ভূমিকা

বর্তমান সময়ে পেন ড্রাইভ ভাইরাসের যে দুর্দান্ত প্রতাপ চলছে, তা ব্যবহারকারী মাত্রই জানেন। নানা জাতের অ্যান্টিভাইরাস ব্যবহারেও যখন কোন ফলাফল পাওয়া যায় না, তখন দুঃখের সাথে উইন্ডোজ রি-ইন্সটল করতে হয়। তারপরও শান্তি নাই। মাত্র উইন্ডোজ সেটআপ করলাম, পেন ড্রাইভটা লাগালাম, ব্যস। আবারও গেল। প্রচলিত অ্যান্টিভাইরাসগুলো এ সকল ভাইরাস ঠিকমত ধরতে না পারায় (দু-একটি অ্যান্টিভাইরাস ধরতে পারলেও পিসি ভাইরাস ইনফেক্টেড হয়ে গেলে Folder Options কখনোই ফিরিয়ে আনতে পারে না) ব্যবহারকারীদের মাঝে হতাশা বেড়েই চলেছে। এখন সমাধান একটিই (যতক্ষণ না কোন কার্যকর অ্যান্টিভাইরাস বের হচ্ছে) - ম্যানুয়ালি এসব ভাইরাস ডিটেক্ট ও ক্লীন করা। কাজটি মোটেও কঠিন নয় এবং অবিশ্বাস্য দ্রুত গতিতে তা করা সম্ভব। এখানে আমি কম্পিউটার ভাইরাস সম্পর্কে পূর্ণাঙ্গ আলোচনা করব ইনশা আল্লাহ। আলোচনা করার সময় আমি দুধরনের ব্যবহারকারীর কথা বিবেচনা করব - যাঁরা ইন্টারনেট ব্যবহার করেন এবং যাঁরা করেন না। সাধারণভাবে আমি ধরে নিব ব্যবহারকারী ইন্টারনেট ব্যবহার করেন না। যেখানে প্রযোজ্য হবে, সেখানে আমি বলে দিব যে, এটি কেবল ইন্টারনেট ব্যবহারকারীর জন্য প্রযোজ্য। উল্লেখ্য, আমি এ টিউটোরিয়ালটিতে ধরে নিয়েছি যে, ব্যবহারকারী উইন্ডোজ এক্সপি (Default Theme) ব্যবহার করেন। তবে উইন্ডোজ এক্সপি ক্লাসিক থীম, উইন্ডোজ ২০০০ বা ভিস্তার ক্ষেত্রেও এটি সমানভাবে প্রযোজ্য; কেবল আমি যে সকল অপশন বর্ণনা করেছি, সেগুলো ঠিক বর্ণিত স্থানে না থেকে অন্য কোন স্থানে থাকতে পারে এবং অপশনগুলোর ব্যবহার একটু অন্য রকম হতে পারে।

ম্যালওয়্যার কী ও কিভাবে ছড়ায়

Malware শব্দটিকে ভাঙলে দাঁড়ায় Mal (Malicious-এর সংক্ষিপ্ত রূপ, অর্থ ক্ষতিকর) এবং Ware (Software-এর সংক্ষিপ্ত রূপ)। অর্থাৎ, পিসির জন্য ক্ষতিকর যে কোন সফটওয়্যারকেই বলা যায় ম্যালওয়্যার। বিশেষজ্ঞগণ প্রায় ১২ ধরনের ম্যালওয়্যারের সন্ধান দিয়েছেন। নিচে প্রধান ও প্রচলিত ১০টি প্রকারভেদ সম্পর্কে সংক্ষেপে আলোচনা করা হল।

১. ভাইরাস (Virus)

কম্পিউটার ভাইরাস হল এমন একটি ক্ষতিকর প্রোগ্রাম যা নিজের প্রতিলিপি তৈরি করতে পারে এবং অন্য কোন প্রোগ্রামের সাথে নিজেকে যুক্ত করার মাধ্যমে ব্যাপকভাবে ছড়িয়ে পড়তে পারে।

এক পিসি থেকে কোন ভাইরাস আক্রান্ত প্রোগ্রাম নিয়ে অন্য কোন ব্যবহারকারীর পিসিতে কপি করে রান করালে ঐ ব্যবহারকারীর পিসিতে ভাইরাসটি সক্রিয় হয়ে উঠবে। এছাড়া নেটওয়ার্ক (ল্যান) কানেকশন থাকলে অন্য কোন পিসিতে যে সকল ফাইল শেয়ার করা থাকবে, সেগুলোকেও ভাইরাস আক্রমণ করতে পারে। উল্লেখ্য, ভাইরাস কেবল মাত্র এক্সিকিউটেবল ফাইলকেই (.exe ও .com এক্সটেনশন[1] যুক্ত ফাইল) আক্রমণ করে, অন্য কোন ধরনের ফাইলকে আক্রমণ করে না। তবে কিছু কিছু ভাইরাসে 'বাগ' থাকার কারণে সেগুলো অন্যান্য এক্সটেনশন যুক্ত ফাইলকেও আক্রমণ করে, তবে সেক্ষেত্রে সেসব ফাইল পুনরায় অন্য কোন ফাইলকে আক্রমণ করতে পারে না, এবং অনেক ক্ষেত্রে আক্রান্ত হওয়ার কারণে ফাইলগুলো নষ্ট হয়ে যায়। এ হিসাবে ভাইরাসের ডেটা ফাইল নষ্ট করার ক্ষমতা রয়েছে।

কয়েক বছর পূর্বেও ভাইরাসের দুর্দান্ত প্রতাপ ছিল, যা বর্তমানে (অন্ততপক্ষে বাংলাদেশে) নেই বললেই চলে।

[1] ফাইলের এক্সটেনশন প্রকাশ করে যে, ফাইলটি কোন্ প্রকারের। যেমন, মাইক্রোসফট ওয়ার্ডের একটি ফাইলের এক্সটেনশন হল doc । এক্সটেনশনকে ফাইলের নাম থেকে আলাদা করা হয় একটি ডট (.) দ্বারা। উদাহরণস্বরূপ, ঐ ওয়ার্ড ফাইলের নাম যদি হয় abc, তাহলে এক্সটেনশন সহ ফাইলটির নাম হবে abc.doc । এখানে abc হল ফাইলের নাম এবং doc হল ফাইলের এক্সটেনশন। অপারেটিং সিস্টেম doc অংশটি দেখলেই বুঝতে পারবে যে, এটি মাইক্রোসফট ওয়ার্ড ডকুমেন্ট ফাইল (যদি পিসিতে ওয়ার্ড ইন্সটল করা থাকে)।

২. ট্রোজান হর্স (Trojan Horse)

ট্রোজান হর্স (বা সংক্ষেপে ট্রোজান) হল এমন ক্ষতিকর প্রোগ্রাম, যা একটি ভাল প্রোগ্রামের ছদ্মবেশে ক্ষতিকর কাজ করে। যেমন, কোন একটি প্রোগ্রাম হার্ড ডিস্ক ফরম্যাট করে। এ প্রোগ্রামটি একটি ইউটিলিটি প্রোগ্রাম হতে পারে, আবার একটি ট্রোজানও হতে পারে। যদি প্রোগ্রামটি ব্যবহারকারীর অনুমতি সাপেক্ষে হার্ড ডিস্ক ফরম্যাট করে, তাহলে তা হল ইউটিলিটি প্রোগ্রাম। কিন্তু তা যদি ব্যবহারকারীর অজান্তে হার্ড ডিস্ক ফরম্যাট করে, তাহলে তা হল ট্রোজান।

৩. ব্যাকডোর (Backdoor)

ব্যাকডোর অনেকটা ভাইরাস কিংবা ওয়ার্মের মতই, কেবল পার্থক্য হল তা কোন কম্পিউটারে একটি 'ব্যাকডোর' তথা নেটওয়ার্ক কানেকশন খুলে দেয়, যেখান দিয়ে কোন হ্যাকার বা অন্য কোন ম্যালওয়্যার পিসিতে প্রবেশ করতে পারে অথবা পিসি থেকে কোন ওয়ার্ম বা স্পাইওয়্যার অন্য কোথাও (প্রতিলিপি তৈরি করার জন্য) যেতে পারে।

৪. ওয়ার্ম (Worm)

ওয়ার্ম হল এমন একটি ক্ষতিকর প্রোগ্রাম, যা নিজের প্রতিলিপি তৈরি করতে পারে, কিন্তু অন্য কোন প্রোগ্রামের সাথে নিজেকে যুক্ত করতে পারে না।

সাধারণত, কোন পিসি যদি ওয়ার্ম দ্বারা আক্রান্ত হয়ে থাকে, তাহলে তাতে কোন ইউ.এস.বি. ড্রাইভ প্রবেশ করালে স্বয়ংক্রিয়ভাবে ওয়ার্ম ফাইলটি তাতে কপি হয়ে যায়। এই ড্রাইভটি অন্য কোন পিসিতে লাগিয়ে কোনভাবে ওয়ার্ম ফাইলটি রান করালেই ঐ পিসি ওয়ার্ম দ্বারা আক্রান্ত হয়ে যাবে। এছাড়া ল্যান কানেকশন থাকলে ওয়ার্ম ল্যানের অন্যান্য পিসিতে শেয়ারকৃত ফোল্ডারে কপি হয়ে যায়। ইন্টারনেট কানেকশন থাকলে কিছু কিছু ওয়ার্ম আপনার অ্যাড্রেস বুক থেকে আপনার অজান্তে মেইল অ্যাড্রেস সংগ্রহ করে ই-মেইল অ্যাটাচমেন্ট হিসেবে স্বয়ংক্রিয়ভাবে সেসব অ্যাড্রেসে চলে যায়।

ম্যালওয়্যারের জগতে বর্তমানে (অন্ততপক্ষে বাংলাদেশে) ওয়ার্মই সবচেয়ে সক্রিয় ভূমিকা পালন করছে।

৫. ওয়্যাবিট (Wabbit)

ওয়্যাবিট ও ওয়ার্ম প্রায় একই, পার্থক্য হল ওয়্যাবিট ই-মেইলের মাধ্যমে ছড়াতে পারে না।

৬. এক্সপ্লোইট (Exploit)

এক্সপ্লোইট কোন সফটওয়্যারে সিকিউরিটি হোল পেলে সেখানে আক্রমণ করে।

৭. রুটকিট (Rootkit)

রুটকিট সিস্টেমের গুরুত্বপূর্ণ প্রসেসের ছদ্মবেশে থেকে ক্ষতিকর কাজ পরিচালনা করে। সকল ম্যালওয়্যারের মধ্যে রুটকিট ডিটেক্ট করা সবচেয়ে কঠিন।

৮. স্পাইওয়্যার (Spyware)

স্পাইওয়্যার আপনার পিসি থেকে গুরুত্বপূর্ণ তথ্য সংগ্রহ করে স্পাইওয়্যার নির্মাতার নিকট তা পাঠিয়ে দেয়। সাধারণত আপনার ব্রাউজিং অভ্যাস স্পাইওয়্যার সংগ্রহ করে থাকে। এরপর এই তথ্যের আলোকে ব্রাউজিংয়ের সময় তা বিভিন্ন বিজ্ঞাপন প্রদর্শন করে থাকে। এছাড়াও স্পাইওয়্যার আপনার নাম, ঠিকানা, ক্রেডিট কার্ড নম্বর ইত্যাদি সংগ্রহ করতে পারে এবং এরপর আপনাকে ব্ল্যাকমেইল করতে পারে।

৯. অ্যাডওয়্যার (Adware)

অ্যাডওয়্যার আপনার কম্পিউটারে বিভিন্ন বিজ্ঞাপন প্রদর্শন করে থাকে। এছাড়াও বেশ কিছু সফটওয়্যার রয়েছে, যেগুলো অ্যান্টিস্পাইওয়্যার হিসেবে আপনাকে পরিচয় দিবে এবং বলবে যে, আপনার পিসিতে বেশ কিছু স্পাইওয়্যার রয়েছে, যেগুলো ঐ অ্যান্টিস্পাইওয়্যারটি না কিনলে দূর করা যাবে না। এসব সফটওয়্যারকে রউগ (Rogue) প্রোগ্রাম বলে, এবং এগুলো এক ধরনের অ্যাডওয়্যার।

১০. কী-লগার (Keylogger)

কী-লগার আপনার প্রতিটি কী-প্রেস রেকর্ড করে রাখে এবং এগুলো তার নির্মাতার নিকট পাঠিয়ে দেয়। এগুলো সাধারণত আপনার কোন পাসওয়ার্ড বা ক্রেডিট কার্ড নম্বর ইত্যাদি গুরুত্বপূর্ণ তথ্য চুরি করার জন্য ব্যবহৃত হয়।

ম্যালওয়্যার প্রতিরোধের উপায়

“Prevention is better than cure” – প্রতিকারের চেয়ে প্রতিরোধ উত্তম। কথাটি খুবই সত্য। ম্যালওয়্যার আক্রান্ত পিসি ম্যালওয়্যারমুক্ত করার চেয়ে তা যাতে কোনভাবেই পিসিকে আক্রমণ করতে না পারে, তার ব্যবস্থা করা অনেক সহজ। উপরে উল্লিখিত ম্যালওয়্যারগুলোর প্রতিরোধের উপায় নিচে আলোচনা করা হল।

ভাইরাস, ট্রোজান হর্স ও ব্যাকডোর প্রতিরোধের উপায়

এগুলো প্রতিরোধের সবচেয়ে সহজ উপায় হল অ্যান্টিভাইরাস ব্যবহার করা। কিন্তু আমি তা Recommend করি না। কেননা, অ্যান্টিভাইরাস ব্যবহারের ফলে অকারণে আপনার পিসি স্লো হয়ে যাবে। ‘অকারণে’ বলছি এ জন্য যে, অধিকাংশ সময়ই অ্যান্টিভাইরাস মনিটরের কোন প্রয়োজন হয় না – কেবল সিডি বা পেন ড্রাইভ প্রবেশ করানোর সময় এর দরকার হয়। কিন্তু অন্যান্য সময়ে, যেমন আপনার হার্ড ডিস্কের কোন একটি ফোল্ডারে ডাবল-ক্লিক করলে সে প্রথমে ফোল্ডারের ভিতর যে সকল ফাইল রয়েছে, সেগুলো কুইক স্ক্যান করে নেয়। ফাইলের সংখ্যা যত বেশি হবে, স্ক্যান করতে সময় তত বেশি লাগবে। ফলে আপনি স্পষ্ট বুঝতে পারবেন যে, পিসি Slow response করছে (যদি না আপনি লেটেস্ট কোর টু ডুয়ো প্রসেসর বা ১/২ জি.বি. র‍্যাম ব্যবহার করেন)। অথচ পুরো হার্ড ডিস্ক একবার স্ক্যান করার পর আপনি নিশ্চিত থাকতে পারবেন যে, হার্ড ডিস্কে কোন ভাইরাস নেই। তাহলে তার পরও প্রতি বার হার্ড ডিস্কের কোন ফোল্ডারে ঢুকতে গেলে কেন পুনরায় স্ক্যান করার প্রয়োজন পড়বে? Low বা Medium Configuration –এর পিসির জন্য তাই অ্যান্টিভাইরাস এক প্রকার বোঝাস্বরূপ।

আপনি হয়ত বলতে পারেন যে, ঠিক আছে, তাহলে সব সময়ের জন্য অ্যান্টিভাইরাসের অন-অ্যাকসেস স্ক্যানার ডিজেবল করে রেখে যখন কোন পেন ড্রাইভ বা সিডি প্রবেশ করানো হবে, কেবল তখনই তা এনেবল করা যাবে। কিন্তু বাস্তব ক্ষেত্রে আমি দেখেছি, অন-অ্যাকসেস স্ক্যানার ডিজেবল করে রাখলেও কেন জানি তা চলতে থাকে। এটি পরীক্ষা করার জন্য আমি একবার একটি নাম করা অ্যান্টিভাইরাসের অন-অ্যাকসেস স্ক্যানার ডিজেবল করে রেখে একটি ভাইরাসযুক্ত ফাইলের উপর ক্লিক করেছিলাম। দেখি তৎক্ষণাৎ অ্যান্টিভাইরাসটি সতর্ক বার্তা দেখাল। যদি অন-অ্যাকসেস স্ক্যানার ডিজেবলই থাকত, তাহলে তা স্ক্যান করা ছাড়া সতর্ক বার্তা দেখাল কি করে? তবে এমনও হতে পারে যে, যে সময় আমি এ পরীক্ষাটি করেছিলাম, সে সময় অ্যান্টিভাইরাস সফটওয়্যারটিতে বাগ ছিল, অথবা কেবল ঐ অ্যান্টিভাইরাসটিতেই এরকম সমস্যা হয়। কেননা, পরবর্তীতে আবার অন্য একটি বিখ্যাত অ্যান্টিভাইরাস চেক করতে গিয়ে আমি দেখেছি যে, তার অন-অ্যাকসেস স্ক্যানার ডিজেবল করে রাখলে তা সত্যিই ডিজেবল হয়ে থাকে। সুতরাং, অন-অ্যাকসেস স্ক্যানার ডিজেবল করার পূর্বে পরীক্ষা করে নিশ্চিত হয়ে নিবেন যে, তা সত্যিই ডিজেবল হয়ে থাকে কি না।

তাছাড়া লেটেস্ট অ্যান্টিভাইরাসগুলোতে রুটকিট প্রোটেকশনের জন্য রেজিস্ট্রি মনিটরিং, স্টার্ট-আপ কন্ট্রোল ইত্যাদি ফীচার থাকে। অধিকাংশ সাধারণ ব্যবহারকারীই এ সকল ফীচার বন্ধ করার পদ্ধতি জানেন না। ফলে আমি একজন ইউজারকে দেখলাম Kaspersky Antivirus 7 চালু রেখে Power DVD Pro 6 ইন্সটল করতে গিয়ে যে ঝামেলায় পড়ল (অ্যান্টিভাইরাসটি বারবার প্রশ্ন করছে যে, এ সফটওয়্যারটি অমুক রেজিস্ট্রি কী পরিবর্তন করতে যাচ্ছে, তা করতে দিব কী? তমুক স্টার্ট-আপে যুক্ত হতে চাচ্ছে, সেটি কি নরাপদ মনে হয়? – ইত্যাদি নানান ফালতু প্রশ্ন। আর ইউজারকে বারবার একই উত্তর দিতে হচ্ছে – হ্যাঁ, হ্যাঁ, হ্যাঁ), তাতে সে ইন্সটলেশন শেষ করে সিদ্ধান্ত নিল যে, অ্যান্টিভাইরাস ব্যবহার না করলেই শান্তি!

এছাড়াও রয়েছে অ্যান্টিভাইরাস আপডেটের ঝামেলা। পিসিতে ব্রডব্যান্ড ইন্টারনেট সংযোগ না থাকলে প্রতি সপ্তাহে সাইবার ক্যাফেতে গিয়ে আপডেটেড Virus Signature File ডাউনলোড করে নিয়ে আসা যে কী ঝামেলাজনক, তা যিনি এ পরিস্থিতিতে পড়েছেন, কেবল তিনিই জানেন। আর যদি নিয়মিত অ্যান্টিভাইরাস আপডেট না করেন, তাহলে নিত্যকার নতুন Threat থেকে তো আর বাঁচতে পারবেন না।

উপরে যা বলা হল, তা ইন্টারনেট সংযোগ নেই এমন পিসির ক্ষেত্রে প্রযোজ্য। এখন, ইন্টারনেট যুক্ত পিসির জন্য কি অ্যান্টিভাইরাস প্রয়োজন? আমি বলব – ইন্টারনেট যুক্ত পিসিতে অ্যান্টিভাইরাস ব্যবহারের চেয়ে ফায়ারওয়াল ব্যবহার করাটা অধিক জরুরী। আপনি যদি নিচে বর্ণিত ভাইরাস প্রতিরোধের কয়েকটি নিয়ম-কানুন অনুসরণ করেন এবং একটি ভাল ফায়ারওয়াল ব্যবহার করেন, তাহলে অ্যান্টিভাইরাসের কোন প্রয়োজন পড়বে না। তারপরও যদি আপনি 'বিশেষ' সতর্কতার জন্য অ্যান্টিভাইরাস ব্যবহার করতে চান, তাহলে কারো কোন আপত্তি থাকার কথা না।

আমি এতটা আত্মবিশ্বাসের সাথে উক্ত কথাগুলো বলছি এ কারণে যে, আমি জুন, ২০০৬ থেকে অ্যান্টিভাইরাস ছাড়াই পিসি ব্যবহার করে আসছি এবং জুলাই, ২০০৭ থেকে ২৪ ঘণ্টা ব্রডব্যান্ড ইন্টারনেট সেবা পেয়ে আসছি; কিন্তু আমার পিসিতে এখন পর্যন্ত কোন ভাইরাস পাওয়া যায় নি। হ্যাঁ, আমি ইন্টারনেট সংযোগ নেওয়ার পর থেকে ফায়ারওয়াল ব্যবহার করে আসছি। একইভাবে, আমার বন্ধু-বান্ধবরা আমারও পূর্ব থেকে পিসি ব্যবহার করে আসছে অ্যান্টিভাইরাস ব্যবহার করা ছাড়াই। তাদের পিসিতেও কোন ভাইরাস পাওয়া যায় না।

যা হোক, আপনি যদি অ্যান্টিভাইরাস ব্যবহার করতে চান, তাহলে কোন্‌টি ব্যবহার করলে উত্তম হবে এবং কোন্‌ ফায়ারওয়ালটি ভাল, তা একটু পরে আলোচনা করছি। এখন ভাইরাস প্রতিরোধের কয়েকটি টিপ্‌স্‌ আলোচনা করা যাক:

১. এমন কোন এক্সিকিউটেবল ফাইলে ডাবল-ক্লিক করবেন না যেটার সম্পর্কে আপনি কিছু জানেন না অথবা ফাইলটির উৎসের নির্ভরযোগ্যতা সম্পর্কে আপনি সন্দিহান। তবে গবেষণার ক্ষেত্রে (অর্থাৎ এক্সিকিউটেবল ফাইলটি কোন সফটওয়্যার হলে তা কিসের সফটওয়্যার, তা জানার ক্ষেত্রে) আপনাকে কিছুটা রিস্ক নিতেই হবে। এক্ষেত্রে অ্যান্টিভাইরাস দিয়ে ফাইলটি স্ক্যান করা আর না করা আমার মতে সমান। কেননা, অধিকাংশ অ্যান্টিভাইরাসই লেটেস্ট ভাইরাস ডিটেক্ট করতে পারে না। তবে তার পরও আপনি অ্যান্টিভাইরাস দিয়ে ফাইলটি স্ক্যান করিয়ে নিতে পারেন। আপনার যদি ইন্টারনেট সংযোগ থাকে, তাহলে সবচেয়ে ভাল হয় যদি আপনি ফাইলটি www.virustotal.com –এ আপলোড করে স্ক্যান করান। এ সাইটটিতে আপনার ফাইলটি ৩২টি অ্যান্টিভাইরাস দ্বারা স্ক্যান করা হবে এবং স্ক্যান শেষে রিপোর্ট দেওয়া হবে।

২. আপনার পরিচিত কোন ব্যক্তি থেকে আসা মেইল ছাড়া অন্য কারো মেইলের অ্যাটাচমেন্ট খুলবেন না। আর আপনার পরিচিত ব্যক্তি যদি অ্যাটাচমেন্ট হিসেবে কোন এক্সিকিউটেবল ফাইল পাঠায়, তাহলে নিশ্চিত না হলে তা খুলবেন না। সন্দেহ হলে ঐ ব্যক্তিকে অ্যাটাচমেন্টের ব্যাপারে জিজ্ঞাসা করুন।

৩. সফটওয়্যারের ক্র্যাক ব্যবহার করার ব্যাপারে সাবধান থাকুন। ভাইরাস ছড়ানোর একটি অন্যতম মাধ্যম হল ক্র্যাক।

৪. আপনি অ্যান্টিভাইরাস ব্যবহার করুন আর নাই করুন, সর্বদা গুরুত্বপূর্ণ ডেটার ব্যাকআপ রাখবেন।

৫. ইন্টারনেটে ব্রাউজ করার সময় যদি আপনাকে কোন অপরিচিত সফটওয়্যার ডাউনলোড করে ইন্সটল করতে বলা হয়, তাহলে সফটওয়্যারটির উৎসের নির্ভরযোগ্যতার ব্যাপারে নিশ্চিত হয়ে তবেই তা ডাউনলোড করবেন।

৬. http://files.avast.com/files/eng/aswclnr.exe -এই লিংক থেকে Avast! Virus Cleaner ডাউনলোড করে নিন। কিছু দিন বা কয়েক মাস পর পর তা রান করিয়ে কেবল মেমরি স্ক্যান করুন। ভাইরাস থেকে থাকলে সাধারণত তা মেমরিতে চলতে থাকে। তাই, যদি মেমরিতে ভাইরাস ধরা পড়ে, তাহলে অ্যান্টিভাইরাস দিয়ে পুরো হার্ড ডিস্ক স্ক্যান করুন। আর যদি মেমরিতে ভাইরাস ধরা না পড়ে, তাহলে আপনি ইচ্ছা করলে ঐ মুহুর্তে অ্যান্টিভাইরাস ইন্সটল করে তা দিয়ে সিস্টেম স্ক্যান করে পুনরায় তা আনইন্সটল করে দিতে পারেন। তবে মনে রাখবেন – সর্বদা আপডেটেড অ্যান্টিভাইরাস ব্যবহার করবেন।

অ্যান্টিভাইরাসের জগতে সবচেয়ে ভাল অ্যান্টিভাইরাস কোন্‌টি – এই প্রশ্নটির উত্তর একেক সময় একেক রকম হবে। এটা নিশ্চিত যে, সব অ্যান্টিভাইরাস সব রকম ভাইরাস ডিটেক্ট বা ক্লীন করতে পারে না। একটি অ্যান্টিভাইরাস কতটা ভাল, তা নির্ভর করে সেটি কত বেশি সংখ্যক ভাইরাস ডিটেক্ট ও ক্লীন করতে পারে, সিস্টেমকে কতটা Fast রাখে, কত দ্রুত নির্দিষ্ট সংখ্যক ফাইল স্ক্যান করতে পারে, কত কম সংখ্যক False Alarm দেয় ইত্যাদি সহ আরো অনেক বিষয়ের উপর। অ্যান্টিভাইরাস টেস্টিংয়ের জন্য বিশ্বজুড়ে স্বীকৃত প্রতিষ্ঠান হল AV-Test (www.av-test.org)। এ প্রতিষ্ঠানের সাথে বিভিন্ন কোম্পানী যৌথভাবে সময়ে সময়ে অ্যান্টিভাইরাস টেস্ট করে থাকে। বিশ্বের একটি অন্যতম বিখ্যাত আইটি ম্যাগাজিন PC World (www.pcworld.com) প্রতি বছরই এ ধরনের একটি টেস্টের আয়োজন করে থাকে। টেস্ট শেষে রিপোর্ট এবং টেস্টিং পদ্ধতি উভয়ই তারা পাবলিশ করে। বাংলাদেশে এ ম্যাগাজিনটি সহজলভ্য। তাই যাঁরা সর্বোত্তম অ্যান্টিভাইরাস ব্যবহার করতে চান, তাঁদের উচিত নিয়মিত এ পত্রিকার উপর নজর রাখা।

সর্বশেষ গত ২৩ এপ্রিল, ২০০৭ –এ পিসি ওয়ার্ল্ড অ্যান্টিভাইরাস রিভিউ পাবলিশ করে। সর্বোত্তম ৮টি অ্যান্টিভাইরাসের পূর্ণাঙ্গ রিপোর্ট ও টেস্টিং পদ্ধতি এখান থেকে জানা যাবে - http://www.pcworld.com/article/id,130869/article.html । সে অনুযায়ী এ মুহুর্তে সর্বোত্তম অ্যান্টিভাইরাস হল Kaspersky Labs (www.kaspersky.com) এর Kaspersky Antivirus (মূল্য: $৪৫, প্রতি বছর নবায়ন মূল্য: $৩৫, ৩০ দিনের Free Trial ডাউনলোড করা যায়)। তবে এ অ্যান্টিভাইরাসের অরিজিনাল ভার্সন বাংলাদেশে এখনও পাওয়া যায় না। আপনি বাংলাদেশে থেকে অরিজিনাল অ্যান্টিভাইরাস সফটওয়্যার কিনতে চাইলে Technics Computers (www.technicscomputers.com) থেকে সুলভ মূল্যে Symantec Norton Antivirus (পিসি ওয়ার্ল্ড টেস্টে ২য় স্থান প্রাপ্ত) বা Bitdefender Antivirus (পিসি ওয়ার্ল্ড টেস্টে ৩য় স্থান প্রাপ্ত) কিনতে পারেন। সত্যি কথা বলতে কি, পিসি ওয়ার্ল্ডের রিপোর্ট পড়লে আপনি বুঝতে পারবেন যে, এ তিনটি অ্যান্টিভাইরাস সফটওয়্যারের মধ্যে প্রকৃতপক্ষে তেমন কোন পার্থক্য নেই।

৭. আপনি নিয়মিত ইন্টারনেট ব্যবহার করলে ফায়ারওয়াল ব্যবহার করা উচিত। ইন্টারনেট থেকে কোন কিছু আপনার পিসিতে অ্যাকসেস করতে চাইলে অথবা আপনার পিসি থেকে কোন কিছু ইন্টারনেটে অ্যাকসেস করতে চাইলে ফায়ারওয়াল আপনার অনুমতি চাইবে। এছাড়া ইন্টারনেট থেকে আপনার পিসি হ্যাক করার চেষ্টা করলে ফায়ারওয়াল স্বয়ংক্রিয়ভাবে তা Block করে দেয়। প্রাথমিক অবস্থায় ব্যবহারকারীদের নিকট এটি বিরক্তিকর মনে হতে পারে, কিন্তু একবার অভ্যস্ত হয়ে উঠলে তখন আর কোন ঝামেলা মনে হয় না।

ফায়ারওয়ালের জগতে নিঃসন্দেহে সেরা ফায়ারওয়াল হল Check Point Software Technologies (www.zonealarm.com) –এর Zone Alarm (www.filehippo.com/download_zonealarm_free), যা সম্পূর্ণ ফ্রী।

আপনি যদি ফায়ারওয়াল ও অ্যান্টিভাইরাস একত্রে ব্যবহার করতে চান, তাহলে আমি Zone Alarm Internet Security Suite (মূল্য: $৬০, প্রতি বছর নবায়ন মূল্য: $৩৫, ১৫ দিনের Free Trial ডাউনলোড করা যায়, ডাউনলোড লিংক: http://www.zonealarm.com/store/content/company/products/znalm/freeDownload.jsp) ব্যবহার করাটা

Recommend করি। কেননা, এতে অ্যান্টিভাইরাস হিসেবে Kaspersky Antivirus ব্যবহার করা হয়। এ ব্যাপারে বিস্তারিত তথ্যের জন্য আপনি এ লিংকটি ভিজিট করতে পারেন:
http://forums.zonealarm.com/zonelabs/board/message?board.id=Antivirus&message.id=19390

৮. আজকাল Security Suite ব্যবহার করার প্রবণতা বেড়ে গেছে। Security Suite –এ একই সাথে Antivirus, Firewall, Antispam, Antispyware ইত্যাদি থাকে। পিসি ওয়ার্ল্ড সর্বশেষ গত ২৫ মে, ২০০৬ তারিখে সিকিউরিটি স্যুট টেস্ট রিপোর্ট পাবলিশ করেছে। সে অনুযায়ী সর্বোত্তম সিকিউরিটি স্যুট হল Symantec Norton Internet Security (মূল্য: $৭০, প্রতি বছর নবায়ন মূল্য: $৫০)। সেরা ১০টি সিকিউরিটি স্যুট সম্পর্কে জানার জন্য এ লিংকটি দেখুন: http://www.pcworld.com/article/id,125857-page,1/article.html । কিন্তু এ টেস্ট অনেক আগের। তাই বর্তমানে এর উপর নির্ভর করা যাবে না। সে সময় Zone Alarm Internet Security Suite ৬ষ্ঠ স্থান অধিকার করেছিল। রিপোর্টে স্পষ্টভাবে উল্লেখ করা হয়েছে যে, তখন Zone Alarm অ্যান্টিভাইরাস হিসেবে CA (www.ca.com) –এর অ্যান্টিভাইরাস ব্যবহার করত, যা বেশ দুর্বল অ্যান্টিভাইরাস ছিল। কিন্তু বর্তমানে Zone Alarm অ্যান্টিভাইরাস হিসেবে Kaspersky ব্যবহার করে, যা পূর্বের বর্ণনা অনুযায়ী এ মুহূর্তের সেরা অ্যান্টিভাইরাস সফটওয়্যার। সুতরাং, কেউ যদি সিকিউরিটি স্যুট ব্যবহার করতে চায়, তবে আমার মতে তার উচিত ৭ নং টিপ্স্ –এ বর্ণিত Zone Alarm Internet Security Suite ব্যবহার করা।

এক্সপ্লোইট প্রতিরোধের উপায়

এক্সপ্লোইট কেবল তখনই আক্রমণ করবে যখন আপনার পিসিতে ইন্টারনেট সংযোগ থাকবে। এক্সপ্লোইটের আক্রমণ থেকে রক্ষা পাওয়ার জন্য আপনাকে সর্বদা সফটওয়্যার ও উইন্ডোজ আপডেটেড রাখতে হবে। কোন Patch বের হবার সাথে সাথে তা ইন্সটল করে নিতে হবে। অবশ্য ফায়ারওয়াল সক্রিয় থাকলে এক্সপ্লোইট দ্বারা আক্রান্ত হবার সম্ভাবনা খুবই কম।

সফটওয়্যার আপডেট করা একটি বিরক্তিকর কাজ। কেননা, কখন কোন্ সফটওয়্যারের আপডেট বা Patch বের হচ্ছে, তার খবর রাখা খুব দুরূহ ব্যাপার। এক্ষেত্রে আপনি ফ্রী filehippo.com Update Checker (www.filehippo.com/updatechecker/udc.exe) ব্যবহার করতে পারেন। ইন্টারনেট সংযোগ থাকাবস্থায় এটি রান করালে আপনার পিসিতে ইন্সটলকৃত সফটওয়্যারগুলো আপপডেটেড কি না, সেই রিপোর্ট আপনাকে দিবে। সেই সাথে সফটওয়্যারের আপডেট ডাউনলোড করার লিংকও দিয়ে দিবে, যাতে সেগুলো ডাউনলোড করতে অযথা সময় নষ্ট না হয়। তবে এ আপডেট চেকারটি আপনার পিসিতে ইন্সটলকৃত সকল সফটওয়্যারের আপডেটেড অবস্থা বলতে নাও পারে, অর্থাৎ, filehippo.com –এর ডেটাবেজে যে সকল সফটওয়্যার রয়েছে, কেবল সে সকল সফটওয়্যারের মধ্যে কোনটি ইন্সটল করা থাকলে তবেই এ প্রোগ্রামটি তার আপডেটেড অবস্থা বলে দিতে পারবে।

ওয়ার্ম ও ওয়্যাবিট প্রতিরোধের উপায়

পেন ড্রাইভ পিসিতে লাগিয়ে ড্রাইভ আইকনে ডাবল-ক্লিক করা মাত্রই ওয়ার্ম (যদি থাকে) সক্রিয় হয়ে যায়। তাই পেন ড্রাইভ প্রবেশ করিয়ে কোন অবস্থাতেই ড্রাইভ আইকনে ডাবল-ক্লিক করা যাবে না। এমনকি পেন ড্রাইভ আইকনে রাইট ক্লিক করে সেখান থেকে Open, Explore, Search প্রভৃতি মেনু সিলেক্ট করে পেন ড্রাইভে ঢুকার চেষ্টা করলেও ওয়ার্ম সক্রিয় হয়ে উঠতে পারে। তাহলে কিভাবে পেন ড্রাইভে অ্যাকসেস করা যাবে? এর বিভিন্ন পদ্ধতি রয়েছে। তবে সবচেয়ে সহজ ও নিশ্চিত কার্যকর পদ্ধতি নিম্নরূপ: (উল্লেখ্য, ধরে নেওয়া হচ্ছে যে, আপনার পিসিতে কোন ধরনের ওয়ার্ম সক্রিয় অবস্থায় নেই। আপনার পিসিতে ওয়ার্ম সক্রিয় অবস্থায় রয়েছে কি না তা জানার জন্য ‘‘ওয়ার্ম প্রতিকারের উপায়’’ অনুচ্ছেদটি দেখুন।)

১. পেন ড্রাইভ প্রবেশ করিয়ে মাই কম্পিউটারে রাইট-ক্লিক করুন। মেনু থেকে Explore-এ ক্লিক করুন।

২. Tools মেনু থেকে Folder Options-এ ক্লিক করুন।

৩. View ট্যাবে ক্লিক করুন।

৪. নিচের Advanced settings অপশনগুলো থেকে Hidden files and folders অপশনের অন্তর্গত Show hidden files and folders অপশনে ক্লিক করুন।

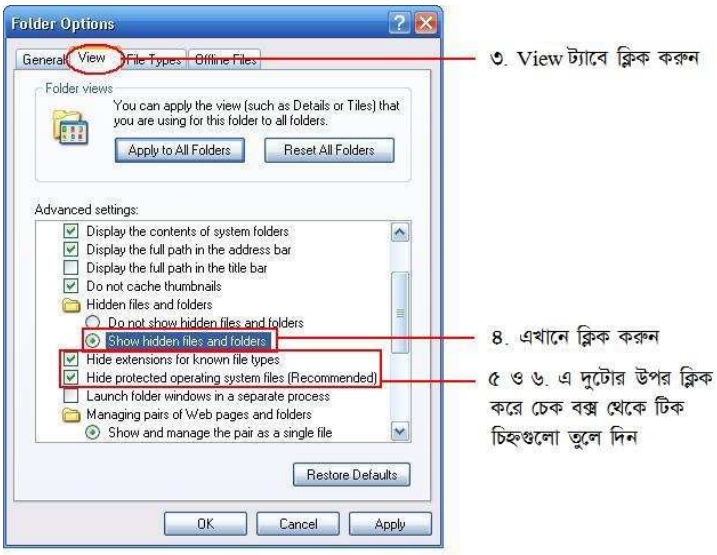
চিত্র: ওয়ার্ম প্রতিরোধের পদ্ধতি (১ম ও ২য় ধাপ)।

৫. ঠিক নিচে অবস্থিত Hide extensions for known file types অপশনের বাম পাশের চেক বক্স থেকে টিক চিহ্ন তুলে দিন।

৬. তার ঠিক নিচে অবস্থিত Hide protected operating system files (Recommended) অপশনের বাম পাশের চেক বক্স থেকেও টিক চিহ্ন তুলে দিন। পর্দায় আগত সতর্ক বার্তার Yes বোতামে ক্লিক করুন।

৭. OK বোতামে ক্লিক করুন।

সামনে অগ্রসর হওয়ার পূর্বে এতক্ষণ কী করা হল তা জেনে নেওয়া দরকার।



চিত্র: ওয়ার্ম প্রতিরোধের পদ্ধতি (৩য় থেকে ৬ষ্ঠ ধাপ)।

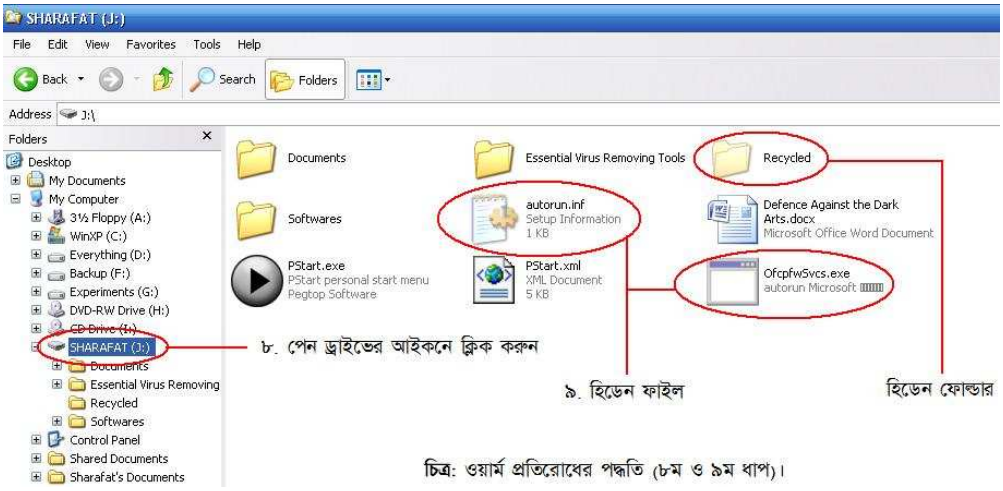
Show hidden files and folders অপশনটি সিলেক্ট করা থাকলে আপনার পিসির সকল hidden ফাইল প্রদর্শিত হবে। ওয়ার্ম ফাইলগুলো হিডেন থাকে। তাই সেগুলোকে ডিটেক্ট করতে হলে এ অপশনটি অবশ্যই সিলেক্ট করতে হবে।

Hide protected operating system files - অপারেটিং সিস্টেমের গুরুত্বপূর্ণ ফাইলগুলো সর্বদা লুকোনো অবস্থায় থাকে। Show hidden files and folders অপশনটি সিলেক্ট করা থাকলেও এ সকল সিস্টেম ফাইল প্রদর্শিত হবে না। কেননা, যদি ভুলবশত এসব ফাইলের কোনটি মুছে যায়, তাহলে অপারেটিং সিস্টেম ঠিকমত বুট হবে না। ফলে উইন্ডোজ নতুন করে রি-ইন্সটল করার প্রয়োজন হতে পারে। তাই অতিরিক্ত সতর্কতার জন্য Show hidden files and folders অপশনটি সিলেক্ট করা থাকা সত্ত্বেও সেগুলো প্রদর্শিত হয় না। সমস্যা হল ওয়ার্ম ফাইলগুলোও সিস্টেম ফাইল হিসেবে থাকে। তাই Hide protected operating system files -এর পাশ থেকে টিক চিহ্ন তুলে দিয়ে সিস্টেম ফাইলগুলো প্রদর্শনের ব্যবস্থাও করতে হবে।

Hide extensions for known file types অপশনটি থেকে টিক চিহ্ন তুলে দিলে সকল ফাইলের এক্সটেনশন দেখা যাবে। ফাইলের এক্সটেনশন প্রকাশ করে যে, ফাইলটি কোন্ প্রকারের। যেমন, মাইক্রোসফট ওয়ার্ডের একটি ফাইলের এক্সটেনশন হল doc । এক্সটেনশনকে ফাইলের নাম থেকে আলাদা করা হয় একটি ডট (.) দ্বারা। উদাহরণস্বরূপ, ঐ ওয়ার্ড ফাইলের নাম যদি হয় abc, তাহলে এক্সটেনশন সহ ফাইলটির নাম হবে abc.doc । এখানে abc হল ফাইলের নাম এবং doc হল ফাইলের এক্সটেনশন। অপারেটিং সিস্টেম doc অংশটি দেখলেই বুঝতে পারবে যে, এটি মাইক্রোসফট ওয়ার্ড ডকুমেন্ট ফাইল (যদি পিসিতে ওয়ার্ড ইন্সটল করা থাকে)। ভাইরাসের ক্ষেত্রে এক্সটেনশন প্রদর্শন কী কাজে দেয়, তা আমরা একটু পরেই দেখব।

এবার বাকি পদক্ষেপগুলো দেখা যাক:

৮. বাম দিকের প্যানেল থেকে পেন ড্রাইভের আইকনে ক্লিক করুন।



চিত্র: ওয়ার্ম প্রতিরোধের পদ্ধতি (৮ম ও ৯ম ধাপ)।

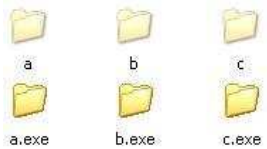
৯. এবার ডান দিকের প্যানেলে ফাইল-ফোল্ডারের তালিকা দেখুন। লক্ষ্য করুন যে, সেখানে autorun.inf নামে কোন ফাইল আছে না কি। যদি থাকে, তাহলে নিশ্চিতভাবে পেন ড্রাইভে ওয়ার্ম রয়েছে। এবার লক্ষ্য করুন আশ-পাশে কোন হিডেন ফাইল দেখা যায় কি না। হিডেন ফাইল-ফোল্ডারগুলো সাধারণ ফাইল-ফোল্ডারের তুলনায় আবছাভাবে প্রদর্শিত হয়। সাধারণভাবে পেন ড্রাইভের স্বত্বাধিকারীর জানা থাকার কথা তাঁর পেন ড্রাইভে কী কী ফাইল-ফোল্ডার রয়েছে। তাই সন্দেহজনক কোন ফাইল-ফোল্ডার (বিশেষত হিডেন অবস্থায়) পেলে সহজেই ধরে নেওয়া যায় যে, তা ওয়ার্ম ফাইল বা ফোল্ডার।

১০. autorun.inf সহ সেসব আবছাভাবে প্রদর্শিত ফাইল-ফোল্ডারগুলো সিলেক্ট করে Shift+Delete চাপুন। তাহলে সেগুলো রিসাইকেল বিনে জমা না হয়ে সরাসরি মুছে যাবে। সিলেক্ট করার সময় লক্ষ্য রাখবেন যেন exe এক্সটেনশন যুক্ত ওয়ার্ম ফাইলে ডাবল-ক্লিক পড়ে না যায়। তাহলে কিন্তু ওয়ার্ম পিসিকে আক্রমণ করে ফেলবে।

অনেক ক্ষেত্রেই দেখা যায় যে, Recycled নামে একটি হিডেন ফোল্ডার থাকে। এর ভিতর সাধারণত driveinfo.exe নামে একটি ওয়ার্ম ফাইল থাকে। সেক্ষেত্রে পুরো ফোল্ডারটিই মুছে ফেলতে হবে।

১১. এবার আরও লক্ষ্য করুন যে, এমন কোন ফাইল পাওয়া যায় কি না, যার আইকন ফোল্ডারের আইকনের মত, কিন্তু এক্সটেনশন exe । উল্লেখ্য, ফোল্ডারের কোন এক্সটেনশন থাকে না। সুতরাং, ফোল্ডারের আইকন সম্বলিত exe এক্সটেনশন যুক্ত ফাইল অবশ্যই ওয়ার্ম ফাইল। একইভাবে, টেক্সট ফাইলের আইকন সম্বলিত, অথচ txt এক্সটেনশনের পরিবর্তে exe এক্সটেনশন যুক্ত ফাইল; এবং ইমেজ ফাইলের আইকন সম্বলিত, অথচ jpeg, jpg, png, bmp বা gif ইত্যাদি এক্সটেনশনের পরিবর্তে exe এক্সটেনশন যুক্ত ফাইল নিঃসন্দেহে ওয়ার্ম ফাইল। এ সকল ফাইলও Shift+Delete চেপে মুছে ফেলুন।

চিত্র: বিভিন্ন ফাইল টাইপের আইকন সম্বলিত, অথচ exe এক্সটেনশন যুক্ত ওয়ার্ম ফাইল।



চিত্র: মূল ফোল্ডার ও ওয়ার্ম ফাইল।

১২. একটি বিশেষ ক্ষেত্রে দেখা যায় যে, পেন ড্রাইভে যেসব ফোল্ডার রয়েছে, সেগুলো হিডেন হয়ে গেছে এবং একই নামের কতগুলো ফাইল রয়েছে যেগুলো ফোল্ডারের আইকন সম্বলিত এবং exe এক্সটেনশন যুক্ত। পাশের চিত্রটি লক্ষ্য করুন। এখানে a, b ও c ফোল্ডারগুলো হল মূল ফোল্ডার এবং a.exe, b.exe ও c.exe হল ওয়ার্ম ফাইল। এক্ষেত্রে exe ফাইলগুলো মুছে ফেলুন। মূল ফোল্ডারগুলো স্বাভাবিক অবস্থায় ফিরিয়ে আনার জন্য ফোল্ডারগুলো সিলেক্ট করে Alt+Enter চাপুন। Hidden অপশনের পাশের চেক বক্স থেকে টিক চিহ্ন তুলে দিন। OK করুন। যদি স্ক্রীনে Confirm Attribute Changes নামে কোন ডায়ালগ বক্স আসে, তাহলে সেখান থেকে নিচের অপশনটি (Apply changes to this folder, subfolders and files) সিলেক্ট করে OK করুন।

চিত্র: হিডেন ফাইল/ফোল্ডারকে আনহাইড করার পদ্ধতি।

১৩. এবার সর্বশেষ আরেকটি বিষয় লক্ষ্য করুন। ধরুন, আপনার পেন ড্রাইভে a নামে কোন ফোল্ডার রয়েছে। a ফোল্ডারটিতে ডাবল-ক্লিক করুন। ভিতরে যদি a.exe নামে ফোল্ডারের আইকন সম্বলিত কোন ফাইল পান, তাহলে তা নিশ্চিতভাবে ওয়ার্ম ফাইল। অর্থাৎ, কোন ফোল্ডারের ভেতর যদি ঐ ফোল্ডারের নামে কোন exe ফাইল থাকে, যার আইকন ফোল্ডারের আইকনের মত, তাহলে ঐ exe ফাইলটি হল ওয়ার্ম ফাইল। এক্ষেত্রেও exe ফাইলটি Shift+Delete চেপে মুছে ফেলতে হবে। যদি পেন ড্রাইভের কোন একটি ফোল্ডারের ভিতর এরকম ফাইল পান, তাহলে বুঝতে হবে যে, বাকি ফোল্ডারগুলোর ভিতরেও এরকম ওয়ার্ম ফাইল রয়েছে। অতএব, প্রতিটি ফোল্ডারের ভেতর ঢুকে চেক করুন ঐ ফোল্ডারের ভিতর ঐ ফোল্ডারের নামে কোন exe ফাইল আছে কি না এবং থাকলে মুছে ফেলুন।

যদি পেন ড্রাইভে ফোল্ডারের সংখ্যা অত্যধিক হয়, তখন কী করবেন? একটি একটি করে চেক করতে তো সারা দিন লেগে যাবে। এর সমাধান ‘‘ওয়ার্ম প্রতিকারের উপায়’’ অনুচ্ছেদে পাওয়া যাবে।

ব্যস, পেন ড্রাইভ এখন ওয়ার্মমুক্ত। পেন ড্রাইভটি বের করে পুনরায় লাগান। এবার আপনি নিশ্চিন্তে ড্রাইভ আইকনে ডাবল-ক্লিক করতে পারেন।

ম্যালওয়্যার প্রতিকারের উপায়

ওয়ার্ম প্রতিকারের উপায়

“Example is better than precept” – উপদেশের চাইতে উদাহরণ উত্তম। ওয়ার্ম নির্মূল করার একটি গদবাঁধা নিয়ম বর্ণনা করার চেয়ে একটি নমুনা ওয়ার্ম কিভাবে দূর করতে হয়, তা দেখালে ওয়ার্ম বধ করার সাধারণ পদ্ধতি আয়ত্ত করতে সুবিধা হবে। যদি আপনি এ টিউটোরিয়ালটি পড়ার পাশাপাশি একটু নিজ হাতে প্র্যাকটিস করতে চান, তাহলে আপনি http://blog.sharafat.info/malware/worms.zip লিংক থেকে কিছু নমুনা ওয়ার্ম সংগ্রহ করতে পারেন।

ওয়ার্ম প্রতিকারের পূর্বে আমাদেরকে আগে নিশ্চিত হতে হবে পিসিটি ওয়ার্ম দ্বারা আদৌ আক্রান্ত হয়েছে কি না। নিচের পদ্ধতিতে আপনি নিশ্চিতভাবে বুঝতে পারবেন যে, আপনার পিসিতে ওয়ার্ম সক্রিয় অবস্থায় রয়েছে:

১. মাই কম্পিউটার আইকনে ডাবল-ক্লিক করার পর উইন্ডোর Tools মেনুতে যদি Folder Options নামে কোন অপশন না থাকে, তাহলে নিশ্চিতভাবে আপনার পিসিতে ওয়ার্ম রয়েছে।

২. যে কোন একটি ড্রাইভ আইকনে রাইট-ক্লিক করলে যদি পাশের চিত্রের মত কিছু উল্টাপাল্টা বর্ণ সম্বলিত মেনু দেখতে পান, তাহলেও নিশ্চিতভাবে আপনার পিসিতে ওয়ার্ম রয়েছে।

এবার, ওয়ার্ম নির্মূল করার জন্য আমাদেরকে অবশ্যই জানতে হবে তা কিভাবে কাজ করে। কোন ওয়ার্ম ফাইল রান করলে তা মেমরিতে (র‍্যামে) স্থান দখল করে। এরপর মেমরিতে বসে থেকে তা সকল ধ্বংসাত্মক কাজ পরিচালনা করে। ওয়ার্ম নির্মূল করার প্রথম ধাপ হল মেমরি থেকে তা মুছে ফেলা। কেননা, সে যদি মেমরিতে বসে থেকে দেখে যে, তার কোন প্রতিলিপি মুছে ফেলা হয়েছে, তাহলে সে তৎক্ষণাৎ তা পুনরায় তৈরি করে ফেলবে। একইভাবে, সে যে সকল সিস্টেম সেটিংস পরিবর্তন করেছে, সেগুলো যদি পূর্বের অবস্থায় ফিরে যেতে দেখে, তাহলে তৎক্ষণাৎ তা পুনরায় পরিবর্তন করে ফেলবে। সুতরাং, সে যাতে কোন অবস্থায়ই আপনার কাজ-কর্মের উপর নজর রাখতে না পারে, সেজন্য তাকে অবশ্যই মেমরি থেকে মুছে ফেলতে হবে। ওয়ার্ম আরেকটি কাজ করে থাকে। আর তা হল সিস্টেম স্টার্ট-আপে নিজেকে যুক্ত করে রাখা। এতে করে প্রতি বার উইন্ডোজ চালু হওয়ার সাথে সাথে তা চালু হয়ে যায়। সুতরাং, আপনার দ্বিতীয় কাজ হবে সিস্টেম স্টার্ট-আপ থেকে তাকে মুছে ফেলা। তৃতীয় কাজ হল ওয়ার্মটি যে সকল সিস্টেম সেটিংস পরিবর্তন করেছে, সে সকল সেটিংস পূর্বাবস্থায় ফিরিয়ে আনা। সর্বশেষ যে কাজটি আপনাকে করতে হবে, তা হল ওয়ার্মের মূল এক্সিকিউটেবল

ফাইল এবং তার প্রতিলিপিগুলো মুছে ফেলা, যাতে পরবর্তীতে ভুলক্রমে সেগুলোতে ডাবল-ক্লিক করার মাধ্যমে ওয়ার্মটি পুনরায় চালু হয়ে না যায়। পিসি থেকে ওয়ার্ম নির্মূল করার জন্য এ চারটি ধাপই অনুসরণ করতে হবে।

SSVICHOSST ওয়ার্ম নির্মূল করার পদ্ধতি

আমরা প্রথমে দেখব কিভাবে SSVICHOSST ওয়ার্মটিকে (যা সর্বাধিক প্রচলিত ওয়ার্ম) আক্রান্ত অবস্থা থেকে নির্মূল করা যায়। SSVICHOSST ওয়ার্মটি যে সকল কাজ করে, তা নিম্নরূপ (এখানকার কিছু কিছু বিষয় হয়ত আপনি বুঝতে পারবেন না। এতে চিন্তিত হওয়ার কিছু নেই। সব কিছুই বিস্তারিতভাবে বর্ণনা করা হবে):

১. প্রথম বার রান করালে মেমরিতে SSVICHOSST.exe নামে একটি প্রসেস চালু করে। পরবর্তীতে উইন্ডোজ রিস্টার্ট করলে মেমরিতে SSVICHOSST.exe নামে এক বা একাধিক প্রসেস চালু করে।

২. Tools মেনু থেকে Folder Options অপশনটি মুছে ফেলে, যাতে আপনি ওয়ার্মটির হিডেন ফাইলগুলো ডিটেক্ট করতে ও মুছে ফেলতে না পারেন।

৩. টাস্ক ম্যানেজার ও রেজিস্ট্রি এডিটর Disable করে দেয়, যাতে আপনি মেমরি থেকে SSVICHOSST.exe প্রসেসটি মুছে ফেলতে না পারেন।

৪. স্টার্ট-আপে SSVICHOSST নামে একটি এন্ট্রি তৈরি করে যা প্রতি বার উইন্ডোজ চালু হবার সাথে সাথে নিচের ৫ নম্বরে বর্ণিত ওয়ার্ম ফাইলটি রান করায়।

৫. C:\Windows\System32 ফোল্ডারে SSVICHOSST.exe নামে একটি ফাইল তৈরি করে যার সাইজ (সাধারণত) ২৩৪ কিলোবাইট, আইকন একটি ফোল্ডারের আইকনের মত, এবং তা হিডেন ও সিস্টেম ফাইল হিসেবে থাকে। এটিই ওয়ার্মটির কেন্দ্রীয় ফাইল হিসেবে সকল কাজ পরিচালনা করে। এছাড়াও C:\Windows ফোল্ডারে একই রকম SSVICHOSST.exe নামে একটি ফাইল তৈরি করে যার সাইজ পূর্বের ফাইলটির সাইজের সমান, আইকন একটি ফোল্ডারের আইকনের মত, কিন্তু তা হিডেন বা সিস্টেম ফাইল হিসেবে থাকে না।

৬. কোন ইউ.এস.বি. ডিভাইস (পেন ড্রাইভ) লাগানো হলে তার ভেতর Autorun.inf ও SSVICHOSST.exe নামে দুটি ফাইল তৈরি করে যেগুলো হিডেন ও সিস্টেম ফাইল হিসেবে থাকে। এছাড়াও New Folder.exe নামে আরেকটি ফাইল তৈরি করে যার সাইজ কেন্দ্রীয় SSVICHOSST.exe ফাইলের সাইজের সমান, আইকন একটি ফোল্ডারের আইকনের মত, কিন্তু তা হিডেন বা সিস্টেম ফাইল হিসেবে থাকে না। এরপর পেন ড্রাইভের প্রত্যেকটি ফোল্ডারের ভিতর সংশ্লিষ্ট ফোল্ডারের নামে একটি করে ফাইল তৈরি করে যার সাইজ হয় একইভাবে ঐ SSVICHOSST.exe ফাইলের সাইজের সমান, আইকন একটি ফোল্ডারের আইকনের মত, এবং তা হিডেন বা সিস্টেম ফাইল হিসেবে থাকে **না**। এতে করে যখন অন্য পিসিতে পেন ড্রাইভটি লাগানো হবে, তখন ব্যবহারকারী ভুলক্রমে এসব ফাইলের কোন না কোনটিতে ডাবল-ক্লিক করে বসবে এবং তার ফলে সেই পিসিতেও ওয়ার্মটি সক্রিয় হয়ে উঠবে। তাছাড়া পেন ড্রাইভটি লাগানোর পর ব্যবহারকারী যদি ড্রাইভ আইকনে ডাবল-ক্লিক করে, অথবা ড্রাইভ আইকনে রাইট-ক্লিক করে Autoplay বা Open মেনুতে ক্লিক করে, তাহলেও সেই পিসিতে ওয়ার্মটি সক্রিয় হয়ে উঠবে।

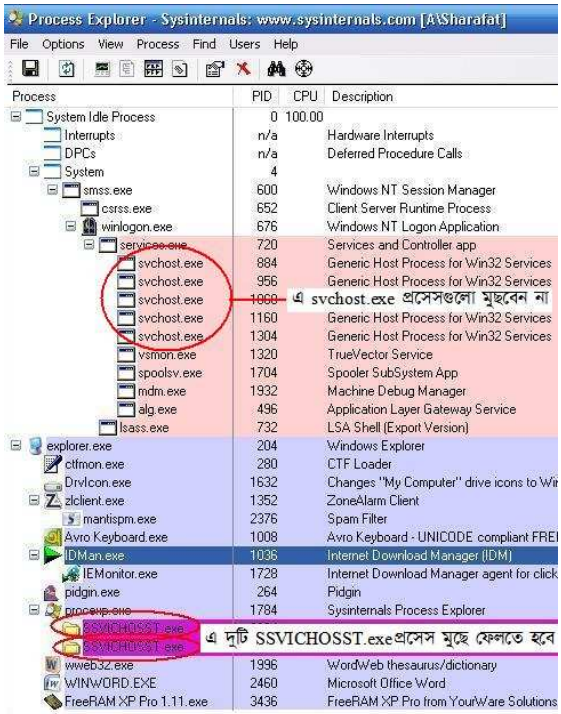
এবার দেখা যাক এ ওয়ার্মের বিরুদ্ধে কী ব্যবস্থা নেওয়া যায়।

১. প্রথমেই, মেমরি থেকে ওয়ার্মটিকে মুছে ফেলতে হবে। সেজন্য আপনার এমন একটি সফটওয়্যার দরকার যা মেমরিতে বর্তমানে যে সকল প্রসেস (তথা প্রোগ্রাম) চলছে, তার তালিকা দেখাবে। উইন্ডোজে এ ধরনের একটি সফটওয়্যার বিল্ট-ইন রয়েছে, যা টাস্ক ম্যানেজার নামে পরিচিত। এটি চালু করার জন্য Alt+Ctrl+Delete চাপতে হয়। এ টাস্ক ম্যানেজারে আপনি হয়ত SSVICHOSST.exe প্রসেসটিকে খুঁজে বের করে মুছে ফেলতে পারবেন, কিন্তু অজানা ম্যালওয়্যার

শিকার করার জন্য এর ইন্টারফেস ততটা সহায়ক নয়। তাছাড়া ওয়ার্ম সাধারণত টাস্ক ম্যানেজারকে ডিজেবল করে দেয়। ফলে আপনি Alt+Ctrl+Delete চাপলে আপনাকে একটি এরর বার্তা দেখাবে - "Task Manager has been disabled by your administrator."। সুতরাং, এক্ষেত্রে আপনাকে থার্ড পার্টি সফটওয়্যার ব্যবহার করতে হবে। এ ধরনের সফটওয়্যারের মধ্যে নিঃসন্দেহে সেরা হল Sysinternals কোম্পানীর Process Explorer । বিনামূল্যের এ প্রোগ্রামটি পাওয়া যাবে এ লিংকে:

http://www.filehippo.com/download_process_explorer/ ।

সফটওয়্যারটি (সাইজ ১.৫৫ মেগাবাইট) ডাউনলোড করে ডাবল-ক্লিক করুন। লাইসেন্স এগ্রিমেন্ট ডায়ালগ বক্স আসলে তাতে I Agree বোতামে ক্লিক করুন। ফলে প্রোগ্রাম উইন্ডো ওপেন হবে এবং আপনি সকল প্রসেসের তালিকা দেখতে পাবেন।

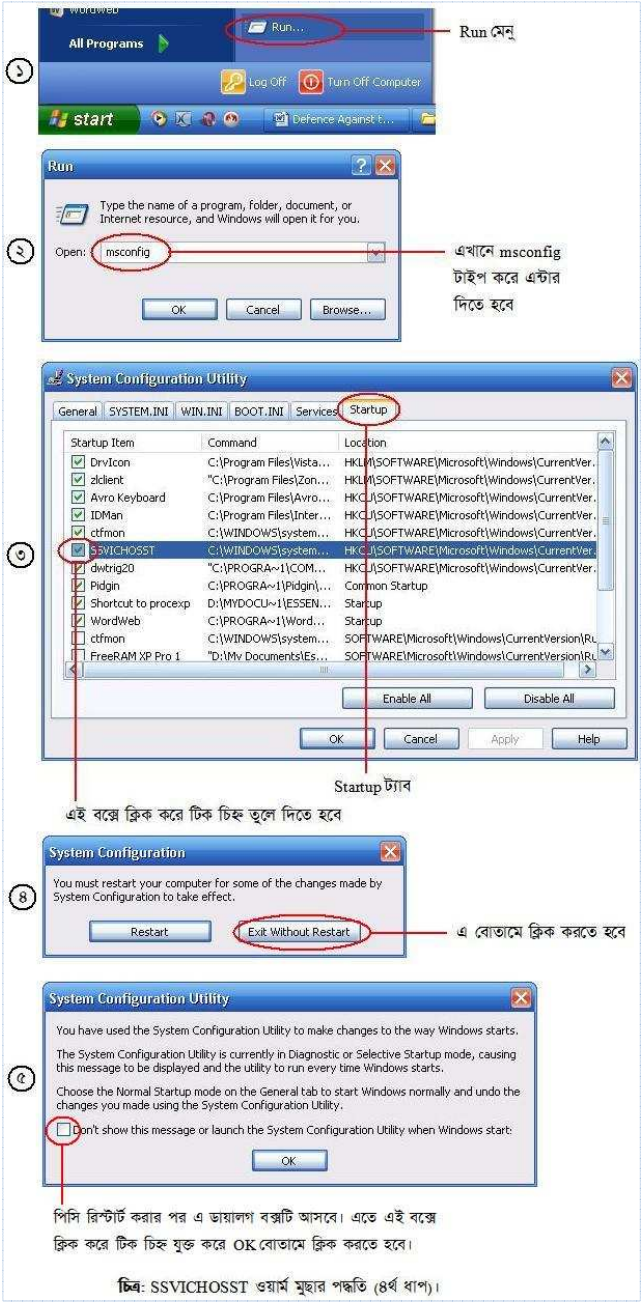


চিত্র: SSVICHOSST ওয়ার্ম মুছার পদ্ধতি (৩য় ধাপ)।

২. Process Explorer উইন্ডোর Options মেনু থেকে Confirm Kill-এর উপর ক্লিক করুন। এতে করে আপনি যখন কোন একটি প্রসেস মুছতে যাবেন, তখন তা "Are you sure you want to kill …?" – এ ধরনের বিরক্তিকর Confirmation Dialog দেখাবে না।

৩. প্রসেস এক্সপ্লোরার উইন্ডোতে SSVICHOSST.exe নামে যতগুলো প্রসেস পাবেন, সেগুলো একটি একটি করে সিলেক্ট করে Delete কী চাপুন। অর্থাৎ, প্রথমে একটি প্রসেস সিলেক্ট করে Delete কী চাপুন, এরপর আরেকটি প্রসেস সিলেক্ট করে Delete কী চাপুন, এভাবে সবগুলো প্রসেস মুছে ফেলুন। লক্ষ্য করুন: SSVICHOSST.exe প্রসেস মুছতে গিয়ে আবার svchost.exe প্রসেস মুছে ফেলবেন না যেন।

৪. মেমরি থেকে ওয়ার্মটি মুছে ফেলা শেষ। এবার স্টার্ট-আপ থেকে তা মুছতে হবে। স্টার্ট-আপ প্রোগ্রামের তালিকা দেখার জন্য উইন্ডোজে একটি বিল্ট-ইন সফটওয়্যার রয়েছে যার নাম System Configuration Utility । এটি চালু করার জন্য Start মেনুতে ক্লিক করে Run মেনুতে ক্লিক করুন। সেখানে টাইপ করুন msconfig এবং এন্টার দিন। সিস্টেম কনফিগারেশন ইউটিলিটির Startup ট্যাবে ক্লিক করুন। সেখানে সকল স্টার্ট-আপ প্রোগ্রামের তালিকা দেখা যাবে। এখান থেকে SSVICHOSST নামক এন্ট্রি খুঁজে বের করুন এবং তার পাশের চেক বক্সে ক্লিক করে টিক চিহ্ন তুলে দিন। OK বোতামে ক্লিক করুন। একটি মেসেজ আসবে যেখানে বলা হবে যে, আপনি যে সেটিংস পরিবর্তন করলেন, তা বাস্তবায়িত করার জন্য সিস্টেম রিস্টার্ট

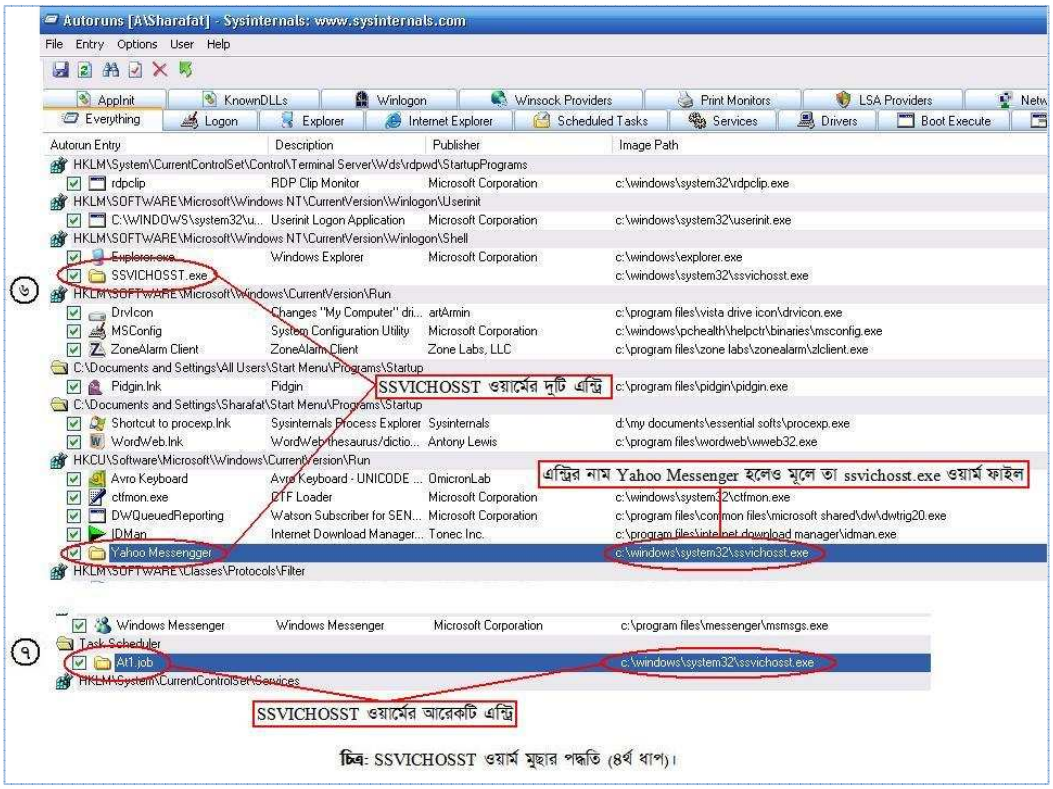


চিত্র: SSVICHOSST ওয়ার্ম মুছার পদ্ধতি (৪র্থ ধাপ)।

করতে হবে। আমাদের কাজ এখনও শেষ হয় নি। তাই Exit Without Restart বোতামে ক্লিক করুন। উল্লেখ্য, পরবর্তীতে সিস্টেম রিস্টার্ট করার পর আরেকটি ডায়ালগ বক্স আসবে। সেখানে "Don't show this message or launch the System Configuration Utility when Windows starts" নামে যে চেক বক্সটি থাকবে, তাতে ক্লিক করে টিক চিহ্ন যুক্ত করে OK বোতামে ক্লিক করতে হবে।

এখন, সিস্টেম কনফিগারেশন ইউটিলিটি দিয়ে আপনি হয়ত SSVICHOSST ওয়ার্মটিকে স্টার্ট-আপ থেকে মুছে ফেলতে পারলেন, কিন্তু অজানা ওয়ার্ম স্টার্ট-আপ থেকে মুছে ফেলার জন্য তা যথেষ্ট নয়। এক্ষেত্রেও সমাধান নিয়ে এসেছে Sysinternals কোম্পানী তাদের Autoruns নামক সফটওয়্যার তৈরি করে। বিনামূল্যের এ প্রোগ্রামটি পাওয়া যাবে এ লিংকে: http://www.filehippo.com/download_autoruns/। সফটওয়্যারটি ডাউনলোড করে (সাইজ ৪৮৫ কিলোবাইট) ডাবল-ক্লিক করুন। লাইসেন্স এগ্রিমেন্ট ডায়ালগ বক্স আসলে তাতে I Agree বোতামে ক্লিক করুন। ফলে প্রোগ্রাম উইন্ডো ওপেন হবে এবং আপনি সকল প্রসেসের তালিকা দেখতে পাবেন।

এখান থেকে SSVICHOSST.exe নামক এন্ট্রি খুঁজে বের করুন এবং Delete কী চাপুন। স্ক্রীনে "Are you sure you want to delete autorun of SSVICHOSST.exe?" উল্লেখ করে যে Confirmation Dialog আসবে, তার Yes বোতামে ক্লিক করুন (দুঃখজনকভাবে এ সফটওয়্যারে Process Explorer-এর মত এমন কোন অপশন নেই যাতে করে এ বিরক্তিকর ডায়ালগটি বন্ধ করে দেওয়া যায়)। একটু নিচেই দেখতে পাবেন Yahoo Messengger (মেসেঞ্জার বানানটি লক্ষ্য করুন – এতে একটি 'g' বর্ণ অতিরিক্ত রয়েছে। ম্যালওয়্যারের একটি সাধারণ বৈশিষ্ট্য হল তা এমন একটি প্রোগ্রামের নাম ধারণ করবে যা ব্যবহারকারীর অত্যন্ত পরিচিত, কিন্তু ঐ আসল প্রোগ্রামের সাথে পার্থক্য করার জন্য নামের বানানে অতি সূক্ষ্ম পরিবর্তন আনবে যাতে করে ব্যবহারকারী সহজে তা বুঝতে না পারে।) নামে একটি এন্ট্রি রয়েছে। এটিও ওয়ার্ম ফাইলের এন্ট্রি। কী করে বুঝা গেল? Image Path কলামে লক্ষ্য করুন - এন্ট্রির নাম Yahoo Messengger হলেও মূল ফাইলটি হল ওয়ার্ম ফাইল। এছাড়াও SSVICHOSST ওয়ার্মটির সাধারণ বৈশিষ্ট্য হল এর ফাইলগুলো ফোল্ডারের আইকন সম্বলিত হয়। এ এন্ট্রিটিও মুছে ফেলুন। এরপর স্ক্রল করে নিচের দিকে দেখুন যে, At1.job নামে এ ওয়ার্মের আরেকটি এন্ট্রি রয়েছে। এটিও মুছে ফেলুন। এবার একেবারে নিচ পর্যন্ত স্ক্রল করে দেখুন যে, ফোল্ডারের আইকন সম্বলিত কোন ধরনের এন্ট্রি পাওয়া যায় কি না। পাওয়া গেলে সেগুলোও মুছে ফেলুন। (লক্ষ্য করুন: পূর্বে বর্ণিত সিস্টেম কনফিগারেশন ইউটিলিটিতে কিন্তু এতগুলো এন্ট্রি কখনোই খুঁজে পেতেন না।) স্টার্ট-আপ থেকে ওয়ার্মের সকল এন্ট্রি মুছে ফেলার কাজ শেষ।



চিত্র: SSVICHOSST ওয়ার্ম মুছার পদ্ধতি (৪র্থ ধাপ)।

৫. এবার তৃতীয় কাজ। আর তা হল ওয়ার্মটি যে সকল সিস্টেম সেটিংস পরিবর্তন করেছে, সে সকল সেটিংস পূর্বাবস্থায় ফিরিয়ে আনা। এ সকল সিস্টেম সেটিংসের মধ্যে রয়েছে Folder Options ফিরিয়ে আনা এবং Task Manager ও Registry editor পুনরায় Enable করা।

রেজিস্ট্রি হল উইন্ডোজ অপারেটিং সিস্টেমের একটি মূল উপাদান। এতে উইন্ডোজের সকল তথ্যাবলী সংরক্ষণ করা হয়ে থাকে। রেজিস্ট্রি এডিটর সফটওয়্যারটি দিয়ে এ সকল তথ্যাবলী সম্পাদনা করা হয়। ওয়ার্ম ফাইলগুলো রেজিস্ট্রিতে নিজেদের কার্যবিবরণী সংরক্ষণ করে থাকে। সুতরাং, ব্যবহারকারী যাতে সেগুলো সম্পাদনা করতে বা মুছে ফেলতে না পারে, সেজন্য রেজিস্ট্রি এডিটরটি ডিজেবল করে দেয়। রেজিস্ট্রি এডিটর এনেবল করার বিভিন্ন উপায় রয়েছে। তন্মধ্যে সবচেয়ে সহজ উপায় হল একটি সেটআপ ইনফরমেশন ফাইল তৈরি করে তা ইন্সটল করা। এতে করে একবারে রেজিস্ট্রি এডিটর, টাস্ক ম্যানেজার এবং ফোল্ডার অপশনস – সবগুলোই পূর্বাবস্থায় ফিরে আসবে। সেটআপ ইনফরমেশন ফাইল তৈরি করার জন্য নিচের ধাপগুলো অনুসরণ করুন:

(১) Start মেনুতে ক্লিক করে All Programs → Accessories → Notepad –এ ক্লিক করুন।

(২) নিচের টেক্সটটি যে রকম স্পেস, বানান ইত্যাদি সহকারে আছে, সেখানে ঠিক সেভাবে টাইপ করুন (লক্ষ্য করুন – একই লাইনে পাশাপাশি দুটি বর্ণের মাঝে কোন স্পেস নেই।):

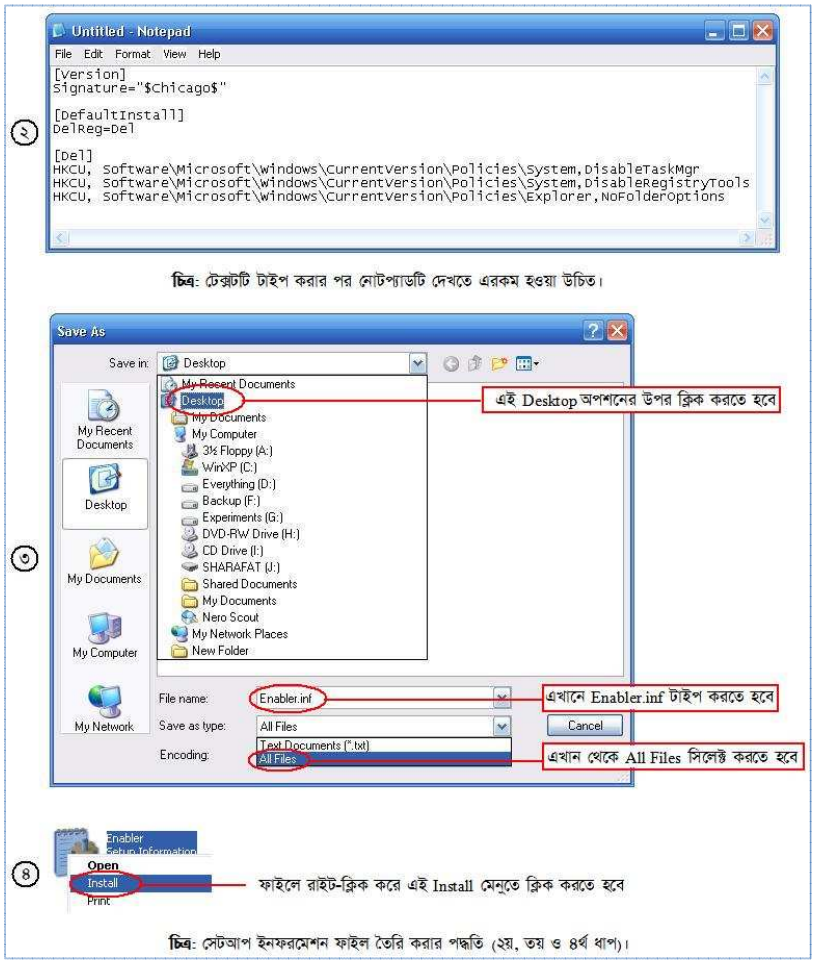
```
[Version]
Signature="$Chicago$"

[DefaultInstall]
DelReg=Del

[Del]
HKCU, Software\Microsoft\Windows\CurrentVersion\Policies\System,DisableTaskMgr
HKCU, Software\Microsoft\Windows\CurrentVersion\Policies\System,DisableRegistryTools
HKCU, Software\Microsoft\Windows\CurrentVersion\Policies\Explorer,NoFolderOptions
```

(৩) Ctrl+S চাপুন। Save As ডায়ালগ বক্সের File name -এ টাইপ করুন Enabler.inf । নিচে Save as type -এর ড্রপ-ডাউন কী-তে ক্লিক করে All Files সিলেক্ট করুন। ডায়ালগ বক্সের উপরের দিকে Save in -এর ড্রপ-ডাউন কী-তে ক্লিক করে Desktop সিলেক্ট করুন। Save বোতামে ক্লিক করুন।

(৪) ডেস্কটপে গিয়ে Enabler ফাইলটিতে রাইট-ক্লিক করে Install মেনুতে ক্লিক করুন। যদি "Installation failed." বার্তা নিয়ে কোন এরর মেসেজ আসে, তাহলে বুঝতে হবে যে, আপনি উপরের টেক্সটি টাইপ করতে কোথাও ভুল করেছেন। আর যদি কোন এরর মেসেজ না আসে, তবে আপনার ফাইলটি কাজ করেছে। এবার Alt+Ctrl+Delete



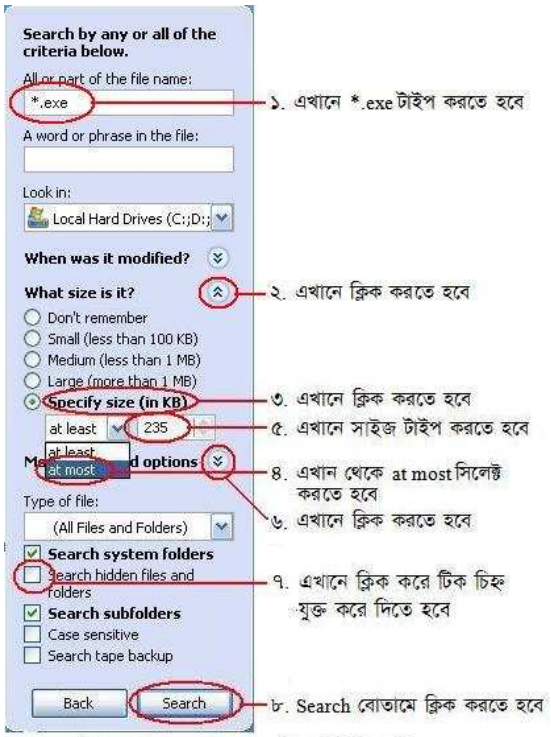
চিত্র: টেক্সটটি টাইপ করার পর নোটপ্যাডটি দেখতে এরকম হওয়া উচিত।

চিত্র: সেটআপ ইনফরমেশন ফাইল তৈরি করার পদ্ধতি (২য়, ৩য় ও ৪র্থ ধাপ)।

চাপুন। Task Manager চালু হবে। Folder Options এখনই ফিরে আসতে নাও পারে। সেক্ষেত্রে উইন্ডোজ রিস্টার্ট করলেই তা ফিরে আসবে।

৬. এবার সর্বশেষ কাজ। আর তা হল ওয়ার্মের মূল এক্সিকিউটেবল ফাইল এবং তার প্রতিলিপিগুলো মুছে ফেলা। আমরা পূর্বেই এ ওয়ার্মটির কার্যাবলীতে বর্ণনা করেছি যে, তা C:\Windows\System32 এবং C:\Windows\ ফোল্ডারে নিজের প্রতিলিপি তৈরি করে, যেগুলো কেন্দ্রীয় ফাইল হিসেবে কাজ করে। যেহেতু C:\Windows\System32 ফোল্ডারে অবস্থিত ফাইলটি হিডেন ও সিস্টেম ফাইল হিসেবে থাকে, তাই তা মুছার জন্য অবশ্যই হিডেন ও সিস্টেম ফাইল Show করার ব্যবস্থা থাকতে হবে। আপনি C: ড্রাইভে ডাবল-ক্লিক করুন। যদি দেখেন যে, সেখানে ntldr নামক কোন ফাইল দেখতে পাচ্ছেন, তাহলে বুঝা যাবে যে, হিডেন ও সিস্টেম ফাইল Show করার ব্যবস্থা রয়েছে। যদি এরকম নামের কোন ফাইল দেখতে না পারেন, তাহলে হিডেন ও সিস্টেম ফাইল Show করার ব্যবস্থা নেই। সেক্ষেত্রে পূর্বে ‘‘ওয়ার্ম প্রতিরোধের উপায়’’ অনুচ্ছেদে বর্ণিত নিয়মানুযায়ী Tools মেনু থেকে Folder Options-এ গিয়ে হিডেন ও সিস্টেম ফাইল Show করার ব্যবস্থা করতে হবে। যদি Tools মেনুতে Folder Options ইতোমধ্যে না এসে থাকে, তাহলে আপনাকে উইন্ডোজ রিস্টার্ট দিতে হবে। এজন্য Start মেনু থেকে Log Off বোতামে ক্লিক করুন। স্ক্রীনে আগত ‘Log Off Windows’ উইন্ডোর Log Off বোতামে ক্লিক করুন। এবার পুনরায় উইন্ডোজে লগ-ইন করুন। পূর্বে বর্ণিত উপায়ে ওয়ার্মটি সঠিকভাবে মুছতে সক্ষম হলে Tools মেনুতে Folder Options ফিরে আসবে। এবার সেখানে গিয়ে হিডেন ও সিস্টেম ফাইল Show করার ব্যবস্থা করুন।

এবার C:\Windows ফোল্ডারে চলে যান। সেখান থেকে SSVICHOSST ফাইলটি (লক্ষ্য করুন: আমি ফাইলের এক্সটেনশন উল্লেখ করছি না। আপনি যদি Folder Options-এ Hide extensions for known file types অপশনের বাম পাশের চেক বক্স থেকে টিক চিহ্ন তুলে দিয়ে থাকেন, তবে ফাইলের শেষে .exe নামে একটি এক্সটেনশন দেখতে পাবেন। যেহেতু আমি জানি না যে, আপনি এ অপশনটি কিভাবে সেট করে রেখেছেন, তাই আমি এখন থেকে ওয়ার্ম ফাইলের নাম বলার সময় এক্সটেনশন উল্লেখ করব না। কোন নতুন এক্সটেনশনের ফাইল উল্লেখ করলে মাত্র প্রথম উল্লেখেই আমি ফাইলটির এক্সটেনশন বলে দিব, কিন্তু পরবর্তীতে ঐ ফাইলটির রেফারেন্সে এক্সটেনশন উল্লেখ করব না।) খুঁজে বের করে Shift+Delete চেপে মুছে ফেলুন। এবার system32 ফোল্ডারের ভিতর গিয়ে একইভাবে SSVICHOSST ফাইলটি খুঁজে বের করে Shift+Delete চেপে মুছে ফেলুন।



চিত্র: SSVICHOSST ওয়ার্মের প্রতিলিপি সার্চ করা।

কেন্দ্রীয় ফাইল মুছার কাজ শেষ। এবার ওয়ার্মটির প্রতিলিপিগুলো মুছার পালা। সম্পূর্ণ হার্ড ডিস্ক জুড়ে এ ওয়ার্ম ফাইলটি থাকতে পারে। তাই সমগ্র হার্ড ডিস্কে একটি সার্চ দিতে হবে। এজন্য Start মেনু থেকে Search মেনুতে ক্লিক করুন। All files and folders –এ ক্লিক করুন। All or part of the file name –এ টাইপ করুন *.exe । *.exe দ্বারা বুঝানো হচ্ছে যে, কেবল exe এক্সটেনশন যুক্ত ফাইলের তালিকা আমরা চাচ্ছি। নিচের দিকে What size is it? –এর ডান পাশের তীর চিহ্নতে ক্লিক করুন। নিচের Specify size (in KB) –এ ক্লিক করুন। তার ঠিক নিচের অপশন থেকে at most –এ ক্লিক করুন। ডান পাশের বক্সের 0 মুছে সেখানে টাইপ করুন কেন্দ্রীয় SSVICHOSST.exe ফাইলের সাইজ + ১। অধিকাংশ ক্ষেত্রেই দেখা যায় যে, SSVICHOSST.exe ফাইলের সাইজ হয় 234 কিলোবাইট (ফাইল সাইজ দেখার জন্য ফাইলটিতে রাইট-ক্লিক করে Properties মেনুতে ক্লিক করুন)। সুতরাং, এক্ষেত্রে সার্চের সময় বক্সটিতে টাইপ করতে হবে (234+1) বা 235 । যদি আপনি এমন কোন SSVICHOSST.exe ফাইল পান যার সাইজ ধরুন 428 কিলোবাইট হয়,

তাহলে উক্ত বক্সটিতে টাইপ করবেন 429 । ফাইল সাইজ নির্দিষ্ট করে দেওয়ার মাধ্যমে আমরা সার্চ ফাংশনটিকে বুঝাতে চাচ্ছি যে, আমরা সর্বোচ্চ (at most) এত কিলোবাইট ফাইল চাচ্ছি। এবার Search বোতামে ক্লিক করুন।

সার্চ শেষ হলে ডান দিকের প্যানেলে লক্ষ্য করুন। এখান থেকে Size কলামের হেডিংয়ের উপর একবার ক্লিক করুন। কিছুক্ষণ অপেক্ষা করুন। দেখবেন যে, সাইজের উচ্চক্রমানুসারে (১, ২, ৩, ...) পুরো তালিকাটি সাজানো হয়ে গেছে। এবার ঐ কলামের হেডিংয়ের উপরে আবারও ক্লিক করুন ও কিছুক্ষণ অপেক্ষা করুন। দেখবেন যে, সাইজের নিম্নক্রমানুসারে (২৩৫, ২৩৪, ২৩৩, ...) পুরো তালিকাটি সাজানো হয়ে গেছে। এবার Name কলামের অধীনের ফাইলগুলো লক্ষ্য করুন। যতগুলো ফাইলের আইকন ফোল্ডারের আইকনের মত পাবেন (যদি আদৌ থাকে), সবগুলো সিলেক্ট করে Shift+Delete চাপুন। ফোল্ডারের আইকন ছাড়াও কয়েকটি ফাইলের আইকন পাশের চিত্রের মত হতে পারে। আপনি যদি নিশ্চিত হন যে, ফাইলগুলো আপনার কোন প্রয়োজনীয় প্রোগ্রামের ফাইল নয় (নিশ্চিত হওয়ার জন্য In Folder কলাম থেকে ঐ ফাইলটির পাথ দেখুন এবং নিশ্চিত করুন যে, ঐ স্থান বা পাথে এরকম কোন exe ফাইল থাকার কোন সম্ভাবনা আছে কি না), তাহলে সেগুলোও Shift+Delete চেপে মুছে ফেলুন। এবার পুনরায় সার্চ দিয়ে একইভাবে তালিকাটি নিম্নক্রমানুসারে সাজান। লক্ষ্য করুন যে, Name কলামের অধীনে ফোল্ডারের আইকন যুক্ত কোন ফাইল রয়ে গেছে কি না। যখন নিশ্চিত হবেন যে, এরকম আর কোন ফাইল নেই, তখন বুঝা যাবে যে, হার্ড ডিস্ক থেকে এ ওয়ার্মটি পুরোপুরি দূর হয়ে গেছে। এখন পেন ড্রাইভ চেক করতে হবে। এজন্য পেন ড্রাইভের আইকনে রাইট-ক্লিক করে সেখান থেকে Search… অপশনে ক্লিক করুন। বাকি কাজ উপরে বর্ণিত সার্চের পদ্ধতির মতই।

কাজ শেষ। উপরে বর্ণিত কার্যাবলী সঠিক এবং সফলভাবে করে থাকলে আপনার পিসি এবং ইউ.এস.বি. ডিভাইস এখন পুরোপুরি SSVICHOSST ওয়ার্মমুক্ত।

আপনার কাছে মনে হতে পারে কাজটি বেশ জটিল এবং সময় সাপেক্ষ। কিন্তু বিশ্বাস করুন আর নাই করুন, সার্চ দেওয়ার আগ পর্যন্ত কাজ সম্পন্ন করতে আমার সময় লাগে সর্বোচ্চ দুই মিনিট। আর সার্চের সময় নির্ভর করে আপনার হার্ড ডিস্ক বা পেন ড্রাইভে থাকা ফাইলের সংখার উপর। ফাইলের সংখ্যা যত বেশি হবে, সার্চের সময় তত বেশি লাগবে। যা হোক, আপনি এ কাজটি যত বেশি চর্চা করবেন, কাজটি সম্পন্ন করতে আপনার সময় তত কম লাগবে।

RavMon ওয়ার্ম নির্মূল করার পদ্ধতি

আমরা আরেকটি জনপ্রিয় (!) তথা অধিক প্রচলিত ওয়ার্ম নির্মূল করার পদ্ধতি দেখব। কেননা, এটি পূর্বেরটি থেকে সামান্য ভিন্ন।

RavMon ওয়ার্ম যে সকল কাজ করে, তা নিম্নরূপ:

১. মেমরিতে Ravmon.exe নামে একটি প্রসেস চালু করে। এই প্রসেসটি C:\Windows ফোল্ডারের ভিতর MDM.EXE, SVCHOST.EXE ও SVCHOST.INI নামে তিনটি ফাইল তৈরি করে, যেগুলো ওয়ার্মটির কেন্দ্রীয় ফাইল হিসেবে কাজ করে। এরপর এ প্রসেসটি SVCHOST.EXE ওয়ার্ম ফাইলটিকে রান করায়। ফলে মেমরিতে SVCHOST.EXE নামে একটি প্রসেস চালু হয় এবং পূর্বের Ravmon.exe প্রসেসটি মেমরি থেকে মুছে যায়।

২. SVCHOST.EXE প্রসেসটি সিস্টেম স্টার্ট-আপে SVCHOST নামে একটি এন্ট্রি তৈরি করে, যার ফলে প্রতি বার উইন্ডোজ চালু হবার সাথে সাথে MDM.EXE ওয়ার্ম ফাইলটি চালু হবে।

৩. ওয়ার্মটি কিছু রেজিস্ট্রি এন্ট্রি মডিফাই করে, যার ফলে সবগুলো হিডেন ফাইল প্রদর্শিত অবস্থা থেকে হিডেন হয়ে যায়। আপনি Tools মেনু থেকে Folder Options-এ গিয়ে Show hidden files and folders অপশনটি সিলেক্ট করে দিলেও কোন হিডেন ফাইল প্রদর্শিত হবে না।

৪. ইউ.এস.বি. ড্রাইভ সহ প্রতিটি ড্রাইভের রুটে (ড্রাইভের Root মানে হচ্ছে ড্রাইভের ঠিক ভিতরে, ড্রাইভের ভিতর অবস্থিত কোন ফোল্ডারের ভিতরে নয়) Autorun.inf ও RavMon.exe নামে দুটি ফাইল তৈরি করে, যার ফলে ড্রাইভ আইকনে ডাবল-ক্লিক করা মাত্রই ওয়ার্ম ফাইলটি চালু হয়ে যায়।

এবার দেখা যাক এ ওয়ার্মের বিরুদ্ধে কী ব্যবস্থা নেওয়া যায়।

১. প্রথমেই, মেমরি থেকে ওয়ার্মটিকে মুছে ফেলতে হবে। Process Explorer চালু করে সেখানে SVCHOST.EXE নামক যতগুলো প্রসেস পাওয়া যাবে, সবগুলো মুছে ফেলুন।

২. সিস্টেম স্টার্ট-আপ থেকে ওয়ার্মটিকে মুছে ফেলার জন্য Autoruns চালু করুন। সেখানে SVCHOST নামক যে এন্ট্রিটি পাবেন, তা মুছে ফেলুন।

৩. এবার সিস্টেম সেটিংস পূর্বাবস্থায় ফিরিয়ে আনতে হবে। এক্ষেত্রে আপনাকে সরাসরি রেজিস্ট্রি এন্ট্রি মডিফাই করতে হবে। (সতর্কতা: রেজিস্ট্রি উইন্ডোজ অপারেটিং সিস্টেমের একটি মূল অংশ। এর কিছু গুরুত্বপূর্ণ এন্ট্রি যদি ভুলক্রমে পরিবর্তন করে ফেলা হয়, তাহলে উইন্ডোজ আর চালু হবে না। তাই, এখানে যে সকল এন্ট্রি পরিবর্তন করতে বলা হবে, কেবল সে সকল এন্ট্রিই পরিবর্তন করবেন। না জেনে অন্য কোন এন্ট্রি নিয়ে গবেষণা করতে না যাওয়াই ভাল।[2])

রেজিস্ট্রি এডিট করার জন্য আপনাকে রেজিস্ট্রি এডিটর ব্যবহার করতে হবে। নিচের ধাপগুলো অনুসরণ করুন:

(১) Start মেনু থেকে Run-এ ক্লিক করুন।

(২) regedit টাইপ করে এন্টার দিন।

(৩) এবার বাম দিকের প্যানেল থেকে HKEY_LOCAL_MACHINE –এর উপর ডাবল-ক্লিক করুন।

(৪) HKEY_LOCAL_MACHINE –এর অধীনের এন্ট্রিগুলো থেকে SOFTWARE –এ ডাবল-ক্লিক করুন।

(৫) এভাবে Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden –এ যান।

(৬) Hidden –এর অধীনের এন্ট্রি দুটি থেকে SHOWALL –এ ক্লিক করুন।

(৭) ডান দিকের প্যানেল থেকে CheckedValue নামক এন্ট্রিটি সিলেক্ট করে Delete কী চাপুন। Confirmation মেসেজ বক্স থেকে Yes বোতামে ক্লিক করুন।

(৮) এবার ডান দিকের প্যানেলে ফাঁকা স্থানে রাইট-ক্লিক করে New মেনু থেকে DWORD Value সিলেক্ট করুন।

(৯) এন্ট্রিটির নাম হিসেবে CheckedValue টাইপ করে এন্টার দিন।

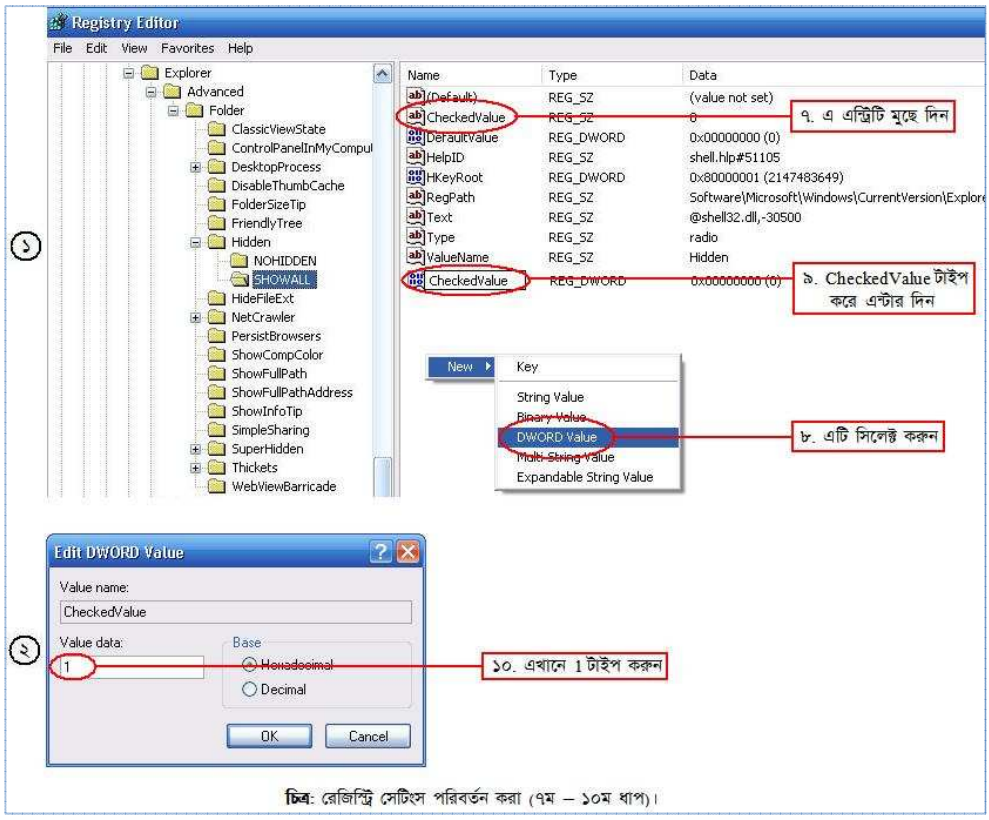
---

[2] আপনি যদি কখনো কোথাও টিপ্স্ জাতীয় লেখা পড়ে থাকেন যেখানে রেজিস্ট্রি নিয়ে কাজ করার কথা বলা হয়েছে, তাহলে লক্ষ্য করলে দেখতে পাবেন যে, সেখানে শুরুতেই স্পষ্টভাবে বলে দেওয়া হয়েছে যে, রেজিস্ট্রি নিয়ে কাজ করার সময় সাবধান এবং কাজ করার পূর্বে অবশ্যই রেজিস্ট্রি ব্যাক-আপ করে রাখুন। আমি বলি, যদি শুরুতেই এরকম ভয় দেখানো হয়, তাহলে সাধারণ ইউজাররা তো কখনোই রেজিস্ট্রি এডিট করতে চাইবেন না। আর ভয় পেয়ে কাজ করা থেকে বিরত থাকলে কিছু শেখা যাবে না। সুতরাং, যেমনটি আমি বলেছি, বর্ণিত এন্ট্রি ছাড়া রেজিস্ট্রির অন্য কোন এন্ট্রি না জেনে পরিবর্তন করবেন না (যদি আপনি একান্তই ভয় পেয়ে থাকেন এবং নিজের থেকে কোন গবেষণা করতে না চান)। যেভাবে রেজিস্ট্রি এডিটিংয়ের বর্ণনা দেওয়া হয়েছে, অন্তত সেভাবে কাজ করার ক্ষেত্রে ভয় পাওয়ার কোন কারণ নেই। আর যদি একান্তই রেজিস্ট্রি এডিটিংয়ের বর্ণনা সঠিকভাবে অনুসরণ করা সত্ত্বেও কিছু গোলমাল করে ফেলেন যার ফলে আপনাকে নতুন করে উইন্ডোজ সেটআপ করতে হয় (সম্ভাবনা ১% মাত্র), তাহলে কি আর করা। না হয় দু-একবার ঝামেলা হলোই। সেটাও তো এক ধরনের অভিজ্ঞতা 😉।

(১০) এন্ট্রিটিতে ডাবল-ক্লিক করে Value data টেক্সট বক্সের অন্তর্গত 0 মুছে দিয়ে সেখানে 1 টাইপ করুন।

রেজিস্ট্রি এডিটরের কাজ শেষ। এডিটর উইন্ডো Close করে দিন।

৪. এবার ওয়ার্ম ফাইলগুলো মুছে ফেলতে হবে। এক বার লগ অফ করে পুনরায় লগ অন করুন। Tools মেনু থেকে Folder Options-এ গিয়ে সকল হিডেন ও সিস্টেম ফাইল Show করার ব্যবস্থা করুন। এবার ডেস্কটপ থেকে My Computer –এ রাইট-ক্লিক করুন। মেনু থেকে Explore সিলেক্ট করুন। বাম দিকের প্যানেল থেকে C: ড্রাইভের আইকনে ক্লিক করুন। এবার ডান দিকের প্যানেলে Autorun ও RavMon নামক দুটি ফাইল খুঁজে বের করে Shift+Delete চেপে মুছে ফেলুন। ইউ.এস.বি. ড্রাইভ সহ বাকি সকল ড্রাইভের জন্য এটি Repeat করুন। এবার C:\Windows ফোল্ডারে গিয়ে MDM.EXE, SVCHOST.EXE ও SVCHOST.INI নামক ফাইগুলো Shift+Delete চেপে মুছে ফেলুন।

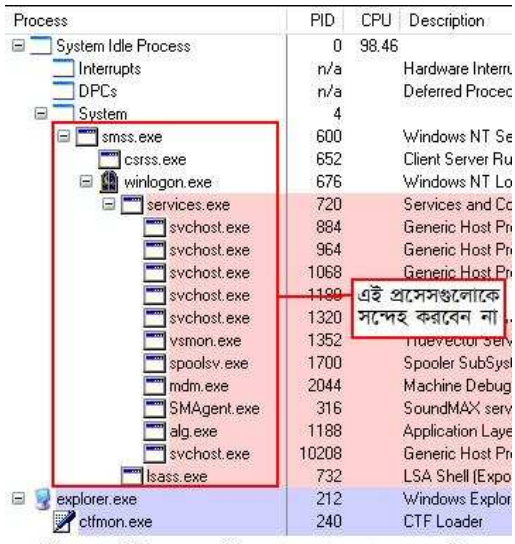


চিত্র: রেজিস্ট্রি সেটিংস পরিবর্তন করা (৭ম – ১০ম ধাপ)।

উপরে বর্ণিত কার্যাবলী সঠিক এবং সফলভাবে করে থাকলে আপনার পিসি এবং ইউ.এস.বি. ডিভাইস এখন পুরোপুরি RavMon ওয়ার্মমুক্ত।

অজানা ওয়ার্ম শিকার করার পদ্ধতি ও টিপ্‌স্‌

সক্রিয় ওয়ার্ম ডিটেক্ট করার জন্য পূর্বে দুটি উপায় বর্ণনা করা হয়েছে (Folder Options –এর অস্তিত্ব ও ড্রাইভের আইকনে রাইট-ক্লিক করে আগত মেনুতে উল্টাপাল্টা বর্ণের অস্তিত্ব পর্যবেক্ষণ করা)। কিন্তু সেগুলো হল সক্রিয় ওয়ার্মের অস্তিত্ব ডিটেক্টের **নিশ্চিত** পদ্ধতি। ওগুলো যদি ঠিকঠাক অবস্থায় পাওয়া যায়, তার মানে এই না যে, পিসিতে কোন সক্রিয় ওয়ার্ম নেই। এ ধরনের ওয়ার্ম ডিটেক্ট করার পদ্ধতি কী? জবাব – Process Explorer এবং Autoruns । সক্রিয় ওয়ার্ম সাধারণত এক বা একাধিক প্রসেস চালু রাখে। সুতরাং, অপরিচিত কোন প্রসেস দেখলে সেটিকে সন্দেহ করা যেতে পারে (যদিও নিশ্চিতভাবে বলা যাবে না যে, সেটি কোন ওয়ার্মেরই প্রসেস)। এখন, আপনি কিভাবে বুঝবেন যে, অপরিচিত প্রসেসটি কোন ম্যালওয়্যারের কি না? কয়েকটি উপায় নিম্নরূপ:

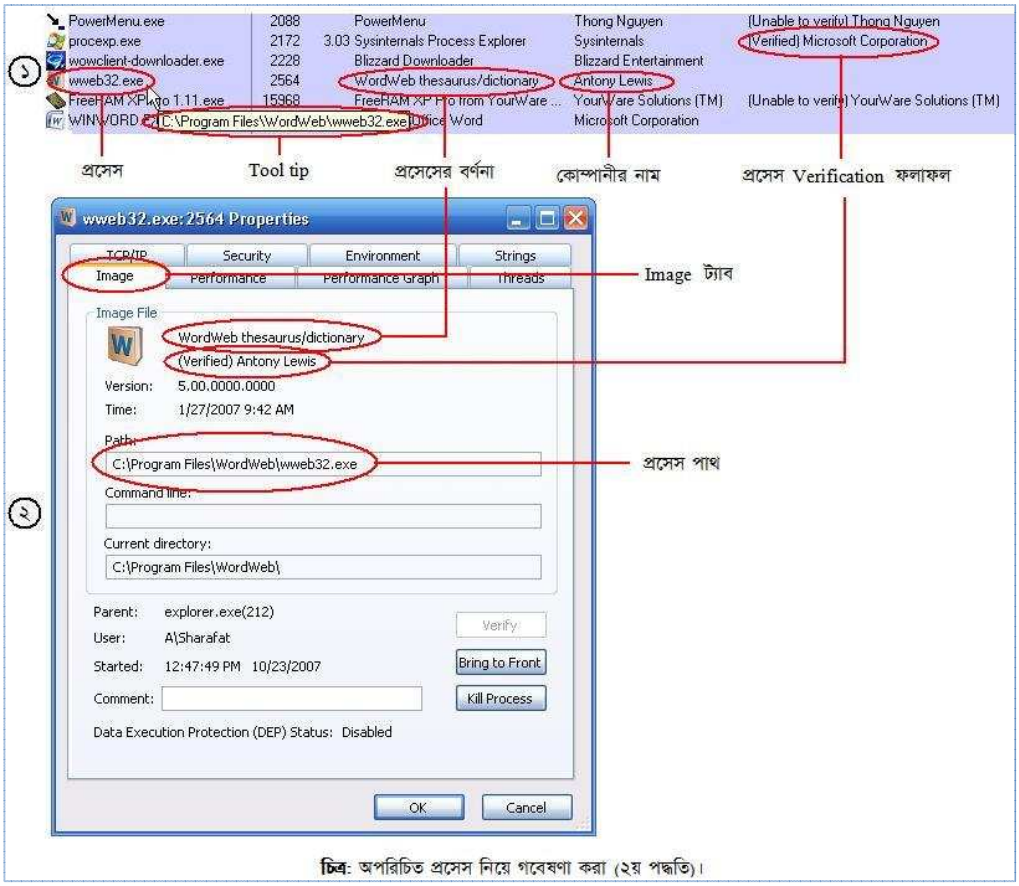


চিত্র: অপরিচিত প্রসেস নিয়ে গবেষণা করা (১ম পদ্ধতি)।

(১) System গ্রুপের অধীনে যে সকল প্রসেস রয়েছে, সেগুলো ম্যালওয়্যার প্রসেস হওয়ার সম্ভাবনা খুবই ক্ষীণ। তাই সেগুলোকে সন্দেহ করা থেকে দূরে থাকুন। যদি System গ্রুপের অধীনে কোন ম্যালওয়্যার থেকেও থাকে, তাহলেও তা ডিটেক্ট করতে পারবে কেবল সফটওয়্যার, উইন্ডোজ ও

ম্যালওয়্যার সম্পর্কে অত্যন্ত অভিজ্ঞ ও দক্ষ কম্পিউটার ব্যবহারকারীগণ; সাধারণ ব্যবহারকারীগণ তা সহজে ডিটেক্ট করতে পারবেন না।

(২) প্রসেসটির নামের উপর কিছুক্ষণ মাউস পয়েন্টার ধরে রাখুন। এতে প্রসেসটি কোন্ পাথ থেকে রান হচ্ছে, তা Tooltip আকারে দেখাবে। এ পাথটি পর্যবেক্ষণ করে দেখুন, প্রসেসটি আপনার ইন্সটলকৃত কোন সফটওয়্যার কর্তৃক চলছে কি না। উদাহরণস্বরূপ পাশের চিত্রটি লক্ষ্য করুন। Process Explorer –এ wweb32.exe নামক প্রসেসটি ওয়ার্ম প্রসেস কি না, তা জানার জন্য তার উপর মাউস ধরা হল। ফলে নিচে Tooltip হিসেবে প্রসেসটির পাথ দেখা যাবে। পাথটিতে WordWeb নামক একটি ফোল্ডারের নাম দেখা যাচ্ছে। আমি জানি যে, WordWeb নামক একটি সফটওয়্যার আমি ইন্সটল করেছি। সুতরাং, এক্ষেত্রে আমি নিশ্চিত যে, প্রসেসটি এ প্রোগ্রামেরই একটি প্রসেস। অতএব, তা ম্যালওয়্যার নয়।



চিত্র: অপরিচিত প্রসেস নিয়ে গবেষণা করা (২য় পদ্ধতি)।

আবার, লক্ষ্য করুন – wweb32.exe প্রসেসটির পাশে তার বর্ণনা (WordWeb thesaurus/dictionary) এবং কোম্পানীর নাম (Antony Lewis) দেখা যাচ্ছে। (উল্লেখ্য, আপনার Process Explorer উইন্ডোতে এগুলো দেখা নাও যেতে পারে। Process Explorer উইন্ডোর View মেনু থেকে Select Columns… অপশনে গিয়ে Process Image ট্যাব থেকে Description, Company Name এবং Verified Signer –এর বাম পাশের চেক বক্সগুলো টিক চিহ্নযুক্ত করে দিলে এগুলো দেখা যাবে। অথবা প্রসেসটির উপর ডাবল-ক্লিক করলে যে ডায়ালগ বক্স আসবে, সেখান থেকেও এ তথ্যগুলো দেখতে পারবেন।) ম্যালওয়্যার প্রসেসের বর্ণনা বা কোম্পানীর নাম সাধারণত থাকে না, অথবা থাকলেও তা কিছু উল্টাপাল্টা বর্ণের সমন্বয়ে গঠিত নাম হয়।

আবার, প্রসেসটি যদি নিশ্চিতভাবে ম্যালওয়্যার **না** হয়, তাহলে তা Verified দেখাবে। ম্যালওয়্যার প্রসেস কখনো Verified দেখাবে না। কিন্তু তার মানে এই নয় যে, সকল Unverified প্রসেসই ম্যালওয়্যার। উল্লেখ্য, প্রসেস Verify করার জন্য আপনার পিসিতে ইন্টারনেট সংযোগ থাকতে হবে।

এছাড়াও, আপনি যদি কোন প্রসেস সম্পর্কে জানতে চান যে, ঐ প্রসেসের কাজ কী; অথবা কোন প্রসেসকে ম্যালওয়্যার প্রসেস হিসেবে সন্দেহ করে থাকেন, কিন্তু সে ব্যাপারে আপনি পুরোপুরি নিশ্চিত হতে না পারেন, তাহলে সোজা www.processlibrary.com –এ ব্রাউজ করুন। সেখানে আপনি একটি প্রসেসের নাম উল্লেখ করে সার্চ করলে ঐ প্রসেসটি সম্পর্কে যাবতীয় তথ্য পেয়ে যাবেন (যদি থাকে)। তাছাড়া সেখানে আপনার পিসিতে সক্রিয় সকল প্রসেস অনলাইনে থেকে স্ক্যান করার ব্যবস্থা রয়েছে, অর্থাৎ, স্ক্যান শেষে আপনার সকল প্রসেসের তালিকা এবং সেই সাথে তাদের বর্ণনা (যদি থাকে)

আপনি দেখতে পারবেন। তারপরও যদি কোন প্রসেস সম্পর্কে আপনার কোন জিজ্ঞাসা থাকে, তাহলে সেখানে একটি ফোরাম রয়েছে – সেখানে আপনি আপনার প্রশ্ন উত্থাপন করবেন এবং অন্যান্য যারা ঐ প্রসেসটি সম্পর্কে জানে, তারা সেটার জবাব দেওয়ার চেষ্টা করবে।

বিশেষভাবে উল্লেখ্য যে, কোন প্রসেসের পাথ যদি C:\WINDOWS\Temp অথবা C:\Documents and Settings*%UserName%*\Local Settings\Temp (*%UserName%* দ্বারা User Account Name বুঝানো হচ্ছে। অর্থাৎ, আপনি যদি Mr. X নামে কোন ইউজার অ্যাকাউন্ট তৈরি করে থাকেন, তাহলে *%UserName%* -এর স্থলে Mr. X ধরতে হবে।) হয়, তাহলে নিশ্চিতভাবে প্রসেসটি একটি ম্যালওয়্যার প্রসেস।

আবার, smss.exe, csrss.exe, winlogon.exe, lsass.exe, svchost.exe, services.exe, userinit.exe ইত্যাদি সিস্টেম প্রসেসগুলো সর্বদা C:\Windows\System32 পাথ থেকে রান করে। যদি এ প্রসেসগুলোর কোনটি অন্য কোন পাথ থেকে (এমনকি C:\Windows\ পাথ থেকে হলেও) রান করে, তাহলেও নিশ্চিতভাবে প্রসেসটি ম্যালওয়্যার প্রসেস।

কোন প্রসেসের পাথ C:\Windows হলে প্রসেসটি সন্দেহযুক্ত। কেননা, ব্যবহারকারী যে সকল সফটওয়্যার ইন্সটল করে থাকে, সেগুলো বিশেষ কোন কারণ ছাড়া কখনো C:\Windows থেকে Run করে না।

আপনি যখন নিশ্চিত হবেন যে, প্রসেসটি একটি ম্যালওয়্যার প্রসেস, তখন আপনি তার পাথটি (অর্থাৎ, প্রসেসটি কোথা থেকে রান করছে তা) দেখে নিন। প্রথমে প্রসেসটি মুছে ফেলুন। এরপর তার পাথে গিয়ে প্রসেস ফাইলটি মুছে ফেলুন। উদাহরণস্বরূপ, ধরুন উপরে বর্ণিত wweb32.exe প্রসেসটি সম্পর্কে আপনি নিশ্চিত হলেন যে, তা একটি ম্যালওয়্যার প্রসেস। এখন, আপনি প্রথমে তা মুছে ফেলুন এবং এরপর তার পাথে (C:\Program Files\WordWeb) গিয়ে প্রসেস ফাইলটি (wweb32.exe) মুছে ফেলুন। এবার নিচের ৩ নম্বর পদ্ধতি অনুসরণ করে সিস্টেম স্টার্ট-আপ থেকে প্রসেসটির এন্ট্রি (যদি থাকে) মুছে ফেলুন।

(৩) কিছু কিছু ম্যালওয়্যার রয়েছে যেগুলো উইন্ডোজ চালু হবার সাথে সাথে এক বা একাধিক প্রসেস চালু করে এবং নিমেষেই আবার চলে যায়। এই সামান্য সময়ের মধ্যেই তাদের কাজ সমাধা হয়ে যায়। যেহেতু পরবর্তীতে এ প্রসেসগুলো আর থাকে না, তাই Process Explorer ব্যবাহার করলেও আপনি এ ম্যালওয়্যারগুলো ডিটেক্ট করতে পারবেন না। আপনি যদি এমন কোন ব্যবস্থা করতে পারেন যে, উইন্ডোজ চালু হবার সাথে সাথে Process Explorer চালু হবে, তাহলে অতি সামান্য সময়ের জন্য আপনি প্রসেসগুলো চালু অবস্থায় দেখতে পারবেন। এখন, যেহেতু প্রসেসগুলো উইন্ডোজ চালু হবার সাথে সাথে চালু হয়, সুতরাং, সেগুলোর এন্ট্রি অবশ্যই সিস্টেম স্টার্ট-আপে থাকবে। Autoruns সফটওয়্যারটি ব্যবহার করে ঐ প্রসেসগুলোর পাথ দেখে নিন। এবার ঐ পাথে গিয়ে প্রসেসটির ফাইল মুছে দিন এবং Autoruns থেকেও তাদের এন্ট্রি মুছে ফেলুন।

সতর্কতা: কিছু সিস্টেম প্রসেস যেমন, userinit.exe ইত্যাদি উইন্ডোজ চালু হবার সাথে সাথে চালু হয়ে কিছুক্ষণ পর আবার চলে যায়। তাই বলে এটি কিন্তু ম্যালওয়্যার প্রসেস নয়। এই প্রসেসটির মূল ফাইল মুছে দিলে উইন্ডোজ আর চালু হবে না। কাজেই, এ ধরনের প্রসেস নিয়ে সাবধানে গবেষণা করবেন।[3] আর নিচে কয়েকটি এন্ট্রি পাথসহ দেখানো হয়েছে; সেগুলোকে কখনো সন্দেহ করবেন না। কেননা, সেগুলো সিস্টেম প্রসেস। তবে হ্যাঁ, যদি এমন কোন এন্ট্রি পাওয়া যায় যার নাম নিচের কোন এন্ট্রির নামের মত, কিন্তু পাথ ঐ এন্ট্রির মত নয়, তাহলে ঐ এন্ট্রিটি অবশ্যই ম্যালওয়্যার প্রসেসের এন্ট্রি।

[3] সত্যি কথা বলতে কি, গবেষণা করতে গেলে কয়েকবার উইন্ডোজ রি-ইন্সটল বা আপগ্রেড করতেই হয়। উইন্ডোজ রি-ইন্সটল করার ভয়ে যদি আপনি গবেষণা করা থেকে বিরত থাকেন, তাহলে অনেক কিছুই জানতে বা শিখতে পারবেন না।

এন্ট্রি	পাথ
rdpclip	c:\windows\system32\rdpclip.exe
userinit.exe	c:\windows\system32\userinit.exe
Explorer.exe	c:\windows\explorer.exe
logonui.exe	c:\windows\system32\logonui.exe

আবার, ম্যালওয়্যার প্রসেসের এন্ট্রির Description বা Company Name সাধারণত থাকে না, অথবা থাকলেও তা কিছু উল্টাপাল্টা বর্ণের সমন্বয়ে গঠিত হয়। সুতরাং, এ ধরনের কোন এন্ট্রি পেলে তা অবশ্যই সন্দেহযুক্ত (তবে উপযুক্ত প্রমাণ ছাড়া নিশ্চিতভাবে বলা যাবে না যে, তা ম্যালওয়্যার ফাইলের এন্ট্রি)।

একইভাবে, যেমনটি Process Explorer –এর ক্ষেত্রে বর্ণনা করা হয়েছে, Autoruns –এ কোন এন্ট্রির পাথ যদি C:\WINDOWS\Temp অথবা C:\Documents and Settings*%UserName%*\Local Settings\Temp হয়, তাহলে নিশ্চিতভাবে এন্ট্রিটি একটি ম্যালওয়্যার ফাইলের এন্ট্রি।

অজানা ম্যালওয়্যার শিকার করার আরো কিছু পদ্ধতি রয়েছে, তবে সেগুলো অ্যাডভান্সড ইউজারদের জন্য। যাঁরা সেগুলো জানতে আগ্রহী, তাঁরা এ লিংক থেকে Advanced Malware Cleaning নামক প্রেজেন্টেশন ফাইলটি ডাউনলোড করে দেখতে পারেন: http://blog.sharafat.info/malware/AdvancedMalwareCleaning.zip

এখানে একটি বিষয় বিশেষভাবে উল্লেখযোগ্য – যদি আপনি দেখেন যে, Tools মেনু থেকে Folder Options –এ গেলে বা Alt+Ctrl+Delete চাপলে বা Process Explorer রান করলে সিস্টেম রিস্টার্ট হয়ে যাচ্ছে, তাহলে নিশ্চিতভাবে বুঝতে পারবেন যে, সিস্টেম ব্রন্টক ওয়ার্ম দ্বারা আক্রান্ত হয়েছে। আমার দৃষ্টিতে সকল ওয়ার্মের মধ্যে ব্রন্টক নির্মূল করা সবচেয়ে কঠিন। তাছাড়া ব্রন্টকের বিভিন্ন ভ্যারিয়েশন থাকায় এবং একেক ভ্যারিয়েশনের নির্মূলকরণ পদ্ধতি একেক রকম হওয়ায় সাধারণ ব্যবহারকারীগণ সহজে এ ওয়ার্ম নির্মূল করতে পারবেন না। ব্রন্টক দূর করার জন্য আমার নিম্নোল্লিখিত ই-মেইল অ্যাড্রেসে যোগাযোগ করুন।

[বি. দ্র.: আপনি এ প্রবন্ধের কোন অংশ বুঝতে না পারলে বা এখানে উল্লেখিত কোন প্রক্রিয়া সম্পন্ন করতে গিয়ে কোন সমস্যায় পড়লে, অথবা ভাইরাস সম্পর্কিত আপনার যে কোন প্রশ্ন থাকলে অনুগ্রহপূর্বক আমার ই-মেইলে যোগাযোগ করুন:

শারাফাত ইবনে মোল্লা মোশাররফ
sharafat_8271@yahoo.co.uk
www.sharafat.info]