সাইবার ওয়ার

অদৃশ্য ঘাতকের কবলে

সাইবার ওয়ার

অ্যান্ডি গ্রিনবার্গ

ফাউন্টেন
পা ব লি কে শ ন্স

সূচিপত্র

প্রকাশকের কথা ৯
ভূমিকা ১১
প্রাককথন ১৫

১ম পর্ব

উত্থান **১৭**
দ্য জিরো ডে ১৭
ব্ল্যাকএনার্জি ২২
আরাকিস ০২ .... ২৫
ফোর্স মাল্টিপ্লায়ার ৩২
স্টারলাইটমিডিয়া ৪৪
হোলোদেমোর থেকে চেরনোবিল ৫৩
ময়দান থেকে দনবাস ৬১
ব্ল্যাকআউট ৭০
প্রতিনিধিদল ৭৯

২য় পর্ব

উৎস **৮৮**
ফ্ল্যাশব্যাক : অরোরা ৮৮
ফ্ল্যাশব্যাক : মুনলাইট মেজ ৯৪
ফ্ল্যাশব্যাক : এস্তোনিয়া ১০৫
ফ্ল্যাশব্যাক : জর্জিয়া ১১৭
ফ্ল্যাশব্যাক : স্টাক্সনেট ১২৬

৩য় পর্ব

বিবর্তন **১৩৮**
সতর্কবার্তা ১৩৮
ফ্যান্সি বিয়ার ১৪৬
এফ-সোসাইটি ১৫৪
পলিগন ১৬১
ইন্ডাস্ট্রিয়ার/ক্র্যাশ ওভাররাইড ১৭১

৪র্থ পর্ব

আবির্ভাব **১৮২**
মারস্ক ১৮২
শ্যাডো ব্রোকারস ১৮৫
ইটারনালব্লু ১৯৫
মিমিক্যাটজ ২০৪
নটপেটয়া ২১১
জাতীয় বিপর্যয় ২১৭
ব্রেকডাউন ২২৩
ক্ষতিপূরণ ২৩০
পরবর্তী ঘটনাপ্রবাহ ২৪০
দূরত্ব ২৪৯

৫ম পর্ব

পরিচয় **২৫৬**
জিআরইউ ২৫৬
দলত্যাগী ২৬৩
ইনফরমাতসিওননয়ে প্রোতিভোবোরস্তভো ২৭২
শাস্তি ২৮১
ব্যাড র‍্যাবিট, অলিম্পিক ডেস্ট্রয়ার ২৮৫

ফলস ফ্ল্যাগস ২৯২
৭৪৪৫৫ .... ২৯৯
দ্য টাওয়ার ৩০৬
রাশিয়া ৩১২
দ্য এলিফ্যান্ট অ্যান্ড দ্য ইনসারজেন্ট ৩১৮

৬ষ্ঠ পর্ব

শিক্ষা **৩২৭**
জেনেভা ৩২৭
ব্ল্যাক স্টার্ট ৩৩৯
রেজিলিয়েন্স বা ঘুরে দাঁড়ানোর ক্ষমতা ৩৫০

উপসংহার ৩৫৮
পরিশিষ্ট ৩৬২

প্রকাশকের কথা

আমরা এমন এক যুগে এসে দাঁড়িয়েছি, যেখানে যুদ্ধের শব্দ আর গোলাগুলির ধ্বনি সবসময় শোনা যায় না—তবুও যুদ্ধ চলছে, অবিরাম, অদৃশ্য এবং গভীরতর। এই যুদ্ধের ময়দান আর সীমান্তে সীমাবদ্ধ নেই; এটি ছড়িয়ে পড়েছে আমাদের ঘরে, আমাদের ব্যবহৃত যন্ত্রে, আমাদের নির্ভরতার প্রতিটি স্তরে। বিদ্যুৎ, যোগাযোগ, স্বাস্থ্যসেবা, অর্থনীতি—সবকিছুর শিরায় শিরায় আজ প্রবাহিত হচ্ছে ডিজিটাল প্রযুক্তি, আর সেই শিরাগুলোতেই নীরবে আঘাত হানছে এক নতুন ধরনের শক্তি—সাইবারযুদ্ধ।

এই বইটি সেই অদৃশ্য যুদ্ধের এক শীতল, কিন্তু বাস্তব প্রতিচ্ছবি। এখানে আমরা দেখি কীভাবে একটি কোড, একটি দুর্বলতা, কিংবা একটি অজানা ম্যালওয়্যার মুহূর্তের মধ্যে বিশ্বব্যাপী বিপর্যয় ডেকে আনতে পারে। ২০১৭ সালের সেই ভয়াল দিনে, যখন নটপেটিয়া নামক একটি ভাইরাসের আক্রমণ পৃথিবীর বিভিন্ন প্রান্তে হাসপাতাল, বন্দর, কারখানা এবং আর্থিক ব্যবস্থাকে অচল করে দিয়েছিল, তখন মানবসভ্যতা প্রথমবারের মতো উপলব্ধি করেছিল—একটি অদৃশ্য আঘাত কতটা দৃশ্যমান ধ্বংস ডেকে আনতে পারে।

এই গ্রন্থে কেবল একদল হ্যাকারের গল্প বলা হয়নি; বরং তুলে ধরা হয়েছে একটি পরিবর্তিত বিশ্বব্যবস্থার চিত্র, যেখানে যুদ্ধের সংজ্ঞাই বদলে গেছে। রাষ্ট্র, গোয়েন্দা সংস্থা, প্রযুক্তি প্রতিষ্ঠান—সবাই এক অদৃশ্য প্রতিযোগিতায় লিপ্ত, যেখানে শক্তির মাপকাঠি আর অস্ত্রের পরিমাণে নয়, বরং তথ্যের দখল এবং সিস্টেমের নিয়ন্ত্রণে নির্ধারিত হয়।

লেখক অত্যন্ত সূক্ষ্ম বিশ্লেষণ ও গবেষণার মাধ্যমে দেখিয়েছেন, কীভাবে ইউক্রেনের মাটিকে পরীক্ষাগার হিসেবে ব্যবহার করে সাইবার অস্ত্রের বিকাশ ঘটেছে, এবং কীভাবে সেই পরীক্ষার প্রতিধ্বনি ধীরে ধীরে পুরো বিশ্বে ছড়িয়ে পড়েছে। একইসাথে,

এই বই আমাদের সামনে নিয়ে আসে সেইসব অজ্ঞাতনামা গবেষক ও বিশ্লেষকদের গল্প, যারা অন্ধকারের ভেতর আলো খোঁজার চেষ্টা করেছেন—ডিজিটাল ছাপ অনুসরণ করে উন্মোচন করতে চেয়েছেন এক ভয়ঙ্কর বাস্তবতাকে।

আমরা এই অনুবাদে কেবল ভাষান্তর করিনি; বরং চেষ্টা করেছি মূল ভাব, আবেগ এবং বোধকে অক্ষুণ্ণ রেখে পাঠকের সামনে একটি জীবন্ত অভিজ্ঞতা তুলে ধরতে। অনেক ক্ষেত্রে শব্দের সরল অনুবাদের পরিবর্তে ভাবানুবাদের পথ অনুসরণ করা হয়েছে, যেন পাঠক কেবল তথ্য গ্রহণ না করে, বরং ঘটনাগুলোর ভেতরে প্রবেশ করতে পারেন।

এই বইটি আমাদের সতর্ক করে, প্রশ্ন করতে শেখায়, এবং ভাবতে বাধ্য করে—আমরা কি সত্যিই প্রস্তুত এই নতুন যুদ্ধের জন্য? আমাদের প্রতিদিনের নির্ভরতা যে প্রযুক্তির ওপর, সেটিই যদি আমাদের সবচেয়ে বড় দুর্বলতা হয়ে ওঠে, তবে ভবিষ্যৎ কোন দিকে গড়াবে?

একজন প্রকাশক হিসেবে আমাদের বিশ্বাস, এই গ্রন্থ কেবল একটি তথ্যভিত্তিক বিবরণ নয়; এটি আমাদের সময়ের এক গুরুত্বপূর্ণ দলিল। যারা প্রযুক্তি, নিরাপত্তা, ভূ-রাজনীতি কিংবা আধুনিক বিশ্বের গতিপথ বুঝতে আগ্রহী—তাদের জন্য এই বই একটি অপরিহার্য পাঠ। অদৃশ্য এই যুদ্ধের কাহিনি আপনাকে কেবল অবাকই করবে না, বরং আপনাকে নতুন করে সচেতন, সতর্ক এবং চিন্তাশীল করে তুলবে—এই প্রত্যাশা রইল।

আবদুর রহমান আদ-দাখিল
বাংলাবাজার, ঢাকা-১১০০
০৬-৪-২০২৬

ভূমিকা

২৭ জুন, ২০১৭। পৃথিবীর পুরো অবকাঠামো জুড়ে অদ্ভুত এবং ভয়ঙ্কর একটা ঢেউ আছড়ে পড়ল। পেনসিলভানিয়ার বেশ কিছু হাসপাতাল সার্জারি পিছিয়ে দিতে বাধ্য হলো, রোগীদের ফিরিয়ে দিতে শুরু করল তারা। তাসমানিয়ার একটা ক্যাডবেরি ফ্যাক্টরিতে হঠাৎ করেই চকলেট বানানো বন্ধ হয়ে গেল। ঔষধ শিল্পের বিশাল বড় কোম্পানি মার্ক হিউম্যান প্যাপিলোমাভাইরাসের ভ্যাকসিন বানানো পুরোপুরি থামিয়ে দিল।

দেখতে দেখতে, বিশ্বের সবচেয়ে বড় শিপিং কোম্পানি মারর্স্কের মালিকানায় থাকা পৃথিবীর বিভিন্ন প্রান্তের সতেরোটি বন্দর পুরোপুরি অচল হয়ে পড়ল। হাজার হাজার আঠারো চাকার ট্রাক শিপিং কনটেইনার নিয়ে সেসব বন্দরের গেটের বাইরে লাইন দিতে শুরু করল। মহাসাগর পাড়ি দিয়ে বিশাল সব জাহাজ বন্দরে এসে ভিড়ল, প্রতিটাতে লাখ লাখ টন মালপত্র। কিন্তু একটা মালও নামানোর মতো কেউ ছিল না। মনে হচ্ছিল যেন মস্তিষ্ক-খেকো কোনো ব্যাকটেরিয়া পুরো পৃথিবীতে ছড়িয়ে পড়েছে। আমাদের এই আধুনিক বিশ্বের একে অপরের সাথে যুক্ত স্বয়ংক্রিয় সিস্টেমগুলো যেন হুট করেই ভুলে গেছে তাদের আসল কাজ কী!

এই আক্রমণের কেন্দ্রবিন্দু ছিল ইউক্রেনে। সেখানে এই প্রযুক্তিগত ধ্বংসযজ্ঞের প্রভাব ছিল আরও ভয়াবহ। এটিএম বুথ আর ক্রেডিট কার্ড পেমেন্ট সিস্টেমগুলো কোনো কারণ ছাড়াই অফলাইন হয়ে গেল। দেশটির রাজধানী কিয়েভের গণপরিবহন ব্যবস্থা পুরোপুরি ভেঙে পড়ল। সরকারি সংস্থা, বিমানবন্দর, হাসপাতাল, ডাক বিভাগ, এমনকি চেরনোবিলের পারমাণবিক বিদ্যুৎ কেন্দ্রের ধ্বংসস্তূপে তেজস্ক্রিয়তা মাপার কাজে থাকা বিজ্ঞানীরাও অসহায় হয়ে তাকিয়ে রইলেন। তাদের চোখের সামনেই নেটওয়ার্কের প্রতিটি কম্পিউটার অদ্ভুত এক ম্যালওয়্যার কোডে আক্রান্ত হয়ে সব ডেটা মুছে ফেলতে শুরু করল।

সাইবারযুদ্ধ আসলে এমনই হয়। একটা অদৃশ্য শক্তি, যা কোনো অজানা জায়গা থেকে আঘাত হেনে মানব সভ্যতার ভিত্তিমূলে থাকা প্রযুক্তিগুলোকে বিশাল পরিসরে ধ্বংস করে দিতে পারে।

দশকের পর দশক ধরে ইন্টারনেট নিরাপত্তার ভবিষ্যৎ নিয়ে বক্তারা আমাদের সতর্ক করে আসছিলেন যে এমন কিছু একটা হতে চলেছে। তারা আগেই বলেছিলেন যে হ্যাকাররা খুব তাড়াতাড়ি সাধারণ অপরাধ বা রাষ্ট্রীয় গুপ্তচরবৃত্তির গণ্ডি পেরিয়ে যাবে এবং আধুনিক বিশ্বের ডিজিটাল অবকাঠামোর দুর্বল জায়গাগুলোতে আঘাত হানতে শুরু করবে। ২০০৭ সালের কথা। রাশিয়ান হ্যাকাররা এস্তোনিয়ার ওপর সাইবার আক্রমণের এমন এক ঝড় বইয়ে দিল যে দেশটির প্রায় সব ওয়েবসাইট অফলাইন হয়ে গেল। সেই আক্রমণ বুঝিয়ে দিয়েছিল ভূ-রাজনৈতিক কারণে হওয়া হ্যাকিং কত বড় আকার ধারণ করতে পারে। ঠিক দুই বছর পর, আমেরিকার এনএসএ এর তৈরি স্টাক্সনেট নামের একটা ম্যালিসিয়াস সফটওয়্যার সবার অগোচরে ইরানের পারমাণবিক সেন্ট্রিফিউজগুলোর গতি বাড়িয়ে দিয়ে সেগুলোকে ধ্বংস করে দিল। এই ঘটনা ভবিষ্যতের আরেকটি ভয়াবহ চিত্র আমাদের সামনে তুলে ধরেছিল। এটি প্রমাণ করে দিয়েছিল যে সাইবারযুদ্ধের হাতিয়ারগুলো এখন আর স্রেফ ডিজিটাল জগতেই আটকে নেই, সেগুলো খুব সহজেই বাস্তব জগতের সবচেয়ে সুরক্ষিত আর সংবেদনশীল জায়গাগুলোতেও ঢুকে পড়তে পারে।

২০১৪ সালের শুরুতে ইউক্রেনে রাশিয়ার যে যুদ্ধ শুরু হয়েছিল, তার দিকে যারা নজর রাখছিলেন, তাদের কাছে এই বিপদের পূর্বাভাস ছিল আরও স্পষ্ট, আরও সরাসরি। ২০১৫ সাল থেকে ইউক্রেনের সরকার, মিডিয়া এবং পরিবহন ব্যবস্থার ওপর একের পর এক ভয়ংকর সাইবার আক্রমণ হতে থাকে। এই আক্রমণগুলোর চূড়ান্ত পরিণতি ছিল হ্যাকারদের দ্বারা ঘটানো পৃথিবীর প্রথম ব্ল্যাকআউট বা বিদ্যুৎ বিপর্যয়। সেই আক্রমণে লাখ লাখ সাধারণ মানুষের ঘরের আলো নিভে গিয়েছিল।

গবেষকদের ছোট্ট একটা দল বিপদঘণ্টি বাজাতে শুরু করল। কিন্তু তাদের সেই সতর্কবার্তায় খুব একটা কাজ হলো না। তারা বলছিলেন, রাশিয়া আসলে ইউক্রেনকে তাদের সাইবারযুদ্ধের নতুন নতুন অস্ত্র পরীক্ষার একটা ল্যাবরেটরি বানিয়ে ফেলেছে। তারা এই ভয়ও দেখাচ্ছিলেন যে, এই নতুন প্রযুক্তিগুলো খুব জলদি আমেরিকা, ন্যাটো এবং পুরো বিশ্বের ওপর প্রয়োগ করা হতে পারে। আর আমাদের এই পৃথিবী এই নতুন মাত্রার যুদ্ধের জন্য একেবারেই প্রস্তুত ছিল না। গবেষকরা ক্রেমলিনের

মদদপুষ্ট একদল হ্যাকারের দিকে আঙুল তুললেন। এই দলটিই যেন ধ্বংসযজ্ঞ চালানোর অভিনব সব অস্ত্র একের পর এক ছুঁড়ে মারছিল। এই হ্যাকার গ্রুপটির নাম স্যান্ডওয়ার্ম।

পরের দুই বছর স্যান্ডওয়ার্ম তাদের আগ্রাসন আরও বাড়িয়ে দিল। নিজেদেরকে তারা প্রমাণ করল পৃথিবীর সবচেয়ে বিপজ্জনক হ্যাকার দল হিসেবে। সাইবারযুদ্ধের সংজ্ঞাই বদলে দিল তারা। শেষমেশ, ২০১৭ সালের জুনের শেষের দিকের সেই ভয়াল দিনে, এই দলটি নটপেটিয়া নামের এমন এক বিশ্ব-কাঁপানো ওয়ার্ম ছড়িয়ে দিল, যাকে এখন পর্যন্ত ইতিহাসের সবচেয়ে ধ্বংসাত্মক এবং ব্যয়বহুল ম্যালওয়্যার হিসেবে ধরা হয়। এই পুরো প্রক্রিয়ায় স্যান্ডওয়ার্ম এমন একটা ব্যাপার প্রমাণ করে দিল যা আগে কখনো দেখা যায়নি। তারা দেখিয়ে দিল, সামরিক ধ্বংসযজ্ঞ চালানোর মানসিকতা সম্পন্ন এবং রাষ্ট্রের মদদপুষ্ট একদল চরম দক্ষ হ্যাকার যেকোনো দূরত্ব থেকে মানবজীবনের ভিত্তিমূলে আঘাত হানতে পারে। তারা একে অপরের সাথে যুক্ত সিস্টেমগুলোতে আঘাত হেনে এমন এক বিপর্যয় ডেকে আনতে পারে, যা কেউ কখনো কল্পনাও করতে পারবে না।

আজ স্যান্ডওয়ার্ম এবং তাদের মতো অন্য দলগুলোর তৈরি করা এই হুমকির কালো ছায়া আমাদের ভবিষ্যতের ওপর বিশাল আকার নিয়ে ঝুলছে। সাইবারযুদ্ধের এই বিস্তার যদি কোনোভাবে ঠেকানো না যায়, তবে রাষ্ট্র-সমর্থিত হ্যাকিংয়ের শিকার হওয়া মানুষগুলোকে ভবিষ্যতে আরও বেশি বিষাক্ত এবং ধ্বংসাত্মক ম্যালওয়্যারের মুখে পড়তে হবে।

ইউক্রেনে প্রথম যে সাইবার হামলাগুলো চালানো হয়েছিল, তা আসলে এক আসন্ন ধ্বংসের পূর্বাভাস দেয়। এমন এক অন্ধকার ভবিষ্যত, যেখানে হ্যাকারদের খেয়ালে দিনের পর দিন, এমনকি সপ্তাহের পর সপ্তাহ ধরে ব্ল্যাকআউট বা বিদ্যুৎ বিপর্যয় চলতে পারে। ইচ্ছে করে চাপিয়ে দেওয়া এই বিদ্যুৎহীনতা পুয়ের্তো রিকোতে হ্যারিকেন মারিয়ার পর ঘটে যাওয়া সেই আমেরিকান ট্র্যাজেডির কথাই মনে করিয়ে দেয়, যার ফলে বিশাল অর্থনৈতিক ক্ষতি আর প্রাণহানি ঘটেছিল। আবার এমনটাও হতে পারে, হ্যাকাররা কোনো শিল্প কারখানার যন্ত্রপাতি ধ্বংস করে দিয়ে প্রাণঘাতী বিপর্যয় ডেকে আনল। অথবা নটপেটিয়া ম্যালওয়্যারের মতো, একেবারে ঠিক সময়ে লাখ লাখ কম্পিউটারের ডেটা মুছে দিয়ে শত্রুর অর্থনীতি বা জরুরি অবকাঠামোর ডিজিটাল সিস্টেমগুলোকে পুরোপুরি অচল করে দিল।

এই বইটা স্যান্ডওয়ার্মের গল্প বলবে। সাইবারযুদ্ধের সেই ধ্বংসাত্মক জগতটাকে যারা একটু একটু করে বাস্তব করে তুলছে, এই হ্যাকার দলটি তাদের সবচেয়ে স্পষ্ট উদাহরণ। বইটিতে বছরের পর বছর ধরে চলা সেই গোয়েন্দাদের অক্লান্ত পরিশ্রমের কথাও থাকবে, যারা এই হ্যাকারদের পিছু নিয়েছিলেন। কারণ একটা ডিজিটাল বিপর্যয়ের পর আরেকটা বিপর্যয়ে বারবার স্যান্ডওয়ার্মের আঙুলের ছাপ পাওয়া যাচ্ছিল। গোয়েন্দারা এদের আসল পরিচয় বের করতে আর আস্তানা খুঁজে পেতে মরিয়া ছিলেন। এই দলটা কতটা ভয়ংকর হতে পারে, সেটা সবাইকে জানিয়ে এদের থামানোর একটা মরিয়া চেষ্টাই ছিল তাদের মূল লক্ষ্য।

তবে স্যান্ডওয়ার্ম কেবল একটি হ্যাকার দল কিংবা বিশ্বজুড়ে সাইবারযুদ্ধ চালানোর পেছনে রাশিয়ার বেপরোয়া মনোভাবের গল্প নয়। এটি আসলে একটা বড় মাপের বৈশ্বিক অস্ত্র প্রতিযোগিতার গল্প, যা আজও চলছে। এমন এক প্রতিযোগিতা, যা আমেরিকা এবং পশ্চিমা বিশ্ব থামাতে তো পারেইনি, উল্টো নিজেরাই ডিজিটাল হামলার হাতিয়ারগুলো সাগ্রহে আপন করে নিয়ে এই প্রতিযোগিতাকে আরও উসকে দিয়েছে। আর এই কাজটা করতে গিয়ে আমরা নিজেদের অজান্তেই পৃথিবীতে এক লাগামহীন বিশৃঙ্খলা ডেকে এনেছি।

প্রাককথন

যখন আলো নিভে গেল, ঘড়ির কাঁটা তখন একেবারে শূন্যের ঘরে।

২০১৬ সালের ডিসেম্বরের এক শনিবার রাতের কথা। ওলেক্সি ইয়াসিনস্কি কিয়েভের অ্যাপার্টমেন্টের বসার ঘরে তার স্ত্রী আর কিশোর ছেলের সাথে সোফায় বসে ছিলেন। চল্লিশ বছর বয়সী এই ইউক্রেনিয়ান সাইবার সিকিউরিটি গবেষক এবং তার পরিবার ঘণ্টাখানেক ধরে অলিভার স্টোনের স্নোডেন সিনেমাটি দেখছিলেন। ঠিক তখনই হঠাৎ করে তাদের পুরো বিল্ডিংয়ের কারেন্ট চলে গেল।

ইয়াসিনস্কির স্ত্রী মজা করে বললেন, হ্যাকাররা বোধহয় চায় না আমরা সিনেমাটা শেষ করি। তিনি আসলে এক বছর আগের একটা ঘটনার কথা মনে করিয়ে দিচ্ছিলেন। ২০১৫ সালের বড়দিনের ঠিক দুই দিন আগে এক সাইবার হামলায় ইউক্রেনের প্রায় আড়াই লাখ মানুষের ঘরের বিদ্যুৎ চলে গিয়েছিল।

কিয়েভের একটি সাইবার সিকিউরিটি ফার্মের চিফ ফরেনসিক অ্যানালিস্ট ইয়াসিনস্কি কিন্তু হাসলেন না। তিনি তার ডেস্কে রাখা পোর্টেবল ঘড়িটার দিকে তাকালেন। সময় দেখাচ্ছে ০০ :০০। ঠিক রাত বারোটা।

ইয়াসিনস্কির টেলিভিশনটা একটা ব্যাটারি ব্যাকআপ দেওয়া সার্জ প্রোটেক্টরের সাথে যুক্ত ছিল। তাই স্ক্রিনের কাঁপা কাঁপা আলোতেই ঘরটা একটু আলোকিত হয়ে ছিল। পাওয়ার স্ট্রিপটা থেকে একটানা বিপ বিপ শব্দ আসতে শুরু করল। চার্জ বাঁচানোর জন্য ইয়াসিনস্কি উঠে গিয়ে সেটা বন্ধ করে দিলেন। মুহূর্তেই ঘরটা একেবারে নিস্তব্ধ হয়ে গেল।

তিনি রান্নাঘরে গেলেন, এক মুঠো মোমবাতি বের করে জ্বালালেন। তারপর এসে দাঁড়ালেন রান্নাঘরের জানালার কাছে। হালকা-পাতলা, সোনালি চুলের এই ইঞ্জিনিয়ার শহরের যে রূপটা দেখলেন, তা আগে কখনো দেখেননি। তার অ্যাপার্টমেন্ট

বিল্ডিংয়ের চারপাশের আকাশরেখা অন্ধকারে ডুবে আছে। মেঘলা আকাশে কেবল দূরের কোনো আলোর ধূসর আভা প্রতিফলিত হচ্ছে, যা আধুনিক সব কন্ডো এবং সোভিয়েত আমলের উঁচু ভবনগুলোর বিশাল কালো অবয়বকে কিছুটা স্পষ্ট করে তুলছিল।

একদম কাঁটায় কাঁটায় সময় আর তারিখটার দিকে খেয়াল করে ইয়াসিনস্কির বুঝতে বাকি রইল না যে, এটা কোনো সাধারণ ব্ল্যাকআউট নয়। কারণ ২০১৫ সালের ডিসেম্বরের সেই গ্রিড হামলার পর প্রায় ঠিক এক বছর কেটে গেছে। তিনি বাইরের কনকনে ঠান্ডার কথা ভাবলেন। তাপমাত্রা প্রায় শূন্য ডিগ্রি ফারেনহাইটের কাছাকাছি। হাজার হাজার বাড়ির ভেতরের তাপমাত্রাও আস্তে আস্তে কমতে শুরু করেছে। পানির পাম্পগুলো বিকল হয়ে পাইপের ভেতরের পানি জমে বরফ হয়ে যাওয়ার কাউন্টডাউন যেন শুরু হয়ে গেছে।

ঠিক তখনই ইয়াসিনস্কির মাথায় একটা সন্দেহ বাসা বাঁধতে শুরু করল। গত চৌদ্দ মাস ধরে তিনি নিজেকে একটা বিশাল সংকটের একেবারে কেন্দ্রে আবিষ্কার করেছেন। একের পর এক ইউক্রেনীয় কোম্পানি আর সরকারি সংস্থা তার কাছে ছুটে এসেছে। কারণ এক ভয়ানক সাইবার হামলার মহামারী তাদের ওপর নির্দয়ভাবে আঘাত হানছিল। এই সবকিছুর পেছনে একটা মাত্র হ্যাকার দলই কলকাঠি নাড়ছে বলে মনে হচ্ছিল। এখন আর তিনি এই ভাবনাটাকে মন থেকে সরাতে পারছিলেন না যে, গত এক বছরেরও বেশি সময় ধরে তিনি যাদের আঙুলের ছাপ খুঁজে বেড়াচ্ছিলেন, সেই একই প্রেতাত্মারা ইন্টারনেটের জগত পেরিয়ে সোজা তার ঘরের

ভেতর হাত বাড়িয়ে দিয়েছে।

১ম পর্ব

উত্থান

শুরুর মুহূর্তগুলোকে ভালোভাবে পর্যবেক্ষণের কাজে লাগান। এভাবে অনেক দ্রুত জয়ের সুযোগ হাতছাড়া হয়ে যেতে পারে, কিন্তু এই পর্যালোচনার সময়টুকুই আপনার সাফল্যের সবচেয়ে বড় নিশ্চয়তা। তাই সময় নিন এবং নিশ্চিত হোন।

দ্য জিরো ডে

বেল্টওয়ের সীমানা ছাড়িয়ে যেখানে ওয়াশিংটন ডিসির ইন্টেলিজেন্স-ইন্ডাস্ট্রিয়াল কমপ্লেক্স শেষ হয়ে বিশাল গাড়ি পার্কিংয়ের জায়গা আর ধূসর রঙের অফিস বিল্ডিংয়ের সাগরে মিশেছে, সেখানকার একটা ভবনের গল্প বলি। বিল্ডিংগুলোর গায়ে এমন সব লোগো আর কর্পোরেট নাম লেখা, যেগুলো দেখলে মনে হয় মানুষ যেন ভুলে যাওয়ার জন্যই এগুলো বানিয়েছে। ভার্জিনিয়ার চ্যান্টিলির এমন একটা ভবনের চারতলায় জানালাবিহীন একটা ভেতরের রুম আছে। সেই রুমের দেয়ালগুলো ম্যাট ব্ল্যাক রঙে রাঙানো, যেন বাইরের কোনো আলো সেখানে ঢুকতে না পারে। একেবারে শূন্য এক নেতিবাচক স্থান তৈরি করার জন্যই এমন ব্যবস্থা।

২০১৪ সাল। ইউক্রেনে সাইবারযুদ্ধ শুরু হওয়ার ঠিক এক বছর একটু বেশি সময় আগের কথা। আইসাইট পার্টনারস নামের ছোট একটা বেসরকারি গোয়েন্দা সংস্থা এই রুমটিকে ডাকত ব্ল্যাক রুম নামে। এর ভেতরে দুইজনের একটা দল সফটওয়্যারের দুর্বলতা খোঁজার কাজ করত। কাজটার জন্য এত বেশি মনোযোগের দরকার ছিল যে, এখানকার কর্মীরাই অনেকটা সেন্সরি-ডিপ্রাইভেশন চেম্বারের মতো একটা অফিসের আবদার করেছিল, যেখানে বাইরের পৃথিবীর কোনো শব্দ বা আলো পৌঁছাবে না।

সেপ্টেম্বরের এক বুধবার সকালে জন হাল্টকুইস্ট অদ্ভুত এক অনুরোধ নিয়ে এই দুই গুহাবাসীর কাছেই হাজির হয়েছিলেন। সেদিনের শুরুতে হাল্টকুইস্ট যখন তার ডেস্কে এসেছিলেন, তখন পরিবেশটা ছিল বেশ আলাদা। তার ডেস্কটা আইসাইট বিল্ডিংয়ের উল্টো দিকে, যেখানে সত্যিকারের জানালা আছে আর আলো-বাতাস খেলে। সেখানে বসে তিনি ইউক্রেনে তাদের কোম্পানির স্যাটেলাইট অপারেশনে থাকা এক সহকর্মীর ইমেইল খোলেন। সেই ইমেইলের ভেতরে একটা চমৎকার উপহার অপেক্ষা করছিল। কিয়েভের কর্মীরা ধারণা করছিলেন যে, তাদের হাতে দারুণ একটা জিরো-ডে ভালনারেবিলিটি বা দুর্বলতা এসে পড়েছে।

হ্যাকারদের ভাষায় জিরো ডে হলো সফটওয়্যারের এমন এক গোপন নিরাপত্তা ত্রুটি, যার কথা সেই সফটওয়্যারটি যে কোম্পানি বানিয়েছে এবং রক্ষণাবেক্ষণ করে, তাদেরও জানা নেই। নামটার পেছনে একটা মজার কারণ আছে। ব্যবহারকারীদের সুরক্ষা দেওয়ার জন্য কোম্পানিগুলোর হাতে এই ত্রুটি সারানোর প্যাচ তৈরি করার সময় থাকে একেবারে জিরো ডে বা শূন্য দিন। একটা শক্তিশালী জিরো ডে, বিশেষ করে যেটা কোনো হ্যাকারকে সেই সফটওয়্যারের গণ্ডি ভেঙে টার্গেট করা কম্পিউটারে নিজেদের কোড চালানোর সুযোগ করে দেয়, সেটা অনেকটা মাস্টার কীর মতো কাজ করে। ইন্টারনেটের সাথে যুক্ত থাকা পৃথিবীর যেকোনো প্রান্তের কোনো মেশিন যদি সেই দুর্বল সফটওয়্যারটি ব্যবহার করে, তবে এই জিরো ডে ব্যবহার করে অনায়াসেই সেই মেশিনের ভেতর অবাধে ঢুকে পড়া যায়।

হাল্টকুইস্টের কাছে আইসাইটের ইউক্রেন অফিস থেকে যে ফাইলটা পাঠানো হয়েছিল, সেটা ছিল একটা পাওয়ারপয়েন্ট অ্যাটাচমেন্ট। পৃথিবীর সবচেয়ে জনপ্রিয় সফটওয়্যারগুলোর একটা হলো মাইক্রোসফট অফিস, আর এই ফাইলটা সেই অফিসের ভেতরেই একদম নিঃশব্দে কোড রান করার কাজটা সেরে ফেলছিল বলে মনে হচ্ছিল।

ইমেইলটা পড়ার সাথে সাথেই হাল্টকুইস্টের মাথার ভেতর বিপদের সাইরেন বাজতে শুরু করল। ইউক্রেনীয়রা যা ভাবছিল, এই আবিষ্কার যদি সত্যিই তা হয়ে থাকে, তার মানে দাঁড়ায় কোনো অচেনা হ্যাকার গোষ্ঠীর হাতে এমন এক ভয়ংকর ক্ষমতা চলে এসেছে যা দিয়ে তারা লাখ লাখ কম্পিউটার চোখের পলকে হাইজ্যাক করে নিতে পারে। আর এই ক্ষমতা তারা এরমধ্যেই ব্যবহারও করেছে। মাইক্রোসফটকে তাদের এই ত্রুটির কথা এক্ষুনি জানানো দরকার। তবে একটু স্বার্থপরের মতো চিন্তা করলে,

একটা জিরো ডে খুঁজে পাওয়া আইসাইটের মতো ছোট একটা কোম্পানির জন্য রীতিমতো বিশাল এক মাইলফলক। থ্রেট ইন্টেলিজেন্স নামের এই নতুন সিকিউরিটি ইন্ডাস্ট্রিতে নাম কামানো আর কাস্টমার টানার জন্য এর চেয়ে ভালো সুযোগ আর কী হতে পারে! কোম্পানিটি বছরে বড়জোর দুই বা তিনটা এমন গোপন ক্রুটির সন্ধান পেত। এর প্রতিটিই ছিল এক ধরনের বিমূর্ত, চরম বিপজ্জনক এক বিস্ময় এবং গবেষণার দুনিয়ায় বিশাল এক জয়। হাল্টকুইস্টের ভাষায়, ছোট একটা কোম্পানির জন্য এমন একটা সোনার টুকরো খুঁজে পাওয়াটা প্রচণ্ড তৃপ্তির ব্যাপার। এটা আমাদের জন্য সত্যিই বিশাল একটা ঘটনা ছিল।

হাল্টকুইস্ট ছিলেন পূর্ব টেনেসির এক সাবেক সেনা কর্মকর্তা। গলার আওয়াজ বেশ চড়া, শরীরের গড়ন অনেকটা ভালুকের মতো, গালভর্তি ঘন কালো দাড়ি, আর ঠোঁটের কোণে সবসময় লেগেই থাকে একটা হাসি। নিজের ডেস্কে বসে মাঝে মাঝেই তিনি পাশের রুমের দিকে চিৎকার করে কথা বলতেন। ওই রুমটার নাম ছিল বুল পেন। রুমটার একপাশে বসতেন ম্যালওয়্যার বিশেষজ্ঞরা, আর অন্যপাশে বসতেন থ্রেট অ্যানালিস্টরা। এই অ্যানালিস্টদের কাজ ছিল ডিজিটাল হামলার পেছনের ভূ-রাজনৈতিক উদ্দেশ্যগুলো খুঁজে বের করা। আইসাইটের ইউক্রেনীয় কর্মীদের পাঠানো ইমেইলটা পড়ার সাথে সাথেই হাল্টকুইস্ট তড়বড় করে নিজের অফিস থেকে বেরিয়ে সোজা বুল পেনে ঢুকে পড়লেন। সবাইকে পরিস্থিতি বুঝিয়ে যার যার কাজ বুঝিয়ে দিলেন। তারা তখনো ঘুণাক্ষরেও টের পাননি যে, তারা আসলে এই ছোট কোম্পানির ইতিহাসের সবচেয়ে বড় আবিষ্কারগুলোর একটা নিয়ে কাজ শুরু করতে যাচ্ছেন।

তবে বারান্দার শেষ মাথায়, সেই ব্ল্যাক রুমের ভেতরে বসে থাকা হ্যাকার সন্ন্যাসীরাই মূলত আইসাইটের এই আবিষ্কারের আসল গুরুত্বটা বুঝতে শুরু করেছিলেন। এটা ছিল ক্ষতিকর ইঞ্জিনিয়ারিংয়ের এক ছোট্ট, গুপ্ত বিস্ময়।

জ্বলজ্বলে মনিটরের আলোই ছিল ওই ঘরের একমাত্র আলোর উৎস। সেই কম্পিউটারগুলোতে বসে রিভার্স ইঞ্জিনিয়াররা ইউক্রেনীয়দের পাঠানো সেই ম্যালওয়্যার যুক্ত পাওয়ারপয়েন্ট অ্যাটাচমেন্টটা একের পর এক ভার্চুয়াল মেশিনের ভেতর চালাতে লাগলেন। এই ভার্চুয়াল মেশিনগুলো হলো আসল কম্পিউটারের ভেতরে তৈরি করা নকল কম্পিউটারের এক ধরনের ক্ষণস্থায়ী রূপ। আর এই নকল কম্পিউটারগুলো মূল কম্পিউটার থেকে ঠিক ততটাই আলাদা আর সুরক্ষিত, যতটা আইসাইটের বাকি অফিস থেকে এই ব্ল্যাক রুমটা আলাদা।

এই সুরক্ষিত আবদ্ধ বাক্সগুলোতে কোডটাকে ঠিক এমনভাবে পরীক্ষা করা যায়, ঠিক যেমন কাঁচের অ্যাকুয়ারিয়ামের ভেতর আটকে পড়া কোনো কাঁকড়াবিছাকে পর্যবেক্ষণ করা হয়। রিভার্স ইঞ্জিনিয়াররা ইচ্ছে করেই ওই কোডটাকে তার ভার্চুয়াল শিকারদের ওপর বারবার আক্রমণ করার সুযোগ দিচ্ছিলেন। হামলার মাত্রা আর ধরন বোঝার জন্য তারা বিভিন্ন ডিজিটাল মেশিনের নকল রূপ তৈরি করছিলেন, যেখানে উইন্ডোজ আর মাইক্রোসফট অফিসের নানা রকম ভার্সন চালানো হচ্ছিল। যখন তারা নিশ্চিত হলেন যে কোডটা পাওয়ারপয়েন্ট ফাইল থেকে নিজেই বেরিয়ে আসতে পারে এবং সফটওয়্যারের একদম নতুন আপডেট করা ভার্সনগুলোরও পুরো নিয়ন্ত্রণ নিয়ে নিতে পারে, তখন তাদের আর কোনো সন্দেহ রইল না। ইউক্রেনীয়রা আর হাল্টকুইস্ট যেমনটা সন্দেহ করেছিলেন, এটা আসলেই একটা জিরো ডে, ঠিক ততটাই দুর্লভ আর ঠিক ততটাই শক্তিশালী। কাজ করতে করতে কখন যে সন্ধ্যা গড়িয়ে রাত হয়ে গেল, ওই ঘরের ভেতরে বসে তারা টেরই পেলেন না। সেই রাতের মধ্যেই তারা মাইক্রোসফট এবং তাদের ক্লায়েন্টদের জন্য বিস্তারিত একটা রিপোর্ট তৈরি করে ফেললেন। এমনকি তারা ওই কোডটার নিজস্ব একটা রূপও দাঁড় করালেন, যাকে বলা যায় প্রুফ অব কনসেপ্ট। টেস্টটিউবে রাখা জীবাণুর মতো এটা চোখে আঙুল দিয়ে দেখিয়ে দিচ্ছিল আক্রমণটা ঠিক কীভাবে কাজ করে।

ব্ল্যাক রুমের দুই রিভার্স ইঞ্জিনিয়ারের একজন জন এরিকসন আমাকে বুঝিয়ে বলেছিলেন, পাওয়ারপয়েন্টের ক্ষমতা আসলে জাদুকরী। বছরের পর বছর ধরে আপডেট হতে হতে এটা এখন এমন এক জটিল যন্ত্রে পরিণত হয়েছে, যার পরতে পরতে ঠাসা অসংখ্য অপ্রয়োজনীয় ফিচার। এর গঠন এতই প্যাঁচানো যে এটাকে আস্ত একটা প্রোগ্রামিং ল্যাঙ্গুয়েজ বললেও খুব একটা ভুল হবে না। আর যে বা যারা এই জিরো ডে বানিয়েছে, তারা এর এমন একটা ফিচার নিয়ে গভীর পড়াশোনা করেছে, যেটা দিয়ে যে কেউ প্রেজেন্টেশনের ভেতর কোনো তথ্য বা অবজেক্ট বসিয়ে দিতে পারে। সেটা হতে পারে পাওয়ারপয়েন্ট ফাইলের ডেটা বান্ডেল থেকে নেওয়া কোনো চার্ট বা ভিডিও, আবার ইন্টারনেটের মাধ্যমে দূরের কোনো কম্পিউটার থেকে টেনে আনা কোনো ফাইল।

এক্ষেত্রে হ্যাকাররা ওই ফিচারটা ব্যবহার করে খুব সাবধানে প্রেজেন্টেশনের ভেতরে দুই টুকরো ডেটা বসিয়ে দিয়েছিল। প্রথম টুকরোটা টার্গেট করা কম্পিউটারের একটা টেম্পোরারি ফোল্ডারে গিয়ে জমা হতো। আর দ্বিতীয় টুকরোটা কাজে লাগাত

পাওয়ারপয়েন্টের অ্যানিমেশন ফিচারকে। পাওয়ারপয়েন্টের অ্যানিমেশন দিয়ে বক্তারা চলমান লেখা আর কার্টুন দেখিয়ে দর্শকদের একঘেয়েমিতে ভোগান, কাজটা এতটুকুর মাঝেই সীমাবদ্ধ নেই। এটা আসলে যেই কম্পিউটারে প্রেজেন্টেশন চলছে, সেখানে নানা রকম কমান্ড বা নির্দেশও চালাতে পারে। এই নির্দিষ্ট ক্ষেত্রে, প্রেজেন্টেশনটা যখন ওই অ্যানিমেশন ফাইলটা লোড করত, তখন স্বয়ংক্রিয়ভাবে একটা স্ক্রিপ্ট চালু হয়ে যেত। সেই স্ক্রিপ্ট প্রেজেন্টেশনের বসিয়ে রাখা প্রথম ফাইলটার ওপর রাইট ক্লিক করত এবং ড্রপ-ডাউন মেনু থেকে ইন্সটল বাটনে ক্লিক করে দিত। ফলে ব্যবহারকারী ঘুণাক্ষরেও টের পাওয়ার আগেই ওই ম্যালওয়্যার কোড কম্পিউটারে নিজের শক্ত ঘাঁটি গেড়ে বসত। ব্যাপারটা অনেকটা এমন, আপনার দরজার সামনে কেউ একটা নিরীহ চেহারার প্যাকেট রেখে গেছে। আপনি সেটাকে ঘরের ভেতরে আনার পরক্ষণেই প্যাকেটটা থেকে একটা হাত গজিয়ে উঠল, সেটা নিজেই নিজেকে কেটে খুলল, আর আপনার বসার ঘরে একগাদা ছোট্ট রোবট ছেড়ে দিল। ভুক্তভোগী ব্যক্তি অ্যাটাচমেন্টটা খোলার জন্য ডাবল ক্লিক করার সাথে সাথে এই পুরো ব্যাপারটা ঘটত চোখের পলকে এবং সম্পূর্ণ লোকচক্ষুর অন্তরালে।

আইসাইটের ব্ল্যাক রুমে বসে এই জিরো ডে নিয়ে প্রথম কাজ করা রিভার্স ইঞ্জিনিয়ার এরিকসন তার সেই কাজটির কথা স্মরণ করেন। এই হামলাটাকে টুকরো টুকরো করে তার কার্যকারিতা নষ্ট করার কাজটা তার কাছে ছিল দুর্লভ, রোমাঞ্চকর, তবে একেবারেই আবেগহীন একটা ঘটনা। নিজের ক্যারিয়ারে তিনি খুব অল্প কয়েকটা সত্যিকারের জিরো ডে নিয়ে কাজ করার সুযোগ পেয়েছেন। তবে তিনি হাজার হাজার ম্যালওয়্যার নমুনা বিশ্লেষণ করেছেন এবং সেগুলোকে স্রেফ গবেষণার উপকরণ হিসেবে ভাবতে শিখেছেন। এসবের পেছনে কোনো কারিগর আছে, কোনো রক্তমাংসের মানুষ এই শয়তানি কলকব্জাগুলো জুড়ে দিয়েছে, এসব নিয়ে তিনি মাথা ঘামাতেন না। তার ভাষায়, এটা ছিল স্রেফ অচেনা কোনো মানুষের তৈরি করা অজানা একটা জিনিস, যা আমি আগে কখনো দেখিনি।

তবে জিরো ডেগুলোর তো একজন জন্মদাতা থাকেই। ওইদিন সকালে নিজের সেই অন্ধকার ল্যাবরেটরিতে বসে এরিকসন যখন প্রথম এটাকে খুলতে শুরু করেছিলেন, তখন তিনি নেহাত প্রাকৃতিকভাবে তৈরি হওয়া কোনো প্রাণহীন ধাঁধা নিয়ে পড়ে ছিলেন না। তিনি আসলে বহুদূরে বসে থাকা কোনো এক অশুভ, ভয়ংকর বুদ্ধিমত্তার প্রথম আভাস দেখে মুগ্ধ হচ্ছিলেন।

ব্ল্যাকএনার্জি

জিরো ডে আবিষ্কারের পর আইসাইটের ভেতরের সেই প্রাথমিক উত্তেজনা যখন একটু থিতিয়ে এল, তখন কয়েকটা প্রশ্ন সামনে এসে দাঁড়াল। এই ক্ষতিকর কোডটা কে লিখেছে? কাদেরকে লক্ষ্য করে এই হামলা চালানো হচ্ছে, আর কেনই বা করা হচ্ছে?

এই প্রশ্নগুলোর উত্তর খোঁজার দায়িত্ব পড়ল আইসাইটের ম্যালওয়্যার অ্যানালিস্ট ড্রিউ রবিনসনের কাঁধে। জন হাল্টকুইস্ট তাকে ডাকতেন ডেওয়াকার বা দিনের বেলা ঘুরে বেড়ানো মানুষ বলে। ব্ল্যাক রুমের সেই ভ্যাম্পায়ার দলের মতো রবিনসনেরও রিভার্স ইঞ্জিনিয়ারিংয়ের দারুণ সব স্কিল ছিল। কিন্তু তিনি বসতেন হাল্টকুইস্টের অফিসের পাশের সেই আলো-ঝলমলে বুল পেনে। হ্যাকিংয়ের এই মিশনগুলোর পেছনে কারা জড়িত, আর তাদের রাজনৈতিক উদ্দেশ্যই বা কী, এমন বিশাল পরিসরের একটা ক্যানভাস নিয়ে বিশ্লেষণ করার দায়িত্ব ছিল তার ওপর।

এই বিশাল গুপ্ত অভিযানের পেছনের রহস্যের জট খোলার দায়িত্ব পড়ল রবিনসনের ঘাড়ে। তার কাজ ছিল ওই পাওয়ারপয়েন্টের ভেতরে থাকা কারিগরি সূত্রগুলো ধরে ধরে সামনে এগিয়ে যাওয়া।

সেই বুধবার সকালে পাওয়ারপয়েন্ট জিরো ডে আবিষ্কারের ঘোষণা দিতে হাল্টকুইস্ট বুল পেনে ঢোকার কয়েক মিনিটের মাঝেই রবিনসন কাজে লেগে গেলেন। তিনি সেই ফাঁদ পাতা অ্যাটাচমেন্টের ভেতরের জিনিসপত্র নিয়ে একেবারে আঠার মতো লেগে রইলেন। আসল প্রেজেন্টেশনটার দিকে তাকালে মনে হয়, নীল আর হলুদ রঙের ইউক্রেনীয় পতাকার ওপর সিরিলিক অক্ষরে কিছু নাম লেখা। সাথে ইউক্রেনের জাতীয় প্রতীকের একটা জলছাপ। হলুদ ঢালের ওপর হালকা নীল রঙের একটা ত্রিশূল। গুগল ট্রান্সলেট ব্যবহার করার পর রবিনসন বুঝতে পারলেন, এই নামগুলো আসলে একদল সন্দেহভাজন সন্ত্রাসীর। সেই বছরের শুরুতে রাশিয়ান সৈন্যরা যখন ইউক্রেনের পূর্বাঞ্চল আর ক্রিমিয়া উপদ্বীপে হামলা চালিয়ে বিচ্ছিন্নতাবাদী আন্দোলন উসকে দিয়ে একটা চলমান যুদ্ধের সূচনা করেছিল, তখন এই লোকগুলো রাশিয়ার পক্ষ নিয়েছিল।

জিরো ডে সংক্রমণ ছড়ানোর জন্য হ্যাকাররা একটা রুশ-বিরোধী বার্তা বেছে নিয়েছে। এটাই ছিল রবিনসনের হাতে আসা প্রথম সূত্র। এই ইমেইলটা খুব সম্ভবত

ইউক্রেনীয়দের লক্ষ্য করে চালানো একটা রাশিয়ান অপারেশন। দেশের মানুষের দেশপ্রেম আর ভেতরের ক্রেমলিন-সমর্থকদের নিয়ে তাদের ভয়কে পুঁজি করেই এই চালটা চালা হয়েছে। এই চক্রান্তের পেছনে থাকা হ্যাকারদের সম্পর্কে আরও সূত্র খুঁজতে গিয়ে তিনি খুব জলদি আরেকটা সুতোর খোঁজ পেয়ে গেলেন। পাওয়ারপয়েন্ট জিরো ডে যখন কাজ শুরু করত, তখন এটি ভুক্তভোগীর সিস্টেমে যে ফাইলটা নামিয়ে দিত, সেটা আসলে এক কুখ্যাত ম্যালওয়্যারেরই একটা রূপ। এই ম্যালওয়্যার অচিরেই আরও অনেক বেশি ভয়ংকর হয়ে উঠবে। এর নাম ব্ল্যাকএনার্জি।

সেই সময় পর্যন্ত ব্ল্যাকএনার্জির ছোট্ট ইতিহাসে সাধারণ হ্যাকিং অপারেশনের নানা স্তরের একটা চমৎকার ধারণা পাওয়া যায়। একেবারের নিচের স্তরের স্ক্রিপ্ট কিডি থেকে শুরু করে পেশাদার সাইবার অপরাধীদের পর্যন্ত এর বিচরণ ছিল। স্ক্রিপ্ট কিডিরা এতই অদক্ষ হ্যাকার যে তারা সাধারণত অন্য কোনো অভিজ্ঞ মানুষের বানানো টুল ব্যবহার করেই কাজ সারে। এই টুলটা আসলে তৈরি করেছিল দিমিত্রো ওলেক্সিউক নামের এক রাশিয়ান হ্যাকার। হ্যাকিংয়ের দুনিয়ায় সে ক্র্যাশ নামে পরিচিত ছিল। ২০০৭ সালের দিকে ওলেক্সিউক রাশিয়ান ভাষার হ্যাকার ফোরামগুলোতে ব্ল্যাকএনার্জি বিক্রি করত। দাম ছিল চল্লিশ ডলারের কাছাকাছি। এর কন্ট্রোল প্যানেলের এক কোণায় গ্রাফিতির মতো জ্বলজ্বল করত তার নাম।

টুলটা বানানো হয়েছিল একটা নির্দিষ্ট উদ্দেশ্য নিয়ে। একে বলা হয় ডিস্ট্রিবিউটেড ডিনায়াল-অব-সার্ভিস বা ডিডস অ্যাটাক। এর কাজ হলো একসাথে শত শত বা হাজার হাজার কম্পিউটার থেকে কোনো ওয়েবসাইটে নকল তথ্যের অনুরোধ পাঠিয়ে তাকে ভাসিয়ে দেওয়া, যার ফলে ওয়েবসাইটটা অফলাইন হয়ে যায়। কোনো ভুক্তভোগীর মেশিনে ব্ল্যাকএনার্জি ঢুকিয়ে দিতে পারলেই সেটা তথাকথিত বটনেটের সদস্য হয়ে যেত। বটনেট হলো হাইজ্যাক করা অনেকগুলো কম্পিউটারের একটা দল, যেগুলোকে বট বলা হয়। বটনেটের অপারেটর খুব সহজেই ওলেক্সিউকের এই ব্যবহারবান্ধব সফটওয়্যারটা দিয়ে ঠিক করে দিতে পারত তার দখলে থাকা মেশিনগুলো কোন ওয়েবসাইটের ওপর ভুয়া অনুরোধের আঘাত হানবে। এমনকি এই ডিজিটাল গোলাবর্ষণের ধরন আর গতি কেমন হবে, সেটাও নিয়ন্ত্রণ করা যেত।

২০০৭ সালের শেষের দিকে নিরাপত্তা প্রদানকারী প্রতিষ্ঠান আর্বর নেটওয়ার্কস গুনে গুনে দেখেছিল যে, ব্ল্যাকএনার্জি দিয়ে বানানো ত্রিশটার বেশি বটনেট কাজ করছে। এগুলোর বেশিরভাগের লক্ষ্যই ছিল রাশিয়ান ওয়েবসাইটগুলোতে হামলা চালানো।

সাইবার হামলার আধুনিকতার স্কেলে বিচার করলে, ডিস্ট্রিবিউটেড ডিনায়াল-অব-সার্ভিস আক্রমণগুলো ছিল একদমই কাঁচা আর ভোঁতা ধরনের। এগুলো দিয়ে ওয়েবসাইট সাময়িকভাবে বন্ধ রেখে আর্থিক ক্ষতি করা যেত ঠিকই, কিন্তু অনেক গভীরে গিয়ে হ্যাকিংয়ের যে আসল কৌশল দিয়ে গুরুত্বপূর্ণ ডেটা চুরি করা হয়, সেই মারাত্মক কাজটা এর দ্বারা সম্ভব ছিল না।

তবে এর পরের বছরগুলোতে ব্ল্যাকএনার্জি অনেক আধুনিক হয়ে উঠেছিল। নিরাপত্তা বিশ্লেষক প্রতিষ্ঠানগুলো এই সফটওয়্যারের একটা নতুন ভার্সন ধরতে শুরু করল। এই নতুন রূপে যুক্ত হয়েছিল ইচ্ছেমতো বদলানো যায় এমন সব ফিচারের এক বিশাল ভাণ্ডার। এই নতুন করে সাজানো টুলটি দিয়ে আগের মতোই ওয়েবসাইটগুলোতে আবর্জনা ট্রাফিকের বন্যা বইয়ে দেওয়া যেত। সেই সাথে একে দিয়ে স্প্যাম ইমেইল পাঠানো, আক্রান্ত কম্পিউটারের ফাইল ধ্বংস করা, এবং ব্যাংকিংয়ের ইউজারনেম আর পাসওয়ার্ড চুরি করার কাজটাও করিয়ে নেওয়া যেত।

এখন রবিনসনের চোখের সামনে ব্ল্যাকএনার্জি একেবারে নতুন আরেকটা রূপে হাজির হয়েছে। আইসাইটের বুল পেনে বসে তিনি যে ভার্সনটা দেখছিলেন, সেটা আগে পড়া যেকোনো ভার্সনের চেয়ে একেবারেই আলাদা মনে হচ্ছিল। নিশ্চিতভাবেই এটা কোনো সাধারণ ওয়েবসাইট আক্রমণের টুল নয়। আর আর্থিক জালিয়াতির টুল হওয়ার সম্ভাবনাও একদমই নেই। আর্থিক জালিয়াতির একটা সাইবার ক্রাইম কেন টোপ হিসেবে রুশ-পন্থী সন্ত্রাসীদের নামের তালিকা ব্যবহার করবে? এই ছদ্মবেশটা পুরোটাই রাজনৈতিক উদ্দেশ্যপ্রণোদিত বলে মনে হচ্ছিল। ইউক্রেনীয় ব্ল্যাকএনার্জির নমুনাটার দিকে প্রথমবার তাকিয়েই তার সন্দেহ হতে শুরু করল যে, তিনি এমন একটা কোডের রূপ দেখছেন যার লক্ষ্য নতুন কিছু। এটা সাধারণ কোনো অপরাধ নয়, এর আসল উদ্দেশ্য হলো গুপ্তচরবৃত্তি।

এরপর খুব তাড়াতাড়িই রবিনসনের ভাগ্য খুলে গেল। তিনি এমন একটা জিনিস খুঁজে পেলেন যা এই ম্যালওয়্যারের উদ্দেশ্য সম্পর্কে আরও পরিষ্কার ধারণা দিল। একটা ভার্চুয়াল মেশিনে এই নতুন ব্ল্যাকএনার্জির নমুনাটা চালানোর পর, সেটা ইন্টারনেটের মাধ্যমে ইউরোপের কোথাও একটা আইপি অ্যাড্রেসের সাথে যুক্ত হওয়ার চেষ্টা করল। তিনি মুহূর্তেই বুঝতে পারলেন যে ওই সংযোগটা আসলে একটা কমান্ড-অ্যান্ড-কন্ট্রোল সার্ভার, যা অনেকটা দূরের কোনো পুতুলনাচের কারিগরের মতো পুরো প্রোগ্রামটাকে নিয়ন্ত্রণ করছিল। রবিনসন যখন তার ওয়েব

ব্রাউজার দিয়ে নিজেই ওই দূরের মেশিনটাতে ঢোকার চেষ্টা করলেন, তখন তিনি রীতিমতো আনন্দিত হওয়ার পাশাপাশি বেশ চমকেও গেলেন। কমান্ড-অ্যান্ড-কন্ট্রোল কম্পিউটারটাকে একদমই অরক্ষিত অবস্থায় ফেলে রাখা হয়েছিল। যে কেউ চাইলেই ইচ্ছেমতো এর ভেতরের ফাইলগুলো ঘাঁটাঘাঁটি করতে পারত।

আশ্চর্যের বিষয় হলো, এই ফাইলগুলোর মাঝে ব্ল্যাকএনার্জির এই নতুন ভার্সনটার একটা হেল্প ডকুমেন্টও ছিল, যেখানে খুব সুন্দর করে এর সব কমান্ডের তালিকা দেওয়া ছিল। এটা রবিনসনের সন্দেহকে একেবারে সত্যি প্রমাণ করে দিল। সাইবার ক্রাইমের তদন্তে সাধারণত ম্যালওয়্যারের যে নমুনাগুলো পাওয়া যায়, তার চেয়ে জিরো ডে দিয়ে পাঠানো ব্ল্যাকএনার্জির এই ভার্সনটার ডেটা বা তথ্য সংগ্রহের ক্ষমতা ছিল অনেক বেশি বিশাল। এই প্রোগ্রামটা স্ক্রিনশট নিতে পারত, ভুক্তভোগীর মেশিন থেকে ফাইল আর এনক্রিপশন কি বের করে আনতে পারত। এমনকি কিবোর্ডে কোন কোন বোতাম চাপা হচ্ছে সেটাও রেকর্ড করে রাখতে পারত। এসব আসলে কোনো টাকা-পয়সার লোভে করা ব্যাংক জালিয়াতির লক্ষণ নয়, এগুলো একদম সুনির্দিষ্ট আর নিখুঁত সাইবার গুপ্তচরবৃত্তির সবচেয়ে বড় প্রমাণ।

তবে ওই হেল্প ফাইলের ভেতরে কী লেখা আছে, তার চেয়েও বড় ব্যাপার ছিল সেটা কোন ভাষায় লেখা। আর ভাষাটা ছিল রাশিয়ান।

আরাকিস ০২

সাইবার সিকিউরিটি ইন্ডাস্ট্রি সবসময় 'অ্যাট্রিবিউশন প্রবলেম' বা আক্রমণকারীকে চিহ্নিত করার সমস্যার কথা বলে সতর্ক করে। যেকোনো অপারেশনের পেছনে, বিশেষ করে এরকম জটিল হামলার পেছনে থাকা দূরের হ্যাকারদের আসল পরিচয় বের করা প্রায় অসম্ভব একটা ব্যাপার। ইন্টারনেটে প্রক্সি ব্যবহার করা, ভুল পথে চালিত করা বা ভৌগোলিক অবস্থান নিয়ে ধোঁয়াশা তৈরির সুযোগ এত বেশি যে আসল কালপ্রিট ধরা কঠিন। কিন্তু আনসিকিউরড কমান্ড-অ্যান্ড-কন্ট্রোল সার্ভারটা খুঁজে বের করে রবিনসন আইসাইটের ব্ল্যাকএনার্জি রহস্যের জাল ছিন্ন করে ফেললেন। তার হাতে চলে এল হ্যাকারদের পরিচয় বের করার এক দুর্লভ সূত্র। পাওয়ারপয়েন্ট হ্যাকিংয়ে এত সাবধানতা অবলম্বন করার পরও, হ্যাকাররা নিজেদের অজান্তেই তাদের জাতীয়তার একটা বড় প্রমাণ ফেলে গিয়েছিল।

তবে এই অপ্রত্যাশিত সৌভাগ্যের পরও রবিনসনের আসল কাজ বাকি ছিল। ম্যালওয়্যার কোডের নাড়িভুঁড়ি ঘেঁটে আরও সূত্র বের করার কাজটা তখনো তার সামনে পাহাড়ের মতো দাঁড়িয়ে। তাকে এমন একটা 'সিগনেচার' বা ডিজিটাল স্বাক্ষর তৈরি করতে হবে, যেটা দিয়ে নিরাপত্তা প্রতিষ্ঠানগুলো আর আইসাইটের ক্লায়েন্টরা বুঝতে পারবে তাদের নেটওয়ার্কও একই প্রোগ্রাম দিয়ে আক্রান্ত হয়েছে কি না। ম্যালওয়্যার কোডের কার্যপদ্ধতি উদ্ধার করাটা কমান্ড-অ্যান্ড-কন্ট্রোল সার্ভার ট্র্যাক করার মতো এত সহজ কাজ ছিল না। টানা কয়েক দিনের হাড়ভাঙা, মাথা-খারাপ-করা খাটুনির পর রবিনসন হাড়ে হাড়ে টের পেলেন যে, কোডটাকে কমপ্রেশন আর এনক্রিপশনের তিনটা আলাদা লেয়ার বা স্তর দিয়ে দারুণভাবে পেঁচিয়ে রাখা হয়েছে।

অন্য কথায় বলতে গেলে, ম্যালওয়্যারের এই গোপন রহস্য ভেদ করাটা ছিল অনেকটা ট্রেজার হান্টের মতো। রবিনসন জানতেন ম্যালওয়্যারটা স্বয়ংসম্পূর্ণ। তাই নিজেকে ডিকোড করে কোডটা চালানোর জন্য সব এনক্রিপশন কি এর ভেতরেই থাকার কথা। তবে প্রতিটি স্তরের চাবি কেবল তার ওপরের স্তরটা ডিকোড করার পরই পাওয়া সম্ভব। এলোমেলো নয়েজের ভেতর থেকে চেনা প্যাটার্ন স্ক্যান করে হ্যাকারদের ব্যবহার করা কমপ্রেশন অ্যালগরিদমটা তো তিনি কোনোমতে আন্দাজ করলেন। কিন্তু তারা ঠিক কোন এনক্রিপশন স্কিম ব্যবহার করেছে, সেটা বের করতে তার আরও কয়েক দিন কেটে গেল। এনক্রিপশনটা ছিল প্রচলিত একটা সিস্টেমের একদমই নতুন আর অন্যরকম একটা রূপ। এই ধাঁধার গভীরে রবিনসন এতটাই ডুবে গেলেন যে, ডেস্কে বসে মাথা তুলতেই দেখতেন হুস করে কয়েক ঘণ্টা পার হয়ে গেছে। এমনকি বাসায় ফিরে শাওয়ারের নিচে দাঁড়িয়েও তার মনে হতো তিনি যেন ঘোরের মধ্যে আছেন, মাথার ভেতর কেবল ওই সাইফার বা গুপ্তসংকেতটাই ঘুরপাক খাচ্ছে।

এক সপ্তাহ ধরে নানা রকম চেষ্টা আর ভুলের পর রবিনসন যখন অবশেষে ওই গোলকধাঁধার স্তরগুলো ভাঙতে পারলেন, তখন পুরস্কার হিসেবে তার সামনে ভেসে উঠল ব্ল্যাকএনার্জির নমুনার লাখ লাখ শূন্য আর এক। একনজরে এই ডেটাগুলোর কোনো অর্থই হয় না। কারণ এটা ছিল প্রোগ্রামের কম্পাইল করা রূপ। মানুষের পড়ার উপযোগী কোনো প্রোগ্রামিং ল্যাঙ্গুয়েজের বদলে মেশিনের পড়ার মতো বাইনারিতে রূপান্তর করা। এই বাইনারি বুঝতে হলে রবিনসনকে তার কম্পিউটারে কোডটাকে ধাপে ধাপে এক্সিকিউট বা রান হতে দেখতে হবে। 'আইডিএ প্রো' নামের খুব পরিচিত একটা রিভার্স ইঞ্জিনিয়ারিং টুল দিয়ে তিনি রিয়েল টাইমে এর জট ছাড়াতে

লাগলেন। টুলটা কমান্ডগুলো রান করার সাথে সাথে সেগুলোর কাজকে কোডে রূপান্তর করে দিচ্ছিল। রবিনসনের ভাষায়, 'ব্যাপারটা অনেকটা এমন যে, আপনি কেবল কারও ডিএনএ দেখে তার চেহারা কেমন হবে সেটা বোঝার চেষ্টা করছেন। আর যে ঈশ্বর ওই মানুষটাকে বানিয়েছেন, তিনি পুরো প্রক্রিয়াটাকে যতটা সম্ভব কঠিন করে রাখার চেষ্টা করছেন।'

তবে দ্বিতীয় সপ্তাহে এসে বাইনারির ওই অণুবীক্ষণিক ধাপে ধাপে করা বিশ্লেষণ অবশেষে কাজে দিতে শুরু করল। তিনি যখন ম্যালওয়্যারের কনফিগারেশন সেটিংস ডিকোড করতে পারলেন, তখন সেখানে একটা ক্যাম্পেইন কোড দেখতে পেলেন। এটা মূলত ওই ম্যালওয়্যার ভার্সনের সাথে যুক্ত একটা ট্যাগ, যা দিয়ে হ্যাকাররা আক্রান্ত শিকারদের আলাদা করতে এবং ট্র্যাক করতে পারত। ইউক্রেনীয় পাওয়ারপয়েন্ট থেকে নেমে আসা ব্ল্যাকএনার্জির নমুনায় থাকা সেই ক্যাম্পেইন কোডটা তিনি দেখামাত্রই চিনে ফেললেন। তবে ম্যালওয়্যার অ্যানালিস্ট হিসেবে তার ক্যারিয়ারের অভিজ্ঞতা থেকে নয়, তার ব্যক্তিজীবনের সায়েন্স ফিকশন প্রেমের কারণে। কোডটা ছিল 'আরাকিস০২'।

আসলে রবিনসন বা সায়েন্স ফিকশন নিয়ে ঘাঁটাঘাঁটি করা যেকোনো গিকের কাছেই 'আরাকিস' শব্দটা খুবই পরিচিত। এটা ট্যাটুইন বা মিডল-আর্থের মতোই চেনা একটা নাম, যা পপ কালচারের একদম মূল ভিত্তির একটা অংশ। আরাকিস হলো সেই মরুভূমির গ্রহ, যেখানে ফ্র্যাংক হারবার্টের ১৯৬৫ সালের বিখ্যাত এপিক উপন্যাস 'ডিউন' এর কাহিনি আবর্তিত হয়েছে।

ডিউন এর গল্প এমন এক জগতকে ঘিরে তৈরি, যেখানে আর্টিফিশিয়াল ইন্টেলিজেন্স বা কৃত্রিম বুদ্ধিমত্তার মেশিনের বিরুদ্ধে হওয়া এক বৈশ্বিক পরমাণু যুদ্ধে পৃথিবী বহুকাল আগেই ধ্বংস হয়ে গেছে। গল্পের কেন্দ্রবিন্দুতে আছে এক মহৎ অ্যাট্রেইডিস পরিবার। আরাকিস বা ডিউন গ্রহের শাসক হিসেবে তাদের বসানো হয়। এরপর তাদের চরম শত্রু হারকোনেনরা রাজনৈতিক চক্রান্ত করে তাদেরকে ক্ষমতা থেকে টেনেহিঁচড়ে নামিয়ে দেয়।

অ্যাট্রেইডিসদের পতন হওয়ার পর, বইয়ের কিশোর নায়ক পল অ্যাট্রেইডিস গ্রহের বিশাল মরুভূমিতে আশ্রয় নেয়। এই মরুভূমির মাটির নিচ দিয়ে হাজার ফুট লম্বা সব স্যান্ডওয়ার্ম ঘুরে বেড়ায়। মাঝেমধ্যে এরা মাটির ওপরে উঠে আসে আর সামনে যা পায় গিলে খায়। পল ধীরে ধীরে বড় হয় এবং আরাকিসের স্থানীয় বাসিন্দা, যাদের

ফ্রিমেন বলা হয়, তাদের জীবনযাপন আয়ত্ত করে। এমনকি সে স্যান্ডওয়ার্মগুলোকে পোষ মানিয়ে তাদের পিঠে চড়তেও শেখে। একসময় সে সাধারণ মানুষের এক গেরিলা অভ্যুত্থানের নেতৃত্ব দেয়। স্যান্ডওয়ার্মের পিঠে চড়ে এক ভয়াবহ যুদ্ধে অবতীর্ণ হয় পল। স্থানীয় ফ্রিমেনদের সাথে নিয়ে সে হারকোনেনদের কাছ থেকে রাজধানী ছিনিয়ে নেয়। শেষমেশ তাদের এই বিদ্রোহ সেই বিশাল সাম্রাজ্যের পুরো নিয়ন্ত্রণ নিয়ে নেয়, যারা হারকোনেনদের ওই ক্ষমতা দখলে মদদ জুগিয়েছিল।

রবিনসনের মনে পড়ে, তিনি তখন ভাবছিলেন, 'এই হ্যাকাররা যে-ই হোক না কেন, এরা মনে হচ্ছে ফ্র্যাংক হারবার্টের বিশাল ভক্ত।'

আরাকিস০২ ক্যাম্পেইন কোডটা খুঁজে পাওয়ার পর রবিনসনের মনে হলো, যারা এই নামটা বেছে নিয়েছে, তিনি কেবল তাদের সম্পর্কে একটা সাধারণ সূত্র পাননি, এর চেয়েও বড় কিছুর সন্ধান পেয়েছেন। জীবনে প্রথমবার তার মনে হলো, তিনি যেন হ্যাকারদের মগজ আর কল্পনার জগতে উঁকি দিতে পারছেন। সত্যি বলতে, তিনি ভাবতে শুরু করলেন যে এটা একটা ফিঙ্গারপ্রিন্ট বা আঙুলের ছাপ হিসেবে কাজ করতে পারে। কে জানে, এই ছাপ মিলিয়ে তিনি অন্য কোনো অপরাধের আস্তানাও খুঁজে পেতে পারেন।

পরের কয়েক দিন রবিনসন ব্ল্যাকএনার্জির ওই ইউক্রেনীয় পাওয়ারপয়েন্ট ভার্সনটা একপাশে সরিয়ে রেখে জোরকদমে খোঁড়াখুঁড়ি শুরু করলেন। তিনি আইসাইটের পুরোনো ম্যালওয়্যার নমুনার আর্কাইভ এবং 'ভাইরাসটোটাল' নামের একটা ডেটাবেস ঘাঁটতে লাগলেন। গুগলের প্যারেন্ট কোম্পানি অ্যালফাবেটের মালিকানায় থাকা ভাইরাসটোটাল হলো এমন একটা জায়গা, যেখানে যেকোনো সিকিউরিটি গবেষক কোনো ম্যালওয়্যার আপলোড করে ডজন ডজন কমার্শিয়াল অ্যান্টিভাইরাস প্রোডাক্টের সাথে সেটা মিলিয়ে দেখতে পারেন। অন্য কোনো নিরাপত্তা প্রতিষ্ঠান এই কোডটা অন্য কোথাও পেয়েছে কি না বা এ বিষয়ে তারা কী জানে, সেটা দ্রুত এবং মোটামুটি একটা ধারণা পাওয়ার জন্য এটা দারুণ একটা উপায়। এক দশকেরও বেশি সময় ধরে ইন্টারনেট দুনিয়ায় ঘুরে বেড়ানো কোডের বিশাল এক সংগ্রহশালা গড়ে তুলেছে এই ভাইরাসটোটাল, যেখানে টাকা দিয়ে গবেষকরা ঢোকার সুযোগ পান। রবিনসন ওই ম্যালওয়্যার রেকর্ডগুলোতে একের পর এক স্ক্যান চালাতে লাগলেন। তার ব্ল্যাকএনার্জি নমুনা থেকে তিনি যে কোডের টুকরোগুলো বের করেছিলেন, সেগুলোর সাথে আইসাইট বা ভাইরাসটোটালের পুরোনো কোনো কোডের নমুনার

মিল পাওয়া যায় কি না, সেটাই ছিল তার মূল লক্ষ্য।

খুব জলদিই তার হাতে মোক্ষম একটা জিনিস চলে এল। চার মাস আগের, ২০১৪ সালের মে মাসের আরেকটা ব্ল্যাকএনার্জির নমুনা, যা ইউক্রেনীয় পাওয়ারপয়েন্ট থেকে নামা সেই নমুনাটার প্রায় হুবহু নকল বলা চলে। রবিনসন যখন এর ক্যাম্পেইন কোডটা খুঁড়ে বের করলেন, তিনি যা খুঁজছিলেন ঠিক সেটাই পেয়ে গেলেন। হাউসঅ্যাট্রেইডিস৯৪, ডিউনের আরেকটা জ্বলজ্যান্ত রেফারেন্স। এবার ব্ল্যাকএনার্জির নমুনাটা একটা ওয়ার্ড ডকুমেন্টের ভেতর চালান করে দেওয়া হয়েছিল। সেখানে তেল আর গ্যাসের দাম নিয়ে আলোচনা করা হচ্ছিল। স্পষ্টতই পোল্যান্ডের একটা এনার্জি কোম্পানির জন্য এটা টোপ হিসেবে বানানো হয়েছিল।

পরের কয়েক সপ্তাহ ধরে রবিনসন তার ক্ষতিকর প্রোগ্রামের আর্কাইভ তন্নতন্ন করে খুঁজতে লাগলেন। শেষমেশ তিনি নিজের মতো করে কিছু টুল বানিয়ে ফেললেন। এগুলো দিয়ে ম্যালওয়্যারের মিলগুলো স্ক্যান করা যেত, ফাইলের জটিল এনক্রিপশনের স্তরগুলো খোলার কাজটা স্বয়ংক্রিয়ভাবে করা যেত, আর তারপর সেখান থেকে ক্যাম্পেইন কোডটা টেনে বের করে আনা যেত। তার নমুনার সংগ্রহ ধীরে ধীরে বড় হতে লাগল। বাশারঅফদ্যসারডৌকারস, সালুসাচেকুনডাস২, এপসিলনএরিডানি০। মনে হচ্ছিল হ্যাকাররা যেন ডিউন উপন্যাসের খুঁটিনাটি নিয়ে তাদের গভীর জ্ঞান জাহির করে রবিনসনকে তাক লাগিয়ে দেওয়ার চেষ্টা করছে।

তার পাওয়া প্রথম দুটোর মতোই, এই ডিউন রেফারেন্সগুলোর প্রতিটাই এমন একটা টোপ-ডকুমেন্টের সাথে যুক্ত ছিল, যা থেকে ম্যালওয়্যারটার আসল শিকারদের সম্পর্কে বেশ কিছু তথ্য বেরিয়ে আসছিল। এর মধ্যে একটা ছিল কূটনৈতিক ডকুমেন্ট। সেখানে ইউক্রেনকে নিয়ে রাশিয়া আর ইউরোপের রশি টানাটানি নিয়ে আলোচনা করা হয়েছিল। কারণ দেশটা তখন একদিকে পশ্চিমা বিশ্বের দিকে টেনে নেওয়া এক জনপ্রিয় আন্দোলন আর অন্যদিকে রাশিয়ার টিকে থাকা প্রভাবের মাঝখানে পড়ে হাবুডুবু খাচ্ছিল। আরেকটা বানানো হয়েছিল ওয়েলসে অনুষ্ঠিত ইউক্রেন বিষয়ক একটা সামিট এবং স্লোভাকিয়ায় ন্যাটোর একটা ইভেন্টে অংশ নেওয়া দর্শনার্থীদের জন্য টোপ হিসেবে, যার একটা বড় অংশ জুড়ে ছিল রাশিয়ার গুপ্তচরবৃত্তির আলোচনা। এমনকি একটা টোপ দেখে মনে হচ্ছিল সেটা নির্দিষ্টভাবে একজন আমেরিকান অ্যাকাডেমিক গবেষককে লক্ষ্য করে বানানো, যিনি রাশিয়ার পররাষ্ট্রনীতি নিয়ে কাজ করতেন। আইসাইট সিদ্ধান্ত নিয়েছিল যে তারা এই

গবেষকের নাম প্রকাশ করবে না। হ্যাকারদের ওই কাজের ডিউন রেফারেন্সগুলোর কল্যাণে, আপাতদৃষ্টিতে আলাদা মনে হওয়া এই সবগুলো আক্রমণকে খুব সহজেই এক সুতোয় গাঁথা সম্ভব হলো।

তবে ভুক্তভোগীদের কয়েকজনকে দেখে রাশিয়ার ভূ-রাজনৈতিক গুপ্তচরবৃত্তির সাধারণ শিকার বলে মনে হচ্ছিল না। উদাহরণ হিসেবে বলা যায়, হ্যাকাররা ঠিক কী কারণে পোল্যান্ডের একটা এনার্জি কোম্পানির পেছনে লেগেছিল? আইসাইট পরে দেখতে পায়, আরেকটা টোপ পাতা হয়েছিল ইউক্রেনের রেলওয়ে সংস্থা উকরজালিজনিতসিয়ার জন্য।

কিন্তু রবিনসন যখন ওই ডিউন রেফারেন্সগুলোর খোঁজে সিকিউরিটি ইন্ডাস্ট্রির আবর্জনার স্তূপে আরও গভীরে খুঁড়তে লাগলেন, তখন নতুন আরেকটা উপলব্ধি তাকে সবচেয়ে বেশি ধাক্কা দিল। তারা যে পাওয়ারপয়েন্ট জিরো ডে আবিষ্কার করেছিলেন সেটা তুলনামূলকভাবে নতুন হলেও, হ্যাকারদের এই বিশাল আক্রমণ কর্মসূচির শেকড় কেবল কয়েক মাস নয়, বেশ কয়েক বছর পেছনে ছড়ানো ছিল। ডিউনের সাথে যুক্ত হ্যাকারদের টোপের সবচেয়ে পুরোনো প্রমাণটা পাওয়া গিয়েছিল ২০০৯ সালে। রবিনসন তাদের এই অপারেশনের ছিটেফোঁটা সূত্রগুলো জোড়া লাগানোর আগ পর্যন্ত, তারা পুরো পাঁচ বছর ধরে একদম গোপনে বিভিন্ন প্রতিষ্ঠানের ভেতরে ঢুকে পড়ছিল।

ছয় সপ্তাহের দীর্ঘ বিশ্লেষণের পর, আইসাইট তাদের পাওয়া তথ্যগুলো সবার সামনে তুলে ধরার জন্য তৈরি হলো। তারা এমন একটা বিশাল আর চরম অত্যাধুনিক গুপ্তচরবৃত্তির অভিযান আবিষ্কার করেছিল, যার সবকিছুই বলে দিচ্ছিল এটা ন্যাটো এবং ইউক্রেনকে লক্ষ্য করে চালানো রাশিয়া সরকারের একটা অপারেশন।

রবিনসন যখন হাড়ভাঙা খাটুনি দিয়ে এই অপারেশনের জট খুলছিলেন, তার বস জন হাল্টকুইস্টও রাশিয়ান হ্যাকারদের এই কাজের প্রতি ঠিক ততটাই মগ্ন হয়ে পড়েছিলেন, যতটা মগ্ন ছিলেন এর কোড ঘাঁটাঘাঁটি করা ম্যালওয়্যার অ্যানালিস্টরা। রবিনসনের বসার জায়গাটা ছিল হাল্টকুইস্টের অফিসের সবচেয়ে কাছের বুল পেনে। হাল্টকুইস্ট সেখান থেকেই চিৎকার করে তাকে নানা প্রশ্ন করতেন। টেনেসির টানে তার সেই ভারি কণ্ঠস্বর খুব সহজেই দেয়াল ভেদ করে চলে আসত। অক্টোবরের মাঝামাঝি সময়ে এসে হাল্টকুইস্ট প্রায় প্রতিদিনই বুল পেনে হানা দিতে শুরু

করলেন রবিনসনের কাছ থেকে নতুন আপডেট জানার জন্য। কারণ সেই প্রথম পাওয়ারপয়েন্ট জিরো ডে থেকে শুরু হওয়া রহস্যের জাল ক্রমেই বড় হচ্ছিল।

হ্যাকারদের এতসব চালাকি সত্ত্বেও হাল্টকুইস্ট জানতেন, তাদের এই আবিষ্কারের দিকে মানুষের নজর কাড়তে হলে মিডিয়াকে ঠিকমতো সামলানোর কায়দাকানুন জানতে হবে। সেই সময়ে আমেরিকান মিডিয়া এবং সিকিউরিটি ইন্ডাস্ট্রির চোখে এক নম্বর শত্রু ছিল চীনা সাইবার গুপ্তচররা, রাশিয়ানরা নয়। নরথ্রপ গ্রুম্যান থেকে শুরু করে ডাউ কেমিক্যাল এবং গুগল পর্যন্ত বড় বড় কোম্পানিগুলো চীনা হ্যাকারদের হামলার শিকার হয়েছিল। একের পর এক ভয়ংকর ডেটা চুরির ঘটনা ঘটছিল, যার মূল লক্ষ্য ছিল মেধাভিত্তিক সম্পদ এবং ব্যবসার গোপন তথ্য। তৎকালীন এনএসএ পরিচালক কিথ আলেকজান্ডার এর নাম দিয়েছিলেন ইতিহাসের সবচেয়ে বড় সম্পদ পাচার। এমন একটা পরিস্থিতিতে, পূর্ব ইউরোপের টার্গেট নিয়ে কাজ করা একটা রাশিয়ান গুপ্তচরবৃত্তির অভিযান, তা যতই দীর্ঘস্থায়ী আর ভয়ানক দক্ষতাসম্পন্ন হোক না কেন, অন্য খবরের ডামাডোলে হারিয়ে যাওয়ার একটা বড় ঝুঁকি ছিল।

কিশোর বয়স থেকেই রবিনসন ডিউনের অন্ধ ভক্ত। তিনি পরামর্শ দিলেন এই হ্যাকিং অপারেশনের নাম বেন জেসেরিট রাখা হোক। বইয়ে থাকা একদল রহস্যময় নারীর নাম এটা, যাদের মন নিয়ন্ত্রণের প্রায় জাদুকরী ক্ষমতা ছিল। হাল্টকুইস্ট জীবনেও ফ্র্যাংক হারবার্টের এই বই পড়েননি। নামটা বড্ড খটমটে আর উচ্চারণ করা কঠিন, এই অজুহাতে তিনি সরাসরি প্রস্তাবটা বাতিল করে দিলেন।

এর বদলে হাল্টকুইস্ট বেশ সহজসাধ্য একটা নাম বেছে নিলেন। তিনি এমন একটা নাম চাইলেন যেটা শুনলে মাটির নিচ দিয়ে চলাফেরা করা কোনো গুপ্ত দৈত্যের কথা মনে পড়ে যায়, যা মাঝে মাঝে তার ভয়ংকর রূপ দেখাতে ওপরে উঠে আসে। হাল্টকুইস্ট সেই মুহূর্তে ঘুণাক্ষরেও বুঝতে পারেননি যে নামটা আসলে কতটা খাপে খাপ হতে চলেছে। তিনি দলটির নাম দিলেন স্যান্ডওয়ার্ম।

তাদের হ্যাকারদের জন্য এমন একটা নাম দরকার ছিল, যা মানুষের মনে গেঁথে যায় আর সহজেই নজর কাড়ে। সাইবার সিকিউরিটি ইন্ডাস্ট্রির নিয়ম অনুযায়ী এই হ্যাকার গ্রুপকে আবিষ্কার করার কারণে তাদের নামকরণ করার বিশেষ অধিকারটা আইসাইটের হাতেই ছিল। আর এটা একদম পরিষ্কার ছিল যে নামটার মাঝে সাইবার গুপ্তচরদের ওই ডিউন প্রীতির একটা ছোঁয়া থাকতে হবে।

ফোর্স মাল্টিপ্লায়ার

স্যান্ডওয়ার্ম আবিষ্কারের প্রথম ছয় সপ্তাহ পর আইসাইটের কর্মীরা অফিসে একটা উদ্‌যাপন পার্টির আয়োজন করল। অ্যানালিস্টদের বুল পেনের একদম বারান্দার শেষ মাথায় কোম্পানির একটা বার ছিল, যেখানে পানীয়র কোনো অভাব ছিল না। সবাই সেখানেই জড়ো হলো। বিশ্বমঞ্চে স্যান্ডওয়ার্মের এই আবির্ভাব ঠিক তেমনই সাড়া ফেলেছিল, যেমনটা হাল্টকুইস্ট আশা করেছিলেন। যখন কোম্পানিটি পাঁচ বছর ধরে চলা, জিরো ডে সজ্জিত এবং ডিউন থিমের এই রাশিয়ান গুপ্তচরবৃত্তির খবর সবার সামনে আনল, তখন সেই খবর পুরো ইন্ডাস্ট্রি আর মিডিয়ায় তুমুল ঝড় তুলল। দ্য ওয়াশিংটন পোস্ট, ওয়্যারড এবং অগণিত প্রযুক্তি ও সিকিউরিটি ইন্ডাস্ট্রির ট্রেড পাবলিকেশনগুলোতে এ নিয়ে রীতিমতো খবর ছাপা হতে লাগল। রবিনসনের এখনো মনে পড়ে, তাদের হাতে ধরা পড়া রাশিয়ান হ্যাকারের এই নতুন প্রজাতির সম্মানে এক গ্লাস ভদকা হাতে তিনি হাল্টকুইস্টের সাথে চিয়ার্স করেছিলেন।

অথচ ঠিক সেই সন্ধ্যাতেই, সেখান থেকে আড়াই হাজার মাইল পশ্চিমে আরেকজন সিকিউরিটি গবেষক তখনো মাটি খুঁড়ে যাচ্ছিলেন। জাপানি সিকিউরিটি ফার্ম ট্রেন্ড মাইক্রোর ম্যালওয়্যার অ্যানালিস্ট কাইল উইলহয়েট সেদিন বিকেলে অনলাইনে আইসাইটের স্যান্ডওয়ার্মের রিপোর্টটা দেখতে পান। ক্যালিফোর্নিয়ার কুপারটিনোর একটা হোটেলে কর্পোরেট কনফারেন্সের অন্তহীন সব মিটিংয়ের মাঝখানেই এটা তার চোখে পড়েছিল।

উইলহয়েট আইসাইটকে তাদের সুনামের জন্যই চিনতেন, বিশেষ করে জন হাল্টকুইস্টকে তো খুব ভালো করেই জানতেন। তাই তিনি ঠিক করে রাখলেন যে দিনের শেষে সময় করে এটা নিয়ে একটু ঘাঁটাঘাঁটি করবেন। তার মনে হচ্ছিল, আইসাইটের এই আবিষ্কারের মতো বড় কোনো ঘটনা ঘটলে তার রেশ অনেক দূর পর্যন্ত গড়ায়। কে জানে, এর সূত্র ধরে তার আর ট্রেন্ড মাইক্রোর হাতে নতুন কোনো চমকপ্রদ তথ্য চলেও আসতে পারে।

ওইদিন রাতে হোটেলের বারের বাইরে বসে উইলহয়েট আর ট্রেন্ড মাইক্রোর আরেক গবেষক জিম গোগোলিনস্কি তাদের ল্যাপটপ বের করলেন। আইসাইট সবার জন্য যা যা উন্মুক্ত করেছিল, তার সবকিছু তারা ডাউনলোড করে ফেললেন। এগুলোকে বলা হয় ইন্ডিকেটর অব কমপ্রোমাইজ। স্যান্ডওয়ার্মের হামলার শিকার হতে পারে এমন সম্ভাব্য ভুক্তভোগীদের সাহায্য করার জন্যই এগুলো প্রকাশ করা হয়েছিল, যাতে

তারা হামলাকারীদের আগেভাগেই ধরে ফেলতে পারে আর আটকে দিতে পারে।

অপরাধের জায়গা থেকে প্লাস্টিকের ব্যাগে ভরে আনা আলামতের মতো, এই প্রমাণের টুকরোগুলোর মাঝে কমান্ড-অ্যান্ড-কন্ট্রোল সার্ভারগুলোর আইপি অ্যাড্রেসও ছিল। ব্ল্যাকএনার্জির নমুনাগুলো এই সার্ভারগুলোর সাথেই যোগাযোগ করত। রাত যত গভীর হতে লাগল, বারের ভিড়ও তত কমতে থাকল। উইলহয়েট আর গোগোলিনস্কি তখন ট্রেন্ড মাইক্রোর নিজস্ব ম্যালওয়্যার আর্কাইভ আর ভাইরাসটোটালের ডেটাবেস থেকে ওই আইপি অ্যাড্রেসগুলো মিলিয়ে দেখতে শুরু করলেন। তাদের উদ্দেশ্য ছিল নতুন কোনো মিল পাওয়া যায় কি না সেটা খুঁজে বের করা।

হোটেলের বারটা যখন বন্ধ হয়ে গেল, তখন ওই অন্ধকার চত্বরে কেবল এই দুই গবেষকই বসে ছিলেন। উইলহয়েট ওই আইপি অ্যাড্রেসগুলোর একটার সাথে দারুন একটা মিল পেয়ে গেলেন। সেটা স্যান্ডওয়ার্মের ব্যবহার করা স্টকহোমের একটা সার্ভারের দিকে নির্দেশ করছিল। তিনি যে ফাইলটা পেয়েছিলেন, যার নাম কনফিগ. ব্যাক, সেটাও ওই সুইডিশ মেশিনটার সাথেই যুক্ত ছিল। সিকিউরিটি ইন্ডাস্ট্রির যেকোনো সাধারণ মানুষের কাছে এটাকে একদমই মামুলি একটা জিনিস বলে মনে হতো। কিন্তু উইলহয়েটের চোখ আটকে গেল সেখানেই, তার মগজে যেন বিদ্যুৎ খেলে গেল।

একজন সিকিউরিটি গবেষক হিসেবে উইলহয়েটের অতীতটা একটু অন্যরকম ছিল। মাত্র দুই বছর আগে তিনি সেন্ট লুইসে আমেরিকার সবচেয়ে বড় কয়লা কোম্পানি পিবডি এনার্জির আইটি সিকিউরিটি ম্যানেজারের চাকরি ছেড়ে এসেছিলেন। তাই তিনি ইন্ডাস্ট্রিয়াল কন্ট্রোল সিস্টেমস বা আইসিএস নিয়ে বেশ ভালোভাবেই জানতেন। কিছু কিছু ক্ষেত্রে এগুলোকে সুপারভাইজরি কন্ট্রোল অ্যান্ড ডেটা অ্যাকুইজিশন বা স্কাডা সিস্টেমস নামেও ডাকা হয়। এই সফটওয়্যারটি কেবল তথ্য আদান-প্রদানই করে না, এটি কারখানার বিভিন্ন যন্ত্রপাতির কাছে নির্দেশ পাঠায় এবং তাদের কাছ থেকে ফিডব্যাক নেয়। এটাই হলো সেই জাদুকরী জায়গা, যেখানে ডিজিটাল দুনিয়া আর বাস্তব পৃথিবীর এক অপূর্ব মিলন ঘটে।

পিবডির খনির ভেতর বাতাস চলাচলের ভেন্টিলেটর থেকে শুরু করে কয়লা ধোয়ার বিশাল সব বেসিন, বিদ্যুৎ কেন্দ্রে কয়লা পোড়ানো জেনারেটর, এমনকি গ্রাহকদের কাছে বিদ্যুৎ পৌঁছে দেওয়া সাবস্টেশনের সার্কিট ব্রেকার পর্যন্ত সব জায়গায় আইসিএস সফটওয়্যার ব্যবহার করা হয়। আইসিএস অ্যাপ্লিকেশনগুলো দিয়ে কারখানা, পানির প্ল্যান্ট, তেল আর গ্যাসের শোধনাগার এবং পরিবহন ব্যবস্থা চালানো