

## মেইনটেইনিং একসেস

### মেইনটেইনিং একসেস

মেইনটেইনিং একসেস হলো আপনি যখন একবার সিস্টেম এ লগিন করতে পেরেছেন সেহেতু রেগুলার ফলোআপ করা। আবার সেই সিস্টেম এর অন্য কোন সার্ভিসকে নিজের হাতে নিয়ে আসা।

অর্থাৎ আপনি যখন কোন সিস্টেমে কোন ম্যালওয়ার ইন্সটল করতে পারবেন। তখন আপনি সিস্টেমে যেকোন যায়গা থেকে মেইনটেইন করতে পারবেন।

এখন কথা হচ্ছে কিভাবে মেইনটেইন করবো?

মেইনটেইন করার জন্য যেকোন একটি ম্যালওয়ার ইন্সটল করে দিতে হবে। বিভিন্ন ধরনের ম্যালওয়ার রয়েছে। তাদের মধ্যে উল্লেখযোগ্য হলো-

১. ট্রোজান হর্স
২. ভাইরাস
৩. স্পাইওয়ার
৪. ডিস্ট্রিবিউটেড ডেনিয়াল অফ সার্ভিস
৫. র্যানসমওয়ার
৬. ওয়্যাম ইত্যাদি

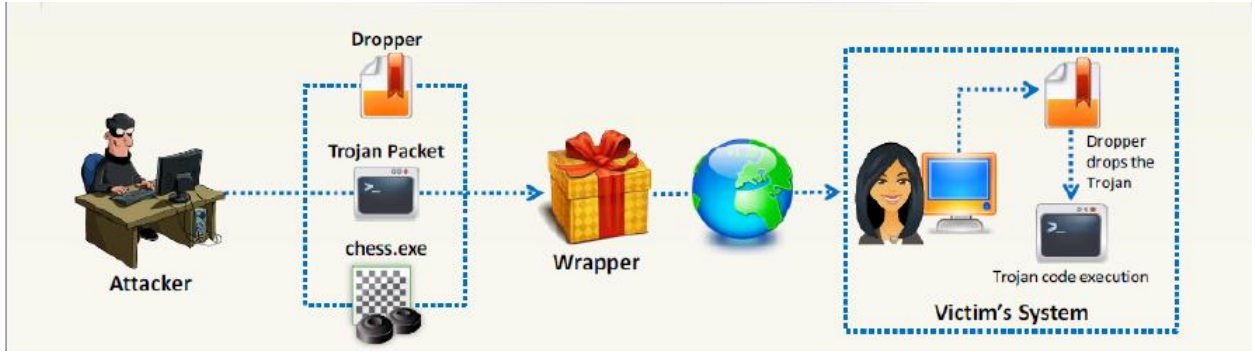
১. ট্রোজান হর্স

ট্রোজান হর্স খুবই ভয়ানক একটি ম্যালওয়্যার। এই ম্যালওয়্যারটি দেখে, আপনার মনে হবে প্রয়োজনীয় কোন এপ্লিকেশন। কিন্তু ম্যালওয়্যারটি আপনার সিস্টেমে প্রবেশ করে সকল ডিভাইসে ছড়িয়ে পরে।

কিভাবে ট্রোজান হর্স আক্রমণ করে?

১. ফায়ারওয়াল এবং এন্টিভাইরাস এগুলো নিষ্ক্রিয় করে দেয়।
২. ব্যাকডোর তৈরি করে রিমুটলি একসেস করার জন্য।
৩. পাসওয়ার্ড, ক্রেডিট কার্ড ইত্যাদি তথ্যগুলো সংগ্রহ করে।
৪. আক্রান্ত পিসির একটিভিটিসগুলো রেকর্ড করে সেন্ড করে।

যেভাবে ট্রোজান হর্স কাজ করে?

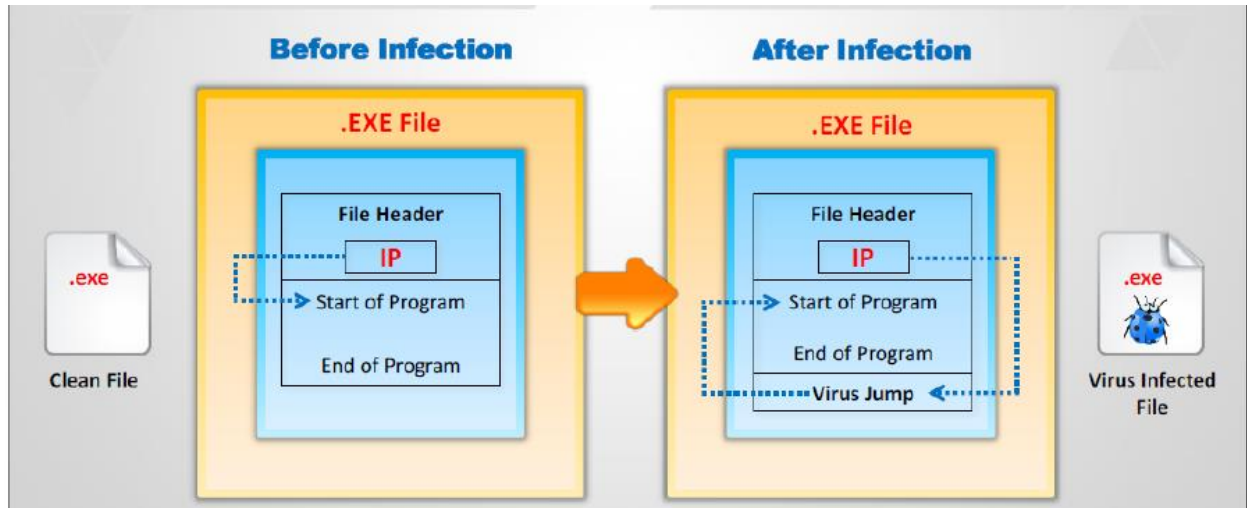


## ২. ভাইরাস

ভাইরাস হলো একটি প্রোগ্রাম। যা একটি সিস্টেম এর ফাইলগুলোকে নষ্ট করে দেয় অথবা নিজেই সিস্টেম ফাইল এর পরিবর্তে অবস্থান করে। সাধারণত যে লক্ষণগুলো দেখা যায়-

- অটোমেটিক্যালি এন্টিভাইরাস ডিসেবলড
- হার্ডডিস্ক এর ফ্রি স্পেস শেষ হয়ে যাওয়া
- অটোমেটিক্যালি মাউস ক্লিক

ভাইরাস যেভাবে কাজ করে-

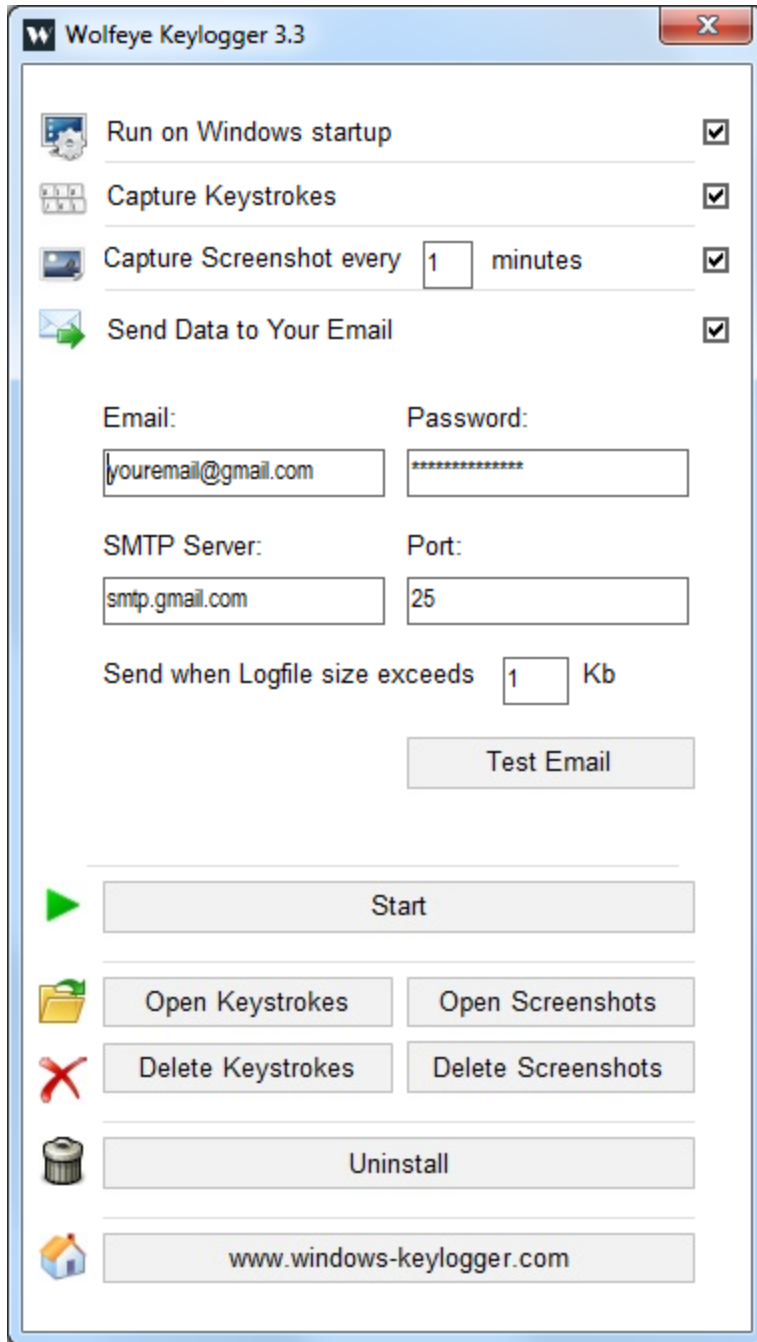


কিভাবে ভাইরাস দূর করা যাবে?

- এন্টিভাইরাস ব্যবহার করতে হবে এবং নিয়মিত স্ক্যান করতে হবে।
- ফোল্ডার অপশন এর হিডেন চেক করতে হবে।
- অপরিচিত কোন সাইট থেকে কোন কিছু ডাউনলোড বন্ধ করতে হবে।

### ৩. স্পাইওয়্যার

স্পাইওয়্যার এমন এক ধরনের ম্যালওয়্যার যা অনুমতি ছাড়াই সিস্টেম এ প্রবেশ করে, সাথে সাথে গোপন তথ্যসমূহ(ইউজার নেইম, পাসওয়ার্ড) ট্রান্সফার করা শুরু করে।

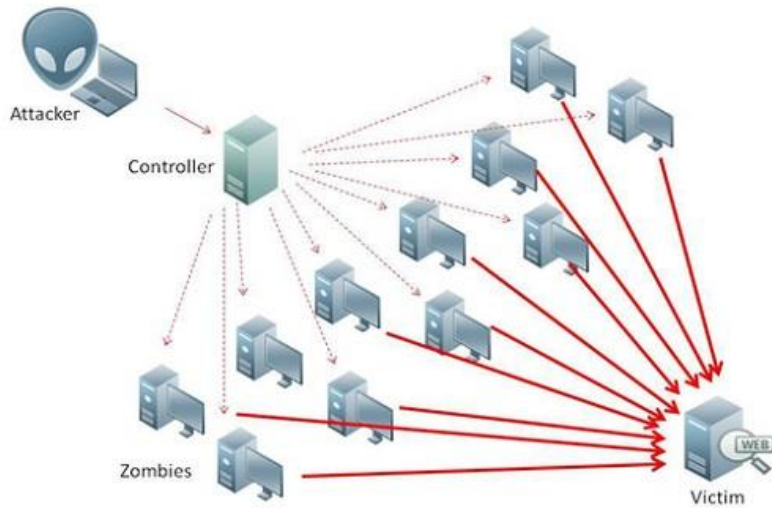


কিভাবে স্পাইওয়্যার থেকে সিস্টেমকে রক্ষা করা যায়?

১. পপ-আপস গুলে ক্লিক করতে হবে।
২. আপডেট এন্টিভাইরাস ব্যবহার করতে হবে।
৩. একসেসপ্ট এ ক্লিক করার পূর্বে অবশ্যই এগ্রিমেন্টগুলো ভাল করে পড়ে নিতে হবে।

## ৪. ডিস্ট্রিবিউটেড ডেনিয়াল অফ সার্ভিস

ডিস্ট্রিবিউটেড ডেনিয়াল অফ সার্ভিস আক্রমণের মাধ্যমে যেকোন সিস্টেম এর সব ব্যান্ডউইদ শেষ করে সিস্টেমকে ডাউন করে দেওয়া হয়।



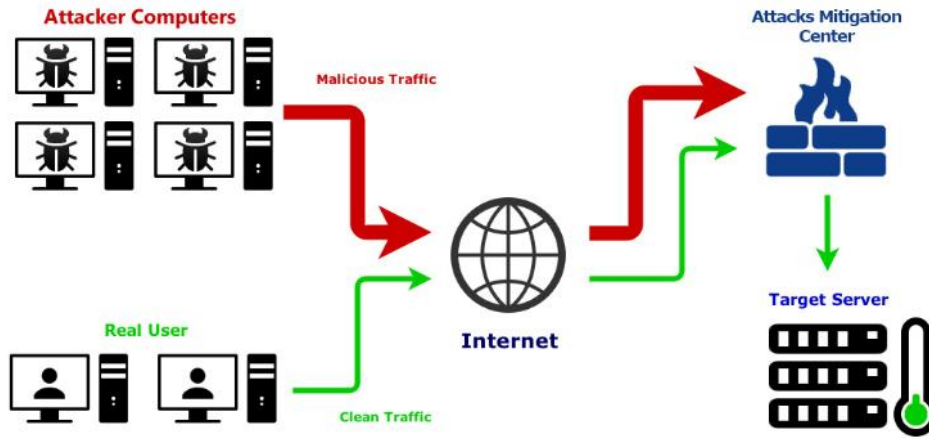
ইহা যেভাবে হয়ে থাকে-

- টিসিপি সিন ফ্লাড
- আইসিএমপি ফ্লাড
- উডিপি ফ্লাড
- এআরপি ফ্লাড
- এইচটিটিপি ফ্লাড ইত্যাদি

কিভাবে সিস্টেমকে ডিস্ট্রিবিউটেড ডেনিয়াল অফ সার্ভিস থেকে রক্ষা করা যায়?

- রেইট লিমিট করে রাখতে হবে।
- আইপি এ্যাড্রেস ভেরিফিকেশন

- এন্টি ডিস্ট্রিবিউটেড ডেনিয়াল অফ সার্ভিস শিল্ড ব্যবহার করতে হবে।



র‍্যানসমওয়ার হ‍ল একটি ধরনের ম‍্যালওয়ার যা আপনার কম্পিউটারের ফাইলগুলি এনক্রিপ্ট করে এবং ফাইলগুলির জন্য ব্যবহারকারীকে মূল্য প্রদানের দাবি করে।



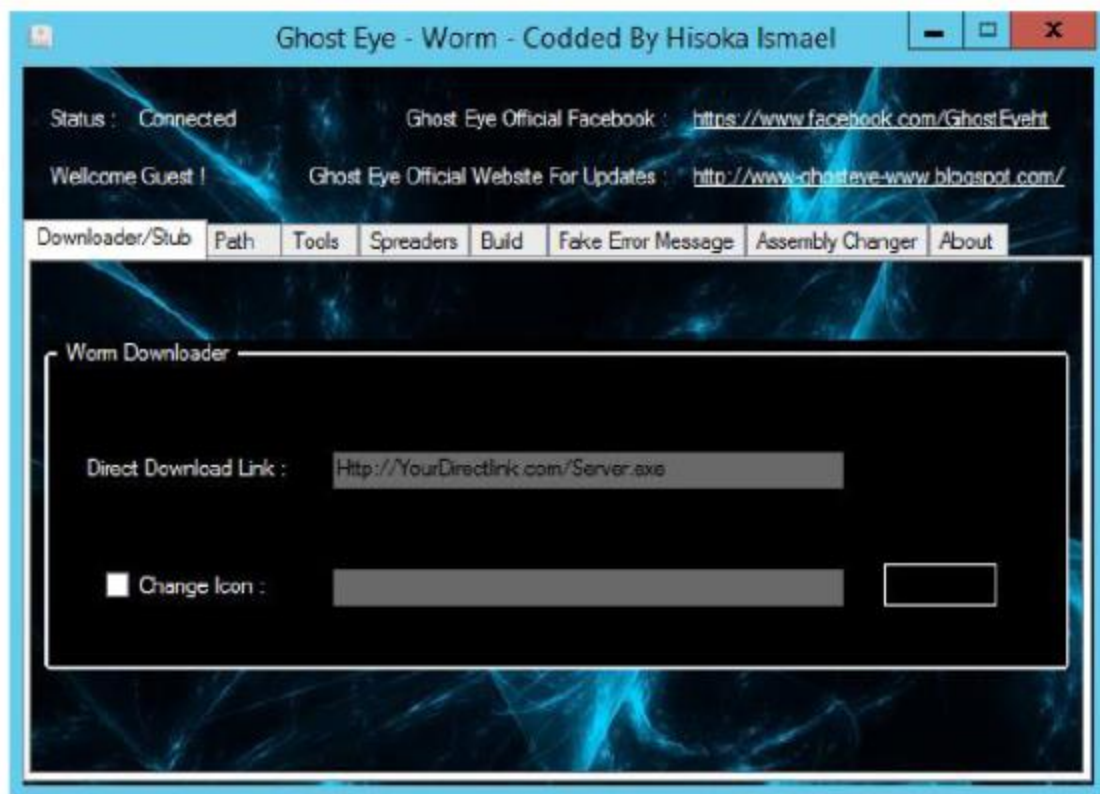
র‍্যানসমওয়ার যেভাবে আক্রমণ করে এই ধরনের একটি ফাইল সেভ করবে। যা রান করানোর সাথে সাথে আপনার সিস্টেম এর সকল ফাইল/ফোল্ডারগুলো এনক্রিপ্ট হয়ে যাবে।

কিভাবে র‍্যানসমওয়ার থেকে সিস্টেমকে রক্ষা করা যায়?

- কোন ইমেইল এর সংযুক্তি খোলার আগে নিশ্চিত করুন যে অনুমোদিত প্রেরক থেকে এসেছে
- মালওয়ার নজরদারির জন্য ওপেন সোর্স টুল সেটআপ করুন।
- সফটওয়ার প্যাচ আপডেট করতে হবে।
- সফটওয়ার ইনস্টলেশন সীমাবদ্ধতা নীতি স্থাপন করতে হবে।
- নিয়মিত ব্যাকআপ নেওয়ার প্র্যাকটিস করতে হবে।

ওয়ার্ম

ওয়ার্ম হলো এমন এক ধরনের ম্যালওয়ার যা এক্সিউট ফাইলকে রি-প্লেইস করে নেটওয়ার্কে ছড়িয়ে পরে। যেমন-Ghost eye worm এপ্লিকেশন। এই এ্যাপ্লিকেশন এর মাধ্যমে র্যানডম ম্যাসেজ নেটওয়ার্কে এ পাঠানো যায়।



কিভাবে ওয়ার্ম থেকে সিস্টেমকে রক্ষা করা যায়?

বিভিন্ন ধরনের এ্যাপ্লিকেশন রয়েছে যেগুলো দিয়ে ওয়ার্ম ডিটেক্ট করা যায়। ডিটেক্ট করে তারপর ব্লক করতে হবে।