরো ব্যাপক পরিসরে, ব্যাকআপের সক্ষমতা অথবা ক্লাউডভিত্তিক স্টোরেজে বিপুল পরিমাণে ডাটা সহজে সঞ্চালন করার ফলে সাইবার হামলাকারীদের হামলার ক্ষেত্র আরো সম্প্রসারিত হবে।

আরো ভয়াবহ ধরনের হামলা

সম্প্রতিক বছরগুলোতে ব্যাপক ধরনের bot-net-powered distributed denial of service (DDoS) হামলা ক্ষতিসাধন করেছে হাজার হাজার সংক্রমিত আইওটি ডিভাইস। এর ফলে হামলার শিকার ওয়েবসাইটে ট্রাফিক জটিলতা সৃষ্টি হয়। এসব হামলার ঘটনার বিষয়টি গণমাধ্যমের তেমন একটা নজর কাড়েনি। কিন্তু এসব মামলা অব্যাহতভাবে চলছে। আগামী বছরগুলোতেও তা অব্যাহতভাবে চলবে। একই সাথে আশঙ্কা করা হচ্ছে, দুর্বল নিরাপত্তার আইওটি ডিভাইসগুলোর ওপর হামলা করে ক্ষতি করার উদ্দেশ্যে। সেইসব আইওটি ডিভাইসের ওপর সবচেয়ে সমস্যাকর হামলা চলে, যেগুলো সংযোগ রচনা করে ডিজিটাল ও ফিজিক্যাল ওয়ার্ল্ডের মধ্যে। এসব আইওটি এনাবল্ড বস্তুগুলো হচ্ছে কাইনেটিক (গতি সম্পর্কিত), যেমন- কার বা অন্যান্য যানবাহন। অন্যগুলো নিয়ন্ত্রণ করে জটিল অবকাঠামো, যেমন- বিদ্যুৎ বিতরণ ও যোগাযোগ নেটওয়ার্ক। ▸

ট্র্যানজিট ডাটা ক্যাপচারের হামলা

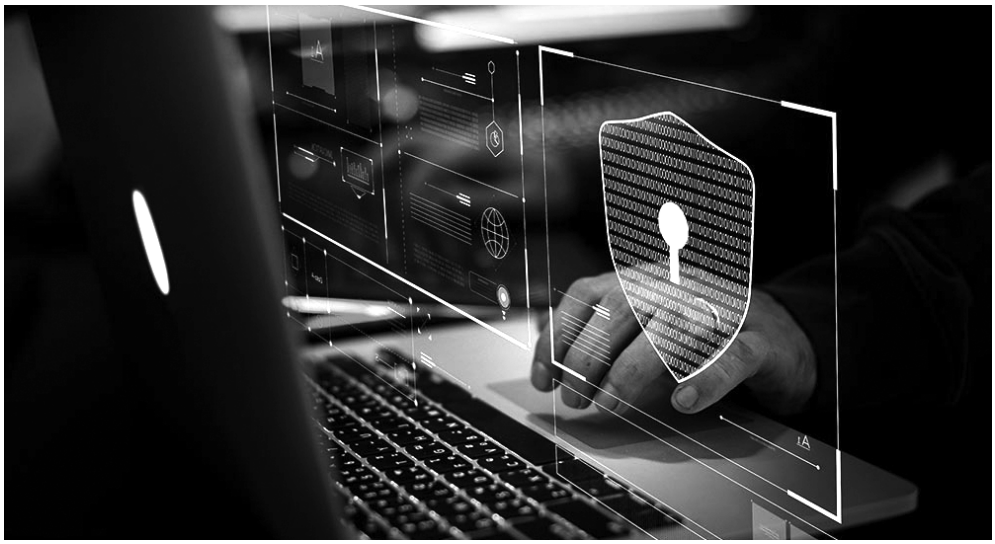
এমন সম্ভাবনা রয়েছে- আমরা দেখব সাইবার হামলাকারীরা নতুন নতুন উপায়ে আঘাত হানবে বাসাবাড়িভিত্তিক ওয়াই-ফাই রাউটার ও অন্যান্য দুর্বল নিরাপত্তার কনজ্যুমার আইওটি ডিভাইসে। ইতোমধ্যেই এ ধরনের একটি হামলা ঘটেছে। এটি হচ্ছে, ক্রিপটোকারেন্সি মাইন করার জন্য ব্যাপক ক্রিপটোজ্যাকিং পরিচালনা করতে আইওটি ডিভাইস মার্শেলিং।

সাইবার নিরাপত্তা বিশ্লেষকেরা ২০১৯ সালে ও তারও পরবর্তী সময়ে ক্রমবর্ধমান হারে হামলাকারীরা চেষ্টা করবে হোম রাউটার ও অন্যান্য আইওটি হাবে ঢুকে পড়ার জন্য- উদ্দেশ্য এগুলোর মধ্য দিয়ে চলা ডাটা ক্যাপচার করা। উদাহরণত, ম্যালওয়্যার ইনসার্ট করা এ ধরনের একটি রাউটার চুরি করতে পারে ব্যাংকিং ক্র্যাডেনশিয়াল (প্রমাণপত্র) এবং ক্যাপচার করতে পারে কার্ড নাম্বারস। ই-কমার্স ব্যবসায়ীরা ক্রেডিট কার্ড সিভিভি নাম্বার স্টোর করেন না হামলাকারীদের কাছে ডাটাবেজ থেকে ক্রেডিট কার্ড চুরি করার কাজটিকে জটিল করে তোলার জন্য। অপরদিকে নিঃসন্দেহে হামলাকারীরা অব্যাহতভাবে উদ্ভাবন করে চলবে তাদের নতুন নতুন কৌশল। এই কৌশল এরা ব্যবহার করবে ট্র্যানজিট অবস্থায় থাকা কনজ্যুমার ডাটা চুরি করার জন্য।

এন্টারপ্রাইজের বেলায় ২০১৮ সালে 'ডাটা-ইন-ট্র্যানজিট কমপ্রোমাইজের' অসংখ্য উদাহরণ রয়েছে। হামলাকারী গোষ্ঠী 'মেগাকার্ট মেলাসিয়াস স্ক্রিপ্টস সরাসরি অথবা ওয়েবসাইটকে টার্গেট করে ওয়েবসাইটের ব্যবহৃত থার্ড-পার্টি সাপ্লায়ারের সাথে কমপ্রোমাইজের মাধ্যমে এমবেডিং করে ক্রেডিট কার্ড নাম্বার ও অন্যান্য ই-কমার্স সাইটের স্পর্শকাতর কনজ্যুমার ইনফরমেশন চুরি করে। এ ধরনের 'ফর্মজ্যাকিং' হামলাগুলো সম্প্রতি ক্ষতিকর প্রভাব ফেলেছে অসংখ্য গ্লোবাল কোম্পানির ওয়েবসাইটে। ট্রানজিটে থাকা এন্টারপ্রাইজ ডাটাকে টার্গেট করে আরেকটি হামলায় VPNFilter ম্যালওয়্যার ক্ষতিকর প্রভাব ফেলে বেশ কিছু রাউটার ও নেটওয়ার্কের ওপর, যেগুলো সংযুক্ত ছিল স্টোরেজ ডিভাইসের সাথে। এর মাধ্যমে হামলাকারী সুযোগ পায় ক্রেডেনশিয়াল চুরির, ডাটা চলাচল পাল্টে দেয়ার, ডাটা ডিক্রিপ্ট করার এবং লক্ষিত প্রতিষ্ঠানে ক্ষতিকর কর্মকান্ড পরিচালনার জন্য একটি লাঞ্চ পয়েন্টকে সহায়তা করায়। আমরা ধরে নিতে পারি, ২০১৯ সালে সাইবার হামলাকারীরা তাদের নজর অব্যাহত রাখবে নেটওয়ার্কভিত্তিক এন্টারপ্রাইজের ওপর হামলার ব্যাপারে।

সাপ্লাই চেইনের ওপর হামলা

২০১৯ সালে সাপ্লাই চেইনের ওপর হামলা বাড়বে এবং প্রভাবও বাড়বে। ক্রমবর্ধমান হারে হামলাগুলোর সাধারণ টার্গেট হচ্ছে সফটওয়্যার সাপ্লাই চেইন। হামলাকারীরা ম্যালওয়্যার ইমপ্ল্যান্ট করছে অন্যান্য বৈধ সফটওয়্যার প্যাকেজে, এর স্বাভাবিক ডিস্ট্রিবিউশন লোকেশনে। এ ধরনের হামলা ঘটবে সফটওয়্যার ভেন্ডর পর্যায়ে উৎপাদনের সময়ে অথবা থার্ড পার্টি সাপ্লায়ার পর্যায়ে। কিছু কিছু সাইবার হামলার ক্ষেত্রে হামলার চিত্রে দেখা গেছে, হামলাকারীরা একটি বৈধ সফটওয়্যার আপডেটকে প্রতিস্থাপন করছে একটি ম্যালিসিয়াস ভার্সনের মাধ্যমে। লক্ষ্যটা হচ্ছে, টার্গেটে তা গোপনে দ্রুত ডিস্ট্রিবিউট করে দেয়া। সফটওয়্যার আপডেট করা যেকোনো ইউজার স্বয়ংক্রিয়ভাবে দেখতে পাবেন, তার কমপিউটার সংক্রমিত হয়ে পড়েছে, যার ফলে হামলাকারীরা এই ইউজারের এনভায়রনমেন্টে হামলার চালানোর জন্য সহজেই জায়গা করে নেবে।



এ ধরনের হামলাকারীর পরিমাণ বাড়ছে এবং হামলার আভিজাত্যও বাড়ছে। আমরা ভবিষ্যতে দেখতে পাব, এভাবে হার্ডওয়্যার সাপ্লাই চেইনে হামলার প্রয়াসও। যেমন- একজন হামলাকারী কমপ্রোমাইজ করতে পারবে অথবা একটি চিপ পাল্টে দিতে পারবে অথবা এ ধরনের কমপোন্যান্ট লাখ লাখ কমপিউটারে স্থানান্তরিত তথা শিপড হওয়ার আগেই UEFI/BIOS-এর ফার্মওয়্যারে সোর্সকোড যোগ করতে পারবে। এ ধরনের হুমকি তাড়ানো খুবই মুশকিল হবে। সম্ভাবনা আছে, এ ধরনের হুমকির আশঙ্কা থাকবে এমনকি কমপিউটার রিবুট করার পরও অথবা হার্ডডিস্ক রিফরমেটেড করা হলেও।

সারকথা হচ্ছে, হামলাকারীরা অব্যাহতভাবে নতুন ও আরো উন্নত ধরনের সুযোগের সন্ধানে থাকবে, তাদের টার্গেটের প্রতিষ্ঠানের সাপ্লাই চেইনকে ইনফিলট্রেট করার জন্য।

সিকিউরিটি ও প্রাইভেসি নিয়ে উদ্বেগ

ক্রমবর্ধমান হারের সিকিউরিটি ও প্রাইভেসি নিয়ে উদ্বেগ বাড়িয়ে তুলবে আইনগত ও নিয়ন্ত্রণমূলক কর্মকান্ড। ইউরোপীয় ইউনিয়নের মধ্য-২০১৮-এ General Data Protection Regulation (GDPR) বাস্তবায়ন হচ্ছে বিভিন্ন সিকিউরিটি ও প্রাইভেসি উদ্যোগ যে ইউরোপীয় ইউনিয়নের বাইরের দেশগুলোতে আরো আসছে, তারই একটি পূর্ব লক্ষণ। কানাডা ইতোমধ্যেই বাস্তবায়ন করেছে জিডিপিআর ধরনের বিধান। আর ব্রাজিল সম্প্রতি পাস করেছে একটি নতুন প্রাইভেসি বিধান, যা জিডিপিআরের মতোই এবং তা কার্যকর হবে ২০২০ সাল থেকে। অস্ট্রেলিয়া ও সিঙ্গাপুর জিডিপিআরের সূত্রে উজ্জীবিত হতে আইন করেছে ৭২ ঘণ্টা ব্রেক নোটিসের। ভারতও বিবেচনা করে দেখছে জিডিপিআর ধরনের বিধান তৈরির। বিশ্বব্যাপী আরো বহু দেশের অ্যাডিকুয়াচি রয়েছে এবং জিডিপিআর অ্যাডিকুয়াচি নিগোশিয়েট করছে। যুক্তরাষ্ট্রে জিডিপিআর আসার অল্প কিছুদিন পর ক্যালিফোর্নিয়া পাস করে প্রাইভেসি আইন। আজ পর্যন্ত যুক্তরাষ্ট্রে করা আইনের মধ্যে এটি বিবেচিত সবচেয়ে কঠোর আইন হিসেবে। ধারণা করা হচ্ছে, জিডিপিআরের পুরোপুরি প্রভাব ২০১৯ সালে বিশ্বব্যাপী আরো স্পষ্টতর হবে। যুক্তরাষ্ট্রের ফেডারেল পর্যায়ে কংগ্রেস এরই মধ্যে গভীর সিকিউরিটি ও প্রাইভেসির অতিকষ্টে জল-কাদাময় পথে চলছে। এ ধরনের আইন বিধানের পদক্ষেপ ২০১৯ সালে আরো জোরালো হবে। অপরিহার্যভাবে, অব্যাহতভাবে ও বর্ধিত হারে আলোকপাত করা হবে ইলেকশন সিস্টেম সিকিউরিটির ওপর। কারণ, ২০২০ সালে শুরু হবে যুক্তরাষ্ট্রের প্রেসিডেন্ট নির্বাচনের প্রচারাভিযান।

সিমানটেকের গবেষক ও নিরাপত্তা বিশ্লেষকেরা প্রায় নিশ্চিত, নতুন বছরে সিকিউরিটি ও প্রাইভেসির চাহিদা মেটাতে প্রচুর আইনি ও নিয়ন্ত্রণমূলক কর্মকান্ড চলবে। এগুলোর কিছু সহায়ক হওয়ার বদলে কাউন্টারপ্রোডাকটিভ বলে প্রমাণিত হওয়ার সমূহ সম্ভাবনা রয়েছে। উদাহরণ টেনে বলা যায়, শুধু ব্যাপক নিয়ন্ত্রণ সিকিউরিটি কোম্পানিগুলোকে তাদের হামলা চিহ্নিত করা ও প্রতিহামলার উদ্যোগের বেলায় বাধাগ্রস্ত করতে পারে তাদের জেনেরিক ইনফরমেশন শেয়ার করার ব্যাপারে। সিকিউরিটি ও প্রাইভেসি রেগুলেশনগুলো সৃষ্টি করতে পারে এক ধরনের নতুন ভঙ্গুরতা তথা ভালনারেবিলিটি কজ