ম্যালওয়্যারের জগত

Written By { **rudra_kaiser** }

Resources : ChatGPT, YouTube, CISCO, TechTarget, Wikipedia, IBM

১. ভূমিকা

ম্যালওয়্যারের সংজ্ঞা ও ইতিহাস

ম্যালওয়্যারের সংজ্ঞা অনুসারে, এটি এমন এক ধরনের সফটওয়্যার যা কম্পিউটার, নেটওয়ার্ক বা ডিভাইসে অনধিকার প্রবেশ ও ক্ষতি করার উদ্দেশ্যে তৈরি হয়। "ম্যালওয়্যার" শব্দটি এসেছে "Malicious Software" বা ক্ষতিকারক সফটওয়্যার থেকে, যা সাধারণত ভাইরাস, ওয়ার্ম, ট্রোজান, স্পাইওয়্যার, র‍্যানসমওয়্যার প্রভৃতি আকারে পাওয়া যায়। ম্যালওয়্যারের মাধ্যমে হ্যাকাররা ব্যবহারকারীর অনুমতি ছাড়াই তাদের ডিভাইসে প্রবেশ করতে পারে এবং গোপনীয় তথ্য চুরি, ডেটা নষ্ট বা লক করে রেখে অর্থ দাবি করতে পারে।

ম্যালওয়্যারের জন্ম ও প্রাথমিক ব্যবহার

ম্যালওয়্যারের ইতিহাস বেশ পুরোনো। প্রথম ম্যালওয়্যারটি ছিল **Creeper Virus** নামে পরিচিত, যা ১৯৭১ সালে রে টমলিনসন তৈরি করেছিলেন। এটি মেইনফ্রেম কম্পিউটারে ছড়িয়ে পড়ে এবং মেশিনে "I'm the creeper, catch me if you can!" বার্তা প্রদর্শন করত। এটি অবশ্য ক্ষতিকারক ছিল না; এটি পরীক্ষামূলক একটি প্রোগ্রাম ছিল। তবে, **Elk Cloner** নামে ১৯৮২ সালে প্রথম কম্পিউটার ভাইরাস প্রকাশিত হয়েছিল, যা Macintosh সিস্টেমে আক্রমণ চালাত। এই ভাইরাসটি ছিল প্রথম "বন্য ভাইরাস," যা ব্যক্তিগত কম্পিউটারের মধ্যে ছড়িয়ে পড়ে এবং ব্যবহারকারীদের বিরক্ত করত।

ম্যালওয়্যারের পরিবর্তনশীল রূপ

১৯৮০-এর দশক থেকে ম্যালওয়্যারের প্রকৃতি ও লক্ষ্য পরিবর্তিত হতে শুরু করে। প্রযুক্তির উন্নতির সাথে সাথে ম্যালওয়্যারের আক্রমণও আরও জটিল হতে থাকে। ১৯৯০-এর দশকে ইন্টারনেটের প্রসারের সাথে, ম্যালওয়্যারের ধরণও ব্যাপকভাবে পরিবর্তিত হয়, এবং এর বিস্তারও দ্রুততর হয়ে ওঠে। ইন্টারনেট সংযোগের সহজলভ্যতার কারণে এই সময়ে **ওয়ার্ম** ও **স্পাইওয়্যার** ম্যালওয়্যারের বিভিন্ন রূপ প্রচলিত হয়ে ওঠে।

আজকের দিনে ম্যালওয়্যারের প্রভাব

বর্তমানে ম্যালওয়্যারের প্রভাব গভীর ও ব্যাপক, যা ব্যক্তিগত, কর্পোরেট এবং রাষ্ট্রীয় স্তরে বিপুল ক্ষতির কারণ হতে পারে। **র‍্যানসমওয়্যার** এখন অন্যতম ক্ষতিকর আক্রমণের মাধ্যম, যা ব্যবহারকারীর ফাইল এনক্রিপ্ট করে এবং ডিক্রিপ্ট করার জন্য অর্থ দাবি করে। ২০১৭ সালের **WannaCry** র‍্যানসমওয়্যার আক্রমণ বিশ্বব্যাপী হাজারো কম্পিউটারকে সংক্রমিত করে এবং কোটি কোটি টাকার ক্ষতি ঘটায়।

২. ম্যালওয়ারের ধরণসমূহ

২.১ ভাইরাস

ভাইরাস হলো এক ধরনের ম্যালওয়্যার যা নিজের কোডকে অন্যান্য প্রোগ্রাম বা ফাইলের মধ্যে যুক্ত করে এবং সেই ফাইল বা প্রোগ্রামটি চালানোর সময় সক্রিয় হয়। ভাইরাসকে বাহক প্রোগ্রামের মাধ্যমে চালানো হয় এবং এটি চালানো হলে আরও অন্যান্য ফাইলে বা প্রোগ্রামে সংক্রমিত হয়। এটি ব্যবহারকারীর ফাইল নষ্ট করতে, কম্পিউটারকে ধীর করতে বা অন্যান্য ক্ষতিকর কাজ করতে পারে। যেমন।

I LOVE YOU ভাইরাস : ২০০০ সালে, ফিলিপাইনে তৈরি এই ভাইরাসটি ইমেইলের মাধ্যমে ছড়িয়ে পড়ে এবং বিশ্বের হাজার হাজার কম্পিউটারে সংক্রমণ ঘটায়। এটি ব্যবহারকারীর সমস্ত ফাইল মুছে ফেলে এবং প্রায় ৫ থেকে ১০ বিলিয়ন মার্কিন ডলারের ক্ষতি করে।

সিক্সথম্যান ভাইরাস : এটি সিক্সথম্যান নামে পরিচিত একটি ভাইরাস, যা নির্দিষ্ট ফাইল বা প্রোগ্রামগুলিকে সংক্রমিত করে ব্যবহারকারীর সিস্টেমে ব্যাঘাত ঘটায়।

২.২ ওয়ার্ম

ওয়ার্ম হলো এক ধরনের ম্যালওয়্যার যা নিজে নিজেই এক কম্পিউটার থেকে অন্য কম্পিউটারে ছড়িয়ে পড়ে। এটি নেটওয়ার্ক ব্যবহার করে দ্রুত বিস্তার ঘটাতে সক্ষম এবং সাধারণত ব্যবহারকারীর অনুমতি বা কোনো প্রোগ্রাম চালানোর প্রয়োজন হয় না। ওয়ার্ম ভাইরাসের চেয়ে আরও বিপজ্জনক কারণ এটি দ্রুত একটি নেটওয়ার্কে ছড়িয়ে পড়ে অনেকগুলো ডিভাইসে প্রভাব ফেলতে পারে।

কোড রেড ওয়ার্ম : ২০০১ সালে এই ওয়ার্মটি ইন্টারনেট এক্সপ্লোরারের মাধ্যমে ছড়িয়ে পড়েছিল এবং এর আক্রমণে হাজারো কম্পিউটার সংক্রমিত হয়েছিল। এটি নেটওয়ার্ক সার্ভারে আক্রমণ চালিয়ে তথ্য সংরক্ষণ ব্যবস্থাকে বিপর্যস্ত করেছিল।

Morris Worm : ১৯৮৮ সালে এটি প্রথমবারের মতো ইন্টারনেটে ছড়িয়ে পড়েছিল এবং প্রায় ৬,০০০ কম্পিউটার সংক্রমিত হয়েছিল, যা ইন্টারনেটের একটি বড় অংশকে অচল করে দিয়েছিল।

২.৩ ট্রোজান হর্স

ট্রোজান হর্স হলো এক ধরনের ম্যালওয়্যার যা নির্দোষ ফাইল বা অ্যাপ্লিকেশন হিসেবে ছদ্মবেশ ধারণ করে। এটি প্রায়শই ডাউনলোড করা সফটওয়্যার বা ইমেইল সংযুক্তির মাধ্যমে আসে। ব্যবহারকারী যখন সেই নির্দোষ মনে করা ফাইলটি চালায়, তখন এটি

ক্ষতিকারক কার্যকলাপ শুরু করে। ট্রোজান হর্স সাধারণত তথ্য চুরি, ডিভাইস নিয়ন্ত্রণ করা বা আরও ম্যালওয়্যার ইনস্টল করতে ব্যবহৃত হয়।

Zeus ট্রোজান : এই ট্রোজান ব্যাংকিং তথ্য চুরি করার জন্য বিখ্যাত। এটি ব্যবহারকারীর কীস্ট্রোক ট্র্যাক করতে সক্ষম এবং ব্যবহারকারীর ব্যাংকিং লগইন তথ্য সংগ্রহ করে আক্রমণকারীর কাছে পাঠায়।

Emotet ট্রোজান : এটি একটি ব্যাংকিং ট্রোজান যা ম্যালওয়্যার বিতরণের জন্য ব্যবহৃত হয় এবং ব্যবহারকারীর ব্যাঙ্কের গোপন তথ্য চুরি করে।

২.৪ স্পাইওয়্যার

স্পাইওয়্যার হলো এমন একটি ধরনের ম্যালওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়া তার কম্পিউটার বা ডিভাইস থেকে গোপনে তথ্য সংগ্রহ করে। এটি বিভিন্ন ব্যক্তিগত তথ্য যেমন ব্রাউজিং হিস্ট্রি, লগইন তথ্য, পাসওয়ার্ড এবং আরও অন্যান্য গোপনীয় তথ্য সংগ্রহ করতে পারে এবং আক্রমণকারীর কাছে পাঠিয়ে দেয়। স্পাইওয়্যার সাধারণত ব্যবহারকারীর অজ্ঞাতসারে সিস্টেমে প্রবেশ করে এবং দীর্ঘ সময় ধরে চলতে থাকে।

Keylogger প্রোগ্রাম : একটি জনপ্রিয় স্পাইওয়্যার প্রোগ্রাম হল keylogger, যা ব্যবহারকারীর কীস্ট্রোক বা টাইপিং নজরদারি করে। এটি একটি আক্রমণকারীর জন্য পাসওয়ার্ড, ব্যাংকিং তথ্য, এবং অন্যান্য গুরুত্বপূর্ণ ডেটা সংগ্রহ করে পাঠাতে পারে।

CoolWebSearch : এটি একটি স্পাইওয়্যার যা ইন্টারনেট এক্সপ্লোরারের হোমপেজ পরিবর্তন করে এবং ব্যবহারকারীদের অজান্তে বিভিন্ন সাইটে রিডিরেক্ট করে।

২.৫ র‍্যানসমওয়্যার

র‍্যানসমওয়্যার হল এমন একটি ম্যালওয়্যার যা ব্যবহারকারীর কম্পিউটারের ফাইল বা ডেটা এনক্রিপ্ট করে রাখে এবং ডিক্রিপশন কীগুলির জন্য মুক্তিপণ দাবি করে। র‍্যানসমওয়্যার সাধারণত গুরুত্বপূর্ণ ফাইল বা সিস্টেম ডেটা লক করে রেখে ব্যবহারকারীর কাছে একটি দাবি জানায়, যাতে তারা টাকা প্রদান করলে ফাইলগুলি আবার খোলার জন্য কীগুলি পায়।

WannaCry র‍্যানসমওয়্যার : ২০১৭ সালে WannaCry র‍্যানসমওয়্যার বিশ্বব্যাপী ছড়িয়ে পড়েছিল এবং এটি Windows অপারেটিং সিস্টেমে থাকা কম্পিউটারগুলির ফাইল এনক্রিপ্ট করে ফেলেছিল। হাজারো প্রতিষ্ঠান, হাসপাতাল, এবং সরকারি সেবা এই আক্রমণের শিকার হয়েছিল এবং প্রায় ৪ বিলিয়ন ডলারের ক্ষতি হয়েছে।

NotPetya র‍্যানসমওয়্যার : ২০১৭ সালে এই র‍্যানসমওয়্যারটি ইউক্রেনের গুরুত্বপূর্ণ অবকাঠামোর উপর আক্রমণ চালিয়েছিল, এবং যদিও এটি র‍্যানসমওয়্যার হিসেবে শুরু হয়েছিল, কিন্তু এর উদ্দেশ্য ছিল মূলত সিস্টেম ধ্বংস করা।

২.৬ অ্যাডওয়্যার

অ্যাডওয়্যার হলো এক ধরনের ম্যালওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়া বিজ্ঞাপন প্রদর্শন করে। এটি সাধারণত সফটওয়্যার বা ব্রাউজার এক্সটেনশনের মাধ্যমে সিস্টেমে প্রবেশ করে এবং ব্যবহারকারীর স্ক্রীনে বিভিন্ন ধরনের বিজ্ঞাপন বা পপ-আপ শো করে। যদিও এটি সাধারণত ক্ষতিকর নয়, তবে এটি ব্যবহারকারীর অভিজ্ঞতা ব্যাহত করে এবং সিস্টেমের কর্মক্ষমতা কমিয়ে দেয়।

Adware/Toolbar : কিছু বিনামূল্যের সফটওয়্যার বা ব্রাউজার টুলবারের সাথে অ্যাডওয়্যার ইনস্টল হয়ে থাকে, যা ব্যবহারকারীকে অপ্রত্যাশিত বিজ্ঞাপন দেখায়। এটি বিশেষত পিসি বা মোবাইল ব্রাউজারে বিজ্ঞাপন বা পপ-আপ ফর্মে প্রবাহিত হয়।

২.৭ ব্যাকডোর

ব্যাকডোর ম্যালওয়্যার এমন এক ধরনের সফটওয়্যার যা একটি সিস্টেমে গোপন প্রবেশপথ তৈরি করে আক্রমণকারীকে সিস্টেমে অনুপ্রবেশের অনুমতি দেয়। এটি সাধারণত বৈধ অ্যাপ্লিকেশন বা সিস্টেম সফটওয়্যারের মাধ্যমে সংক্রমিত হয় এবং আক্রমণকারীকে সিস্টেমে দূরবর্তীভাবে প্রবেশ করতে সহায়তা করে। ব্যাকডোরের মাধ্যমে হ্যাকাররা সিস্টেমের পূর্ণ নিয়ন্ত্রণ গ্রহণ করতে পারে এবং বিভিন্ন ধরণের ক্ষতিকারক কার্যকলাপ চালাতে পারে।

Mirai Botnet : Mirai হল একটি ব্যাকডোর যা IoT (Internet of Things) ডিভাইসে ব্যবহৃত হয়েছিল। এটি ব্যবহারকারীদের ডিভাইসগুলোকে সংক্রমিত করে এবং সেগুলিকে একটি বৃহত্তর বটনেটে পরিণত করেছিল, যা DDoS (Distributed Denial of Service) আক্রমণ চালানোর জন্য ব্যবহার করা হয়। এই আক্রমণের ফলে সার্ভার এবং ইন্টারনেট পরিষেবাগুলিতে ব্যাপক ক্ষতি হয়েছিল।

৩. ম্যালওয়ারের আরও বিশেষ প্রকার

৩.১ ফাইল ইনফেক্টর

ফাইল ইনফেক্টর হলো এমন একটি ধরনের ম্যালওয়্যার যা কম্পিউটারের ফাইলগুলোর মধ্যে প্রবেশ করে এবং সেগুলিকে সংক্রমিত করে। এটি সাধারণত এক্সিকিউটেবল ফাইলগুলোর সাথে যুক্ত হয় এবং ফাইলটি চালানো হলে সক্রিয় হয়। ফাইল ইনফেক্টরগুলি মূলত কোডের একটি অংশ যোগ করে ফাইলগুলির আচরণ পরিবর্তন করে এবং নতুন ফাইলগুলিকে সংক্রমিত করার চেষ্টা করে।

Sasser ভাইরাস : এটি একটি ফাইল ইনফেক্টর যা উইন্ডোজ সিস্টেমে প্রবেশ করে এবং এক্সিকিউটেবল ফাইলগুলিকে সংক্রমিত করে। এটি ২০০৪ সালে ব্যাপক ক্ষতি করেছিল এবং হাজার হাজার কম্পিউটারকে সংক্রমিত করে ইন্টারনেটের উপর চাপ সৃষ্টি করেছিল।

৩.২ পলিমরফিক ম্যালওয়্যার

পলিমরফিক ম্যালওয়্যার এমন একটি ধরনের ম্যালওয়্যার যা প্রতিবার নতুন সংস্করণে পরিবর্তিত হয়, ফলে এটি সিস্টেমে সনাক্তকরণ কঠিন করে তোলে। এটি কোড বা বডি পরিবর্তন করে, কিন্তু তার কার্যকারিতা অপরিবর্তিত থাকে। পলিমরফিক ম্যালওয়্যার সাধারণত অ্যান্টিভাইরাস সফটওয়্যারকে এড়িয়ে চলে এবং একই কোড ব্যবহার করতে থাকে, কিন্তু আক্রমণের পদ্ধতি পরিবর্তন করে।

Storm Worm : ২০০৭ সালে এই পলিমরফিক ম্যালওয়্যারটি ইমেইলের মাধ্যমে ছড়িয়ে পড়েছিল এবং প্রতিটি নতুন সংস্করণে এটি নিজেকে পরিবর্তন করেছিল। এটি সিস্টেমে প্রবেশ করে কম্পিউটারগুলোকে বটনেটে পরিণত করেছিল এবং ইন্টারনেটে স্প্যাম মেইল পাঠাতে ব্যবহৃত হয়েছিল।

৩.৩ মেটামরফিক ম্যালওয়্যার

মেটামরফিক ম্যালওয়্যারটি পলিমরফিক ম্যালওয়্যারের মতোই কিন্তু এটি শুধু কোড পরিবর্তন করে না, বরং নিজেকে সম্পূর্ণ নতুনভাবে রচনা করে। এটি নিজের কোডের গঠন পরিবর্তন করে, যাতে কোনও সিগনেচার সনাক্তকরণ যন্ত্র এটিকে চিহ্নিত করতে না পারে। মেটামরফিক ম্যালওয়্যার আরও শক্তিশালী এবং অ্যান্টিভাইরাস সফটওয়্যারকে বিভ্রান্ত করার জন্য তার আচরণ পরিবর্তন করতে সক্ষম।

ZMist ম্যালওয়্যার : এটি একটি মেটামরফিক ম্যালওয়্যার যা কিছু সময় পর পর নিজের কোড রূপান্তরিত করে। এটি ইন্টারনেটে ছড়িয়ে পড়ে এবং বিভিন্ন কোড পরিবর্তন করার মাধ্যমে সিকিউরিটি সফটওয়্যারকে এড়িয়ে চলতে থাকে।

Simda Botnet : এটি একটি মেটামরফিক ম্যালওয়্যার যা কম্পিউটারগুলিকে সংক্রমিত করে এবং একটি বটনেটে পরিণত করে, পাশাপাশি এটি তার কোড রূপান্তরিত করে আক্রমণ চালায়।

৩.৪ ক্রিপ্টোগ্রাফিক র‍্যানসমওয়্যার

ক্রিপ্টোগ্রাফিক র‍্যানসমওয়্যার হলো এমন একটি ধরনের র‍্যানসমওয়্যার যা ব্যবহারকারীর ফাইলগুলি এনক্রিপ্ট করে রাখে এবং তাদের ডিক্রিপ্ট করার জন্য একটি বিশাল পরিমাণ টাকা দাবি করে। এটি সাধারণত শক্তিশালী ক্রিপ্টোগ্রাফিক অ্যালগরিদম ব্যবহার করে, যার ফলে ডেটা পুনরুদ্ধার করা অনেক কঠিন হয়। এটি আর্থিক লাভের জন্য ব্যবহারকারীর গুরুত্বপূর্ণ ডেটা দখল করে রাখে এবং অর্থ না দিলে ডেটা উদ্ধার করতে দেয় না।

CryptoLocker : এটি একটি জনপ্রিয় ক্রিপ্টোগ্রাফিক র‍্যানসমওয়্যার যা ২০১৩ সালে ছড়িয়ে পড়েছিল। এটি ব্যবহারকারীর কম্পিউটারের ফাইলগুলি এনক্রিপ্ট করে এবং এর জন্য মুক্তিপণ দাবি করে। এর পরবর্তী সংস্করণগুলোও অন্যান্য র‍্যানসমওয়্যার আক্রমণের মতোই অন্যান্য কম্পিউটারগুলিতে ছড়িয়ে পড়ে।

TeslaCrypt : এই ক্রিপ্টোগ্রাফিক র‍্যানসমওয়্যারটি গেমারদের লক্ষ্য করে তাদের গেম ফাইল এনক্রিপ্ট করেছিল এবং মুক্তিপণ হিসেবে Bitcoins দাবি করেছিল।

৪. বাস্তব ঘটনা ও উদাহরণ

ম্যালওয়ারের আক্রমণগুলি সব সময়ই প্রযুক্তি এবং সাইবার নিরাপত্তার ক্ষেত্রে একটি বড় চ্যালেঞ্জ তৈরি করে। বিভিন্ন ম্যালওয়্যার আক্রমণ, বিশেষ করে বৃহৎ আক্রমণগুলি, বিভিন্ন প্রতিষ্ঠানের জন্য বিপদ ডেকে আনতে পারে এবং অনেক সময় সামগ্রিকভাবে অর্থনৈতিক ক্ষতি বা প্রযুক্তিগত বিপর্যয় সৃষ্টি করে। এই বিভাগে আমরা কিছু পরিচিত এবং বড় ম্যালওয়্যার আক্রমণের ঘটনা আলোচনা করব।

৪.১ Stuxnet

Stuxnet একটি অত্যন্ত জটিল এবং সুনির্দিষ্টভাবে ডিজাইন করা ম্যালওয়্যার ছিল, যা বিশেষভাবে ইরানের নাতাঞ্জ নিউক্লিয়ার ফ্যাসিলিটি লক্ষ্য করে তৈরি করা হয়েছিল। এটি একটি টার্গেটেড ম্যালওয়্যার, যা একটি বিশেষ শিল্পকৌশল সিস্টেমে, বিশেষত SCADA (Supervisory Control and Data Acquisition) সিস্টেমে প্রবেশ করেছিল। Stuxnet ম্যালওয়্যারটি সেন্ট্রিফিউজ মেশিনগুলোকে ক্ষতিগ্রস্ত করার জন্য ডিজাইন করা হয়েছিল, যা ইরানের ইউরেনিয়াম সমৃদ্ধকরণ প্রক্রিয়াতে ব্যবহৃত হতো।

Stuxnet একটি বহুমুখী ম্যালওয়্যার যা কম্পিউটার সিস্টেমে প্রবেশ করে এবং একটি বিশেষ কমান্ড দিয়েছিল, যার ফলে সেন্ট্রিফিউজ মেশিনগুলো দ্রুত ঘুরতে শুরু করেছিল এবং তারপর ধ্বংস হয়ে গিয়েছিল। এটি শুধুমাত্র একটি দেশের লক্ষ্যেই ছিল না, এটি বিশ্বের নিরাপত্তা গবেষক এবং প্রযুক্তি বিশ্লেষকদের জন্য একটি নতুন যুগের সূচনা ছিল, যেখানে সাইবার আক্রমণগুলি শারীরিক অবকাঠামোকে লক্ষ্য করতে সক্ষম হয়েছে।

২০১০ সালে Stuxnet প্রথম সনাক্ত হয় এবং তখন থেকেই এটি সাইবার নিরাপত্তার ক্ষেত্রে একটি বড় আলোচনার বিষয় হয়ে ওঠে। এটি প্রমাণ করেছে যে সাইবার আক্রমণগুলি কেবল সফটওয়্যার বা তথ্যের ক্ষতি করার জন্য নয়, বরং শারীরিক উপকরণকে লক্ষ্য করে তা ধ্বংস করতে পারে।

৪.২ WannaCry

WannaCry ছিল একটি বিশাল র‍্যানসমওয়্যার আক্রমণ, যা ২০১৭ সালের মে মাসে ব্যাপকভাবে ছড়িয়ে পড়েছিল। এটি মূলত একটি ম্যালওয়্যার ছিল যা Windows অপারেটিং সিস্টেমের একটি দুর্বলতা ব্যবহার করে নিজেকে ছড়িয়ে পড়ে এবং ব্যবহারকারীর কম্পিউটার বা ডিভাইসের ফাইল এনক্রিপ্ট করে। এরপর এটি মুক্তিপণ দাবি করে, যাতে ব্যবহারকারী তার ফাইলগুলিকে পুনরুদ্ধার করতে পারে।

WannaCry তার সিস্টেমে প্রবেশ করার পর, ফাইলগুলি এনক্রিপ্ট করে এবং একটি র‍্যানসমওয়্যার পেমেন্ট ডেমান্ড প্রদর্শন করে। এটি একটি 'Cryptolocker' ধরনের আক্রমণ ছিল এবং মূলত রুশ বা চীনা হ্যাকারদের দ্বারা পরিচালিত হয় বলে মনে করা হয়।

WannaCry আক্রমণটি সারা পৃথিবীজুড়ে লক্ষ লক্ষ কম্পিউটার সিস্টেমকে সংক্রমিত করেছিল, যার মধ্যে যুক্তরাজ্যের NHS (National Health Service) সহ অনেক গুরুত্বপূর্ণ প্রতিষ্ঠান ছিল। এটি ইন্টারনেটের মাধ্যমে দ্রুত ছড়িয়ে পড়েছিল এবং বিভিন্ন দেশের সাইবার নিরাপত্তা বিশেষজ্ঞরা এর প্রতিরোধে তৎপর হয়েছিল। এর ক্ষতির পরিমাণ প্রায় ৪ বিলিয়ন ডলারেরও বেশি বলে অনুমান করা হয়।

৪.৩ NotPetya

NotPetya ছিল আরেকটি ধ্বংসাত্মক র‍্যানসমওয়্যার আক্রমণ, যা ২০১৭ সালের জুন মাসে ইউক্রেনে শুরু হয়েছিল। এটি মূলত র‍্যানসমওয়্যার আক্রমণ হিসেবে পরিচিত হলেও, এর মূল উদ্দেশ্য ছিল সিস্টেম ধ্বংস করা, মুক্তিপণ আদায় করা নয়। NotPetya ব্যবহারকারীর ফাইল এনক্রিপ্ট করেছিল এবং আক্রমণকারীরা মুক্তিপণ দাবি করলেও এটি আসলে কোন ফাইলের ডিক্রিপশন কী প্রদান করত না।

NotPetya প্রথমে ইউক্রেনের একটি সফটওয়্যার কোম্পানির মাধ্যমে ছড়িয়েছিল এবং পরে এটি সারা বিশ্বে ছড়িয়ে পড়ে। এটি এমনভাবে ডিজাইন করা হয়েছিল যাতে সিস্টেম থেকে গুরুত্বপূর্ণ ডেটা এবং ফাইল ধ্বংস হয়ে যায়। এই আক্রমণের ফলে বিশ্বের বিভিন্ন বড় প্রতিষ্ঠানে ব্যাপক ক্ষতি হয়েছিল।

NotPetya আক্রমণটি মূলত ইউক্রেনের অবকাঠামো এবং বড় বড় প্রতিষ্ঠানগুলিতে আক্রমণ চালিয়েছিল, যেমন Maersk, FedEx এবং অন্যান্য বহুজাতিক কোম্পানি। NotPetya এর মাধ্যমে প্রায় ১০ বিলিয়ন ডলারের ক্ষতি হয়েছিল।

৪.৪ CryptoLocker

CryptoLocker ছিল একটি র‍্যানসমওয়্যার ভাইরাস যা ২০১৩ সালে সারা বিশ্বে ছড়িয়ে পড়েছিল। এটি ফাইল এনক্রিপ্ট করত এবং মুক্তিপণ হিসেবে Bitcoins দাবি করত। CryptoLocker আক্রমণের সময়, ব্যবহারকারীর ফাইলগুলি এনক্রিপ্ট হয়ে যেত এবং ব্যবহারকারীর কাছে মুক্তিপণের জন্য একটি বিজ্ঞপ্তি পাঠানো হত।

CryptoLocker আক্রমণটি সাধারণত ইমেইল আক্রমণের মাধ্যমে ছড়িয়ে পড়ত, যেখানে একটি সংযুক্ত ফাইল বা লিংক ব্যবহারকারীকে প্রতারণা করে সিস্টেমে প্রবেশ করত। এটি বিশ্বের বিভিন্ন বড় প্রতিষ্ঠান এবং ব্যক্তিগত ব্যবহারকারীদের লক্ষ্য করেছিল।

CryptoLocker আক্রমণটি অনেক বড় কর্পোরেট প্রতিষ্ঠান এবং ব্যাংকিং সেক্টরের জন্য বিপদের কারণ হয়ে দাঁড়িয়েছিল। এটি এমনভাবে ডিজাইন করা হয়েছিল যে পেমেন্ট না করা হলে ফাইলগুলি স্থায়ীভাবে হারিয়ে যেত।

৫. প্রতিরোধ ও সুরক্ষা ব্যবস্থা

ম্যালওয়ারের আক্রমণ প্রতিরোধ করতে সঠিক নিরাপত্তা ব্যবস্থা গ্রহণ করা অত্যন্ত গুরুত্বপূর্ণ। সিস্টেম, ডেটা এবং ব্যবহারকারীর ব্যক্তিগত তথ্য সুরক্ষিত রাখতে বিভিন্ন নিরাপত্তা ব্যবস্থা এবং সতর্কতা অবলম্বন করা উচিত। এই অধ্যায়ে আমরা ম্যালওয়ারের আক্রমণ থেকে প্রতিরোধ করার জন্য কিছু গুরুত্বপূর্ণ নিরাপত্তা পরামর্শ এবং পদ্ধতি আলোচনা করব।

৫.১ সাধারণ নিরাপত্তা পরামর্শ

ফায়ারওয়াল ব্যবহার : ফায়ারওয়াল হলো একটি নিরাপত্তা সিস্টেম যা আপনার কম্পিউটার এবং নেটওয়ার্কের মধ্যে একটি বাধা হিসেবে কাজ করে, যাতে অননুমোদিত ব্যবহারকারীরা আপনার সিস্টেমে প্রবেশ করতে না পারে। এটি ইনবাউন্ড এবং আউটবাউন্ড ট্র্যাফিক নিয়ন্ত্রণ করতে সাহায্য করে। ব্যক্তিগত কম্পিউটারের জন্য ফায়ারওয়াল ব্যবহার করা অত্যন্ত গুরুত্বপূর্ণ, কারণ এটি অনলাইনে হ্যাকিং প্রচেষ্টা এবং ম্যালওয়ারের আক্রমণ প্রতিরোধ করতে সাহায্য করে।

অ্যান্টি-ম্যালওয়্যার সফটওয়্যার ইনস্টল রাখা : আপনার কম্পিউটারে একটি শক্তিশালী অ্যান্টি-ম্যালওয়্যার সফটওয়্যার ইনস্টল রাখা অপরিহার্য। এই সফটওয়্যারটি ম্যালওয়্যার স্ক্যান এবং দূষিত ফাইল শনাক্ত করতে সাহায্য করে। এটি নতুন ধরনের ম্যালওয়্যার থেকেও সুরক্ষা প্রদান করতে সক্ষম, যদি আপনি সফটওয়্যারটি নিয়মিতভাবে আপডেট করেন। জনপ্রিয় অ্যান্টি-ম্যালওয়্যার সফটওয়্যারগুলোর মধ্যে Norton, McAfee, Bitdefender, Kaspersky ইত্যাদি রয়েছে।

নিয়মিত আপডেট : আপনার কম্পিউটার এবং সফটওয়্যারগুলোর নিয়মিত আপডেট রাখা অত্যন্ত গুরুত্বপূর্ণ। বেশিরভাগ ম্যালওয়্যার আক্রমণ সফল হয় যখন সিস্টেমে পুরনো বা দুর্বল নিরাপত্তা প্যাচ থাকে। সফটওয়্যার আপডেটের মাধ্যমে নিরাপত্তা ফিচারগুলিও উন্নত হয়, যা ম্যালওয়্যার আক্রমণ থেকে সিস্টেমকে সুরক্ষিত রাখে।

৫.২ সিস্টেম ব্যাকআপ

ব্যাকআপের গুরুত্ব : ম্যালওয়ারের আক্রমণ যেমন র‍্যানসমওয়্যার সিস্টেমের ডেটা এনক্রিপ্ট করতে পারে এবং মুক্তিপণের জন্য দাবি করতে পারে। তাই গুরুত্বপূর্ণ ডেটা হারানোর ঝুঁকি কমাতে, নিয়মিত ব্যাকআপ রাখা অত্যন্ত গুরুত্বপূর্ণ। সিস্টেমের ব্যাকআপ রাখতে হলে আপনি আপনার গুরুত্বপূর্ণ ফাইলগুলি ক্লাউড বা বাহ্যিক ড্রাইভে রাখতে পারেন, যাতে ম্যালওয়ারের আক্রমণ বা সিস্টেম ক্র্যাশের পর আপনি আপনার তথ্য পুনরুদ্ধার করতে পারেন।

ব্যাকআপ পদ্ধতি : ব্যাকআপ করার জন্য বিভিন্ন পদ্ধতি রয়েছে:

- **ক্লাউড ব্যাকআপ** : Google Drive, Dropbox, OneDrive ইত্যাদি ক্লাউড স্টোরেজ সেবা ব্যবহার করে আপনার ফাইল ব্যাকআপ করা। এটি সহজে অ্যাক্সেসযোগ্য এবং নির্ভরযোগ্য।
- **এক্সটার্নাল হার্ড ড্রাইভ** : বাহ্যিক হার্ড ড্রাইভে বা SSD তে আপনার ডেটা স্থানান্তর করা। এটি অনলাইনে না থাকার কারণে সুরক্ষিত থাকে।
- **অটো ব্যাকআপ সিস্টেম** : এমন সফটওয়্যার ব্যবহার করুন যা আপনার ফাইলগুলোর অটো ব্যাকআপ তৈরি করে।

৫.৩ সতর্ক ইন্টারনেট ব্রাউজিং

ফিশিং লিঙ্ক এড়ানো : ফিশিং আক্রমণগুলি সাধারণত ইমেইল, সোশ্যাল মিডিয়া বা সন্দেহজনক লিঙ্কের মাধ্যমে ঘটে, যেখানে ব্যবহারকারীকে একটি প্রতারণামূলক ওয়েবসাইটে নিয়ে যাওয়া হয় এবং তাদের ব্যক্তিগত তথ্য চুরি করা হয়। এই ধরনের আক্রমণ থেকে রক্ষা পাওয়ার জন্য, কখনোই সন্দেহজনক ইমেইল বা লিঙ্কে ক্লিক করবেন না, এবং শুধুমাত্র বিশ্বস্ত ওয়েবসাইট থেকে সফটওয়্যার ডাউনলোড করুন।

সন্দেহজনক ইমেইল এড়ানো : অনেক সময় ম্যালওয়্যার ইমেইল অ্যাটাচমেন্টের মাধ্যমে ছড়িয়ে পড়ে। আপনি যদি কোনো অজানা বা সন্দেহজনক প্রেরকের কাছ থেকে ইমেইল পান, তবে সেই ইমেইল খোলার আগে সতর্ক থাকুন। কখনোই অজানা অ্যাটাচমেন্ট ডাউনলোড বা ওপেন করবেন না, এবং ইমেইল থেকে কোনো লিঙ্কে ক্লিক না করার চেষ্টা করুন।

অনিরাপদ ওয়েবসাইট এড়ানো : সব ওয়েবসাইট নিরাপদ নয়। এমন কিছু ওয়েবসাইট রয়েছে যেগুলো হ্যাকাররা তৈরি করে থাকে, যাতে ব্যবহারকারীর সিস্টেমে ম্যালওয়্যার প্রবেশ করানো যায়। যখন আপনি ইন্টারনেট ব্রাউজ করেন, তখন চেষ্টা করুন শুধু নিরাপদ, HTTPS প্রোটোকল ব্যবহৃত সাইটগুলোতে প্রবেশ করতে। এছাড়া, ব্রাউজারের নিরাপত্তা সেটিংস বাড়ানোর মাধ্যমে অনিরাপদ সাইটগুলো থেকে সুরক্ষা নিতে পারেন।

৫.৪ অন্যান্য পরামর্শ

পাসওয়ার্ড ব্যবস্থাপনা : শক্তিশালী পাসওয়ার্ড ব্যবহার করুন এবং একাধিক সাইটে একই পাসওয়ার্ড ব্যবহার করবেন না। পাসওয়ার্ড ম্যানেজার ব্যবহার করে আপনি সহজেই শক্তিশালী পাসওয়ার্ড তৈরি করতে পারেন এবং সেগুলি নিরাপদে রাখতে পারেন।

অথেনটিকেশন (Two-Factor Authentication) : আপনার গুরুত্বপূর্ণ অ্যাকাউন্টগুলোর জন্য দুই-ফ্যাক্টর অথেনটিকেশন (2FA) চালু করুন। এটি আপনার অ্যাকাউন্টে অননুমোদিত প্রবেশের ঝুঁকি কমিয়ে দেয়।

নিরাপত্তা সচেতনতা প্রশিক্ষণ : প্রতিষ্ঠানে কর্মরত কর্মচারীদের ম্যালওয়্যার এবং অন্যান্য সাইবার আক্রমণ সম্পর্কে সচেতন করা উচিত। সঠিক প্রশিক্ষণ দিয়ে ব্যবহারকারীদের নিরাপত্তা মানসিকতা তৈরি করা যেতে পারে, যাতে তারা সাইবার আক্রমণের ঝুঁকি থেকে রক্ষা পায়।

এই পরামর্শগুলো অনুসরণ করলে আপনি আপনার সিস্টেম, ডেটা এবং ব্যক্তিগত তথ্যকে ম্যালওয়ারের আক্রমণ থেকে সুরক্ষিত রাখতে পারেন। প্রযুক্তির উন্নতির সাথে সাথে ম্যালওয়ারের ধরণও পরিবর্তিত হচ্ছে, তাই সাইবার নিরাপত্তার উপরে সতর্ক থাকা এবং সর্বদা সর্বশেষ নিরাপত্তা ব্যবস্থা গ্রহণ করা জরুরি।