কমপিউটার সিকিউরিটি ডিকশনারি

পরিবারে ব্যবহার হওয়া হোম কমপিউটার থেকে শুরু করে দেশের বৃহত্তম করপোরেশনের ডেস্কটপ কমপিউটার পর্যন্ত সব কমপিউটারই বর্তমানে নিরাপত্তাসংশ্লিষ্ট ঝুঁকিতে রয়েছে। এই ঝুঁকির মাত্রা দিন দিন এমনভাবে বেড়েছে যে প্রযুক্তিবিশ্বে এখন সবচেয়ে আলোচিত বিষয় হয়ে উঠেছে কমপিউটার সিকিউরিটি তথা নিরাপত্তা। এর ফলে আমরা প্রায় সময় সিকিউরিটিসংশ্লিষ্ট কিছু কিছু সাধারণ টার্মের মুখোমুখি হই যেগুলো সম্পর্কে ন্যূনতম ধারণা বেশিরভাগ ব্যবহারকারীই নেই। এ সত্য উপলব্ধিতে *কমপিউটার জগৎ*-এর নিয়মিত বিভাগ পাঠশালায় এবার উপস্থাপন করা হয়েছে কমপিউটারের নিরাপত্তাসংশ্লিষ্ট বিষয়ের ওপর বহুল পরিচিত বেশ কিছু টার্মের ব্যাখ্যা, যা ইংরেজি বর্ণ অনুসারে ধরা হয়েছে।

অ্যাডওয়্যার

অ্যাডওয়্যার প্রোগ্রাম হলো সেগুলো যেগুলো ব্যবহারের সময় বিজ্ঞাপনের কনটেন্ট ডাউনলোড ও ডিসপ্লে করে। বাস্তবতা হলো, অ্যাডগুলো নিজেরাই বিরক্তিকর, কিন্তু মূল বিপদ হলো অ্যাডওয়্যারগুলো বিরক্তিকর পপ-আপ গ্রাফিক্স এবং অডিও ডাউনলোড করা ছাড়া এরচেয়ে বেশি কিছু ডাউনলোড করে। হতে পারে এই অ্যাডওয়্যারগুলো ইচ্ছাকৃতভাবে বা অন্যের ক্ষতি করে নিজের স্বার্থ হাসিলের উদ্দেশ্যে আপনার কমপিউটারে ডাউনলোড করতে পারে ম্যালওয়্যার।

অ্যানোনিমাস

ইদানীং নেটওয়ার্ক হ্যাকাররা ইন্টারনেটে সবচেয়ে নিরাপদ নেটওয়ার্কে অ্যাক্সেস করতে সক্ষম হচ্ছে। এসব নেতাবিহীন এবং ছদ্মবেশী গ্রুপ প্রযুক্তিবিশ্বে অ্যানোনিমাস হিসেবে পরিচিত। সবচেয়ে পরিচিত অ্যানোনিমাস গ্রুপ কার্যকর করছে কমপিউটারভিত্তিক আইনবহির্ভূত আন্দোলন। এদের অনেকের অ্যাকশন হ্যাকিং হিসেবে ক্যারেক্টারাইজড অথবা এজেন্সির ওয়েবসাইট প্রতিষ্ঠানে ক্র্যাক হিসেবে প্রতিষ্ঠিত।

অটোরান

যখন আপনার কমপিউটারের সিডি বা ডিভিডি ড্রাইভে সিডি বা ডিভিডি ঢোকানো হবে, তখন অপারেটিং সিস্টেম ডিস্ক স্পিন করবে এবং সরাসরি কোড রিড করবে। অটোরানের উদ্দেশ্য খুবই খারাপ। এটি ডিস্কে রেখে দিতে পারে বিদ্বেষপরায়ণ কোড, যা আপনার কমপিউটারকে সংক্রমিত করতে পারে আপনাকে প্রতিরোধের কোনো সুযোগ না দিয়ে। অটোরান ফিচারকে ডিজ্যাবল করে এ ধরনের হামলা থেকে সিস্টেমকে রক্ষা করতে পারবেন।

বোটনেট

বোটনেট হলো ইন্টারনেট সংযোগসহ কিছু কম্প্রোমাইজ কমপিউটারের সংগ্রহ, যেগুলো নিয়ন্ত্রিত হয় অনাকাঙ্ক্ষিত থার্ড পার্টির মাধ্যমে। এর ফলে ভেঙে পড়ে নিরাপত্তা বেষ্টনী এবং সমশ্রেণীভুক্ত কিছু অ্যাকশন কার্যকর করার জন্য ব্যবহার হয়। সাধারণত এগুলো হলো DDoS গঠনের হামলা। এখানে পাসওয়ার্ড ক্র্যাক করার জন্য ব্যবহার হয় সম্মিলিত কমপিউটিং পাওয়ার অথবা কার্যকর করে অন্য ধরনের টাস্ক। যেসব সিস্টেম বোটনেটকে অন্তর্ভুক্ত করে সেগুলোকে সাধারণত রেফার করা হয় জুমবাই (Zombie) কমপিউটার হিসেবে। কেননা এগুলো নির্বোধের মতো কাজ করে।

কার্নিভোর

কার্নিভোর হলো এমন সিস্টেম, যা ফেডারেল ব্যুরো অব ইনভেস্টিগেশন তথা এফবিআই ই-মেইল এবং ইলেকট্রনিক কমিউনিকেশন মনিটর করার জন্য ডিজাইন করে। এতে ব্যবহার হয় কাস্টোমাইজেবল স্লিফার প্যাকেট, যা টার্গেট ইউজারের সব ইন্টারনেট ট্রাফিক মনিটর করতে পারে। কার্নিভোর বাস্তবায়ন করা হয় ১৯৯৭ এবং ব্যাপকভাবে সমালোচিত হওয়ায় তা প্রতিস্থাপিত হয় আরো উন্নত বাণিজ্যিক সফটওয়্যার দিয়ে। এটি মাইক্রোসফট উইন্ডোজভিত্তিক ওয়ার্ক স্টেশন। এতে সমন্বিত রয়েছে এক প্যাকেট স্লিফারিং সফটওয়্যার এবং রিমোভাল ডিস্ক ড্রাইভ।

সার্টিফিকেট

সার্টিফিকেট ডিজিটাল সার্টিফিকেট হিসেবে পরিচিত। এই টার্মটি সাধারণত ই-কমার্সে ব্যবহার হয়। ডিজিটাল সার্টিফিকেট হলো সেটি, যা আপনার ওয়েব ব্রাউজারে ওয়েবসাইটের আইডেন্টিটি। সার্টিফিকেট সংশ্লিষ্ট তথ্য ব্যবহার হয় এনক্রিপটেড সেশন সেটআপ করার জন্য, যাতে কেউ ওই তথ্য দেখতে না পারে, যা আপনার এবং সিকিউর সাইটের মধ্যে দেয়া-নেয়া হয়।

কম্প্রোমাইজ

কমপিউটারের নিরাপত্তাসংশ্লিষ্ট বিষয়ে কম্প্রোমাইজ টার্মটি ব্যবহার করা হয় কমপিউটারের ওপর নিয়ন্ত্রণহীনতা ও বিশুদ্ধতা বোঝাতে, কোনো সম্মতিতে উপনীত না হওয়া। বিশেষ করে কম্প্রোমাইজ বলতে বোঝানো হচ্ছে কমপিউটারে বা নেটওয়ার্কের নিরাপত্তার এক ত্রুটি বা হোল। কম্প্রোমাইজ কমপিউটার অনেকটা গর্তযুক্ত এক সাবমেরিনের মতো। এই সিকিউরিটি হোল হতে পারে দুর্ঘটনাক্রমে অথবা ক্ষতিকর বা ম্যালিশাস সফটওয়্যার আপনার কমপিউটারে অ্যাক্সেস করে এগুলো তৈরি করেছে। যেভাবেই হোক না কেনো, কম্প্রোমাইজ কমপিউটার হলো ব্যবহারকারীর জন্য দুঃসংবাদ।

ক্র্যাকার

ক্র্যাকার বলতে বোঝায় বিদ্বেষপরায়ণ ব্যক্তি, যারা নিরাপদ কমপিউটার সিস্টেমকে ভেঙে ফেলে বা ভাঙতে চেষ্টা করে। এদের ইচ্ছা থাকে গুরুত্বপূর্ণ তথ্য হাতিয়ে নেয়া অথবা তথ্যের ক্ষতিসাধন কিংবা সিস্টেমকে ডিজ্যাবল করা।

ডিডিওএস

ডিডিওএসের পূর্ণ রূপ হলো ডিস্ট্রিবিউটেড ডিনায়েল অব সার্ভিস। এটি এক ধরনের ডিনায়েল অব সার্ভিস তথা ডস (DoS) অ্যাটাক, যেখানে মাল্টিপল কম্প্রোমাইজ সিস্টেম সাধারণত ট্রোজানে আক্রান্ত। এই ট্রোজান একটি সিঙ্গেল সিস্টেমকে টার্গেট করে ডিনায়েল অব সার্ভিস আক্রমণের কারণ হয়ে দাঁড়ায়। ডিস্ট্রিবিউটেড ডিনায়েল অব সার্ভিস অ্যাটাকে টার্গেট সিস্টেম অতিরিক্ত এক্সটারনাল ট্রাফিক দিয়ে প্লাবিত করে ফেলে, যা সিস্টেম হ্যান্ডেল করতে পারে। এর ফলে সিস্টেম নিশ্চল হয়ে পড়ে।

এনক্রিপশন

এনক্রিপশন হলো তথ্য মেসেজ এনকোডিংয়ের এমন এক প্রসেস, যা হ্যাকাররা রিড করতে বা বুঝতে পারে না, তবে বৈধ ব্যবহারকারীরা পড়তে ও বুঝতে পারেন। মূলত এনক্রিপশন ডাটাকে সাইবার টেক্সট ফরমেটে রূপান্তর করে। ফলে অনাকাঙ্ক্ষিত বা অবৈধ ব্যবহারকারীর বুঝতে পারে না অবৈধ কেউ এনক্রিপট করা ডাটা ভিউ করার জন্য ওপেন করে তাহলে তিনি কনটেন্টগুলো দেখতে পারবেন দুর্বোধ্যভাবে। ডাটা যত দৃঢ়ভাবে এনক্রিপট হবে, তা পাঠোদ্ধার করতে হ্যাকারদের তত বেশি বেগ পেতে হবে।

এক্সপ্লয়েট

অন্য কোনো প্রোগ্রামের কোডের লুপহোল কাজে লাগিয়ে সুবিধা আদায় করে নেয়াকে সফটওয়্যারে এক্সপ্লয়েট বলা হয়। একজন হামলাকারী এই লুপহোলকে কাজে লাগিয়ে কমপিউটার বা নেটওয়ার্কে অ্যাক্সেস করতে পারবে। এক্সপ্লয়েন্ট হলো এমন এক বিষয়, যা মারাত্মক এক কম্প্রোমাইজ।

ফায়ারওয়াল

ফায়ারওয়াল হলো হার্ডওয়্যার বা সফটওয়্যার সলিউশন সিকিউরিটি পলিশি প্রয়োগ করার জন্য। ফিজিক্যাল সিকিউরিটি অ্যানালজিতে ফায়ারওয়াল হলো বাড়ির প্রধান ফটকের তালার মতো অথবা বাড়ির ভেতরের কোনো কক্ষের তালার মতো, যা শুধু বৈধ ব্যবহারকারীরা চাবি বা অ্যাক্সেস কার্ড ব্যবহার করে ঢুকতে পারবেন। ফায়ারওয়ালে থাকে বিল্টইন ফিল্টার, যা অবৈধ বা সম্ভাব্য ক্ষতিকর উপাদানকে সিস্টেমে ঢুকতে বাধা দেয়।

হ্যাকার

যেকোনো দক্ষ কমপিউটার অপারেটর বা ▸

প্রোগ্রামারের জন্য নিরপেক্ষ টার্ম হলো হ্যাকার। দুর্ভাগ্যজনকভাবে এই টার্মের ব্যাখ্যা খারাপ অর্থে বেশি ব্যবহার হচ্ছে সব মহলে, কেননা বেশিরভাগ ক্ষেত্রে মিডিয়া হ্যাকার টার্মটি ব্যবহার করে যেখানে ক্র্যাকার টার্মটি বেশি উপযোগী।

হাইজ্যাক

বিমান হাইজ্যাকারেরা যেভাবে বিমানের নিয়ন্ত্রণ দখল করে তাদের ইচ্ছেমতো গন্তব্যের দিকে বিমানকে নিয়ে যায়, অনুরূপভাবে ব্রাউজার হাইজ্যাকের ওয়েব ব্রাউজারকে ভুল পথে নিয়ে যায় একটি ভিন্ন সাইট বা ওয়েব পেজে, যেখানে ভিজিট করার ইচ্ছে ব্যবহারকারীর নেই। হতে পারে এর মাধ্যমে পেজ ভিউ বাড়িয়ে সাইটের স্বত্বাধিকারী প্রচুর বিজ্ঞাপনী রেভিনিউ অর্জন করতে পারে, চেষ্টা করে ম্যালওয়্যার ইনস্টল করতে কিংবা কৌশলে ডিজিটরের ইউজারনেস ও পাসওয়ার্ড এন্টার করতে প্ররোচিত করে। এ সবকিছুই খারাপ।

এইচটিটিপিএস

এইচটিটিপিএসের নিরাপদ গঠন হলো হাইপারটেক্সট ট্রান্সফার প্রটোকল। এই স্ট্রাকচার হলো পুরো ওয়েবের ভিত্তি। যখন https:// লিঙ্ক ব্যবহার করে একটি সাইটে কানেক্ট হবেন, তখন আপনার ব্রাউজার এবং সাইটের সার্ভার সব তথ্য এনক্রিপ্ট করার জন্য সহযোগী হিসেবে কাজ করবে। যখন অনলাইন শপিং করবেন, যেকোনো ধরনের ফিন্যান্সিয়াল ম্যানেজমেন্ট (যেমন আপনার ব্যাংক এবং ক্রেডিট ইউনিয়ন) কার্যকর করবেন এবং ওয়েবমেইল সার্ভিসে অ্যাক্সেস করবেন, তখন নিশ্চিত হয়ে নিন যে সাইট অ্যাড্রেস যেনো http://-এর পরিবর্তে https:// দিয়ে শুরু হয় এবং আপনার গুরুত্বপূর্ণ তথ্য যেনো প্রোটেকটেড থাকে।

ইনফরমেশন সিকিউরিটি

ইনফরমেশন সিকিউরিটি টার্মটি ইনফোসেক হিসেবে পরিচিত। এই প্রফেশনাল ডিল তথা কাজটি সরাসরি কমপিউটার সিকিউরিটিসংশ্লিষ্ট। ইনফরমেশন সিকিউরিটি প্রফেশনাল প্রোগ্রাম লেখা থেকে শুরু করে সবকিছু স্ক্যান করে যাতে নোংরা বা অবাঞ্ছিত উপাদান থেকে রক্ষা পায়, যেমন অ্যান্টিভাইরাস প্রোগ্রাম। এজন্য নেটওয়ার্ক ট্রাফিকের প্রতি লক্ষ রাখতে হবে যাতে সন্দেহজনক তথ্যের ধারা শনাক্ত (যেমন ট্রোজান, ভিডিও এস বা অন্যান্য সম্পাদিত কর্ম) করতে পারে।

ম্যালওয়্যার

ম্যালিশাস সফটওয়্যার হলো সেই সফটওয়্যার, যা ব্যবহার করে বা তৈরি করে হামলাকারীরা কমপিউটারের ব্যবহারে বাধা সৃষ্টি করার জন্য, গুরুত্বপূর্ণ ও সংবেদনশীল তথ্য হাতিয়ে নেয়ার জন্য অথবা প্রাইভেট কমপিউটার সিস্টেমে অ্যাক্সেস পাওয়ার জন্য। ম্যালওয়্যার আবির্ভূত হতে পারে কোড, স্ক্রিপ্ট, অ্যাক্টিভ কন্টেন্ট এবং অন্যান্য সফটওয়্যার রূপে। ম্যালওয়্যার হলো সাধারণ টার্ম, যা ব্যবহার হয় বিভিন্ন ধরনের বিরোধী বা অনধিকার প্রবেশকারী সফটওয়্যারে।

প্যাকেট স্নিফিং

প্যাকেট স্নিফারকে কখনো কখনো রেফার করা হয় একজন নেটওয়ার্ক মনিটর বা নেটওয়ার্ক অ্যানালাইজার হিসেবে। নেটওয়ার্ক ট্রাফিক মনিটর এবং ট্রাবলশুট করার জন্য একজন নেটওয়ার্ক বা সিস্টেম অ্যাডমিনিস্ট্রেটর বৈধভাবে প্যাকেট স্নিফার ব্যবহার করতে পারেন। প্যাকেট স্নিফারের মাধ্যমে ক্যাপচার করা তথ্য ব্যবহার করে একজন অ্যাডমিনিস্ট্রেটর শনাক্ত করতে পারেন ত্রুটিপূর্ণ প্যাকেট এবং ডাটাকে ব্যবহার করে বটলনেককে পিন পয়েন্ট করতে এবং সহায়তা করে দক্ষতার সাথে নেটওয়ার্কে ডাটা ট্রান্সমিশনে। সহজ কথায় বলা যায় একটি ডিভাইস বা প্রোগ্রাম, যা মনিটর করে নেটওয়ার্কের কমপিউটারে ভ্রমণরত ডাটাকে।

পাসওয়ার্ড

আপনার কমপিউটার সিস্টেম পাসওয়ার্ড প্রোটেকটেড তা নিশ্চিত করতে যদি পারেন, তাহলে আপনার কমপিউটারে বা কমপিউটারের নেটওয়ার্কের কিছু অংশে অ্যাক্সেসের সুবিধা পেতে পারেন। ব্যক্তিগত তথ্য ব্যক্তিগত রাখতে চাইলে প্রথম করণীয় কাজ হলো প্রতিরোধ করা, তথা পাসওয়ার্ড সেট করা। পাসওয়ার্ড হলো গোপন ওয়ার্ড বা ফ্রেস, যা অবশ্যই ব্যবহার করতে হবে কোনো কিছুতে অ্যাক্সেস পাওয়ার জন্য। আরেকভাবে বলা যায়, পাসওয়ার্ড হলো কিছু ক্যারেক্টার স্ট্রিং, যা কমপিউটার ইন্টারফেস বা সিস্টেমে অ্যাক্সেসকে অনুমোদন করে।

ফিশিং

ফিশিং হলো তথ্য হাতিয়ে নেয়ার প্রচেষ্টা। যেমন ইউজার নেম, পাসওয়ার্ড এবং ক্রেডিট কার্ডের বিস্তারিত তথ্য (কখনো কখনো পরোক্ষভাবে অর্থও) ইলেকট্রনিক কমিউনিকেশনে বিশ্বস্ত ও আস্থাশীল হিসেবে ছদ্মবেশী ব্যক্তি বা প্রতারক। ছদ্মবেশী ব্যক্তিরা বৈধ ব্যবসায়ী হিসেবে আচরণ করে, ই-মেইলের মাধ্যমে আপনাকে উপদেশ দেবে যে আপনার অ্যাকাউন্ট ফ্রোজেন করা হয়েছে অথবা কম্প্রোমাইজ হয়ে গেছে এবং নিশ্চিত হওয়ার জন্য লগইন করতে বলবে। কিন্তু দুর্ভাগ্যজনকভাবে আপনি যে লিঙ্কে ক্লিক করলেন লগ করার জন্য তা বৈধ নয়। এভাবে আপনার ব্যক্তিগত গোপন তথ্য জেনে নিয়ে প্রতারণার জালে আপনাকে আবদ্ধ করে ফেলবে।

রেপ্লিকেটর : যেসব প্রোগ্রাম এমন আচরণ করে যে নিজেই নিজের কপি তৈরি করছে। যেমন ওয়ার্ম, ভাইরাস ইত্যাদি।

রুটকিট

রুটকিট একটি হ্যাকার সিকিউরিটি টুল, যা একটি কমপিউটারে এবং কমপিউটার থেকে পাসওয়ার্ড ও মেসেজ ট্রাফিক ক্যাপচার করে। রুটকিট প্রোগ্রাম রুটকিট হিসেবেও পরিচিত। এটি একটি টুলের কালেকশন, যা হ্যাকারদেরকে অনুমোদন করে এবং সিস্টেমের ব্যাকডোর প্রদান করে, নেটওয়ার্কের অন্যান্য সিস্টেমের তথ্য সংগ্রহ করে, সিস্টেম যে কম্প্রোমাইজড সিস্টেম এ সত্য আড়াল করে এবং এ ধরনের আরো অনেক কাজ করে। বলা যায় রুটকিট হলো ট্রোজান হর্স সফটওয়্যারের এক ক্লাসিক উদাহরণ। এই টুল বিভিন্ন অপারেটিং সিস্টেম রেঞ্জে ব্যাপকভাবে পরিলক্ষিত হয়।

স্প্যাম

স্প্যাম বাছবিচারহীনভাবে অযাচিত, অনাকাঙ্ক্ষিত, অসংশ্লিষ্ট অথবা যথাযথ নয় এমন প্রচুর মেসেজ পাঠায়, বিশেষ করে বাণিজ্যিক বিজ্ঞাপনে। স্প্যাম মূলত বিরক্ত করা ছাড়া তেমন কোনো ক্ষতি করে না সিস্টেমে। স্প্যামকে 'ইলেকট্রনিক জাঙ্ক মেইল'ও বলা হয়।

স্পাইওয়্যার

আপনি কমপিউটারে যে অ্যাকশন যেমন– উইন্ডোজ ওপেন করা, মাউস ক্লিক এবং বিশেষ করে কিবোর্ড ইনপুট কার্যকর করবেন, স্পাইওয়্যার সফটওয়্যার তা কাউকে রিপোর্ট করে অথচ আপনি তা জানেন না বা আপনি ওই তথ্য পেতে চান। চুরি হওয়া লগইন, পাসওয়ার্ড এবং ব্যাংক অ্যাকাউন্ট বা ক্রেডিট কার্ড নম্বর যা স্পাইওয়্যারের রচয়িতারা সাধারণত চুরি করতে চায়।

ট্রোজান

ট্রোজান হলো একটি কমপিউটার হুমকি, যা সহজেই (অনাকাঙ্ক্ষিতভাবে) ডাউনলোড হয় এবং কার্যকর করে ম্যালিশাস ফাংশন, যা মেশিনকে অনাকাঙ্ক্ষিত অ্যাক্সেসের জন্য সবার সামনে উপস্থাপন করে।

ভাইরাস

ভাইরাস ম্যালওয়্যার কমপিউটারকে আক্রান্ত করে এবং এরপর নিজেই বিস্তৃত হতে চেষ্টা করে। এটি সম্ভব হতে পারে ই-মেইল আইএম বা নেটওয়ার্ক জুড়ে নিজেকেই সেন্ড করার মাধ্যমে। ট্রান্সমিশন বা সংক্রমণের প্রক্রিয়া কেমন তা বিবেচ্য বিষয় নয়। ভাইরাস হোস্ট কমপিউটারকে কোনো রূপ সমর্থন দেয় না। অনেক সময় ভাইরাস নিজেই ক্ষতিকর না হলেও ভাইরাস কোড উন্মুক্ত করতে পারে ভলনিয়ারিবিলিটি, যা অন্য কোনো ধরনের ম্যালওয়্যার ব্যবহার করতে পারে।

ওয়ার্ম

ওয়ার্ম হলো সবচেয়ে জটিল ধরনের ম্যালওয়্যার। এগুলো খুব ধীরে মুভ করা প্রোগ্রাম, যা এমনভাবে তাদের টার্গেট নেটওয়ার্কে ধীরে ধীরে সুকৌশলে প্রবেশ করে এবং সাধারণত এক সপ্তাহ বা এক মাস বা তার বেশি সময় নেয় পুরো প্রোগ্রামের কম্পোনেন্ট অংশকে অ্যাসেম্বেল করতে। আর এ কাজটি সম্পন্ন করে চূড়ান্তভাবে সিস্টেমকে আক্রমণ করার আগে। যেমন ব্যাপক পরিচিত স্টাক্সনেট ওয়ার্ম। সহজ কথায় বলা যায়, ওয়ার্ম হলো স্বতন্ত্র প্রোগ্রাম যা নেটওয়ার্ক সংযুক্ত মেশিন থেকে মেশিনে রেপ্লিকেট করে তথা হুবহু নকল করে এবং যেভাবে বিস্তৃত হবে সেই অনুযায়ী নেটওয়ার্ক ও ইনফরমেশন সিস্টেমকে ব্যাহত করবে কজ

ফিডব্যাক : swapan52002@yahoo.com