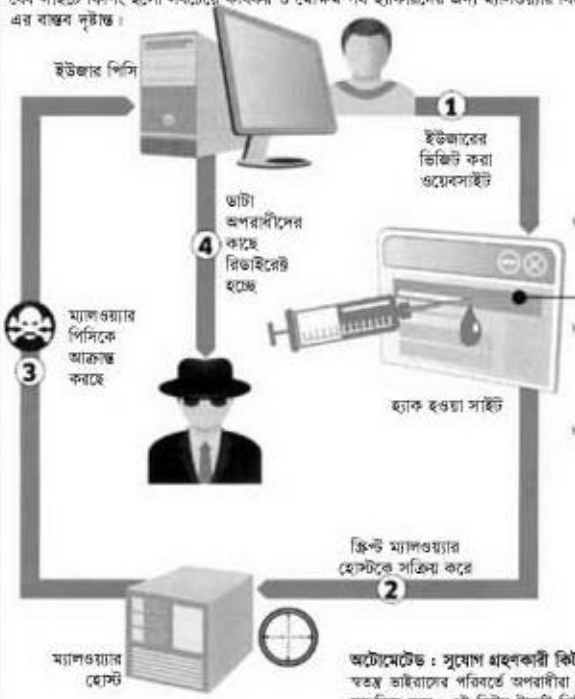
বিভিন্ন ধরনের ভাইরাস থেকে পরিত্রাণের উপায়

তাসনীম মাহমুদ

কমপিউটার জগৎ-এর নিয়মিত বিভাগ ব্যবহারকারীর পাতায় সাধারণত ব্যবহারকারীদের উদ্দেশে দৈনন্দিন কমপিউটিং জীবনধারায় বিভিন্ন প্রয়োজনীয় বিষয়ের আলোকে লেখা উপস্থাপন করা হয়, যার বেশিরভাগই উইন্ডোজ বা বিভিন্ন ধরনের অ্যাপ্লিকেশন প্রোগ্রাম বা পিসির বিভিন্ন ধরনের সাধারণ সমস্যার সমাধানের আলোকে। কিন্তু এবারের ব্যবহারকারীর পাতায় উপস্থাপন করা হয়েছে পিসি যেভাবে বিভিন্ন ধরনের এবং বিভিন্ন পদ্ধতিতে ভাইরাসে সংক্রমিত হয় এবং যেভাবে ভাইরাস থেকে প্রতিকার বা রক্ষা পাওয়া যায় তার উপায় ও কৌশল নিয়ে। কেননা এমন কোনো ব্যবহারকারীই খুঁজে পাওয়া যাবে না, যিনি ভাইরাস যন্ত্রণায় জর্জরিত হননি কখনই। অবশ্য কমপিউটার জগৎ-এর আরেকটি নিয়মিত বিভাগ রয়েছে, যা 'সিকিউরিটি' হিসেবে পরিচিত, যেখানে সাধারণত আলোচনা করা হয় ভাইরাস প্রতিরোধে বিভিন্ন ধরনের টুলের বৈশিষ্ট্য বা ফিচার নিয়ে। লেখাটি মূলত ব্যবহারকারীর পাতায় উপস্থাপন করা হয়েছে এ কারণে যে, ভাইরাস সমস্যা এখন সর্বজনীন এবং তা থেকে রক্ষা পাওয়ার জন্য রয়েছে কিছু সাধারণ কৌশল, যা সব ব্যবহারকারীকেই মেনে চলতে হয় তাদের সিস্টেমের সুরক্ষার জন্য। 'প্রতিরোধই প্রতিকারের সেরা উপায়'–এ প্রবাদবাক্যটি এখন

অনলাইন : ক্ষতিকর ওয়েবসাইটের মাধ্যমে ডাটা চুরি

বৈধ সাইটে ফিশিং হলো সবচেয়ে কার্যকর ও মোক্ষম পথ হ্যাকারদের জন্য ম্যালওয়্যার বিস্তারের। লেনোভো, টমটম এবং ইউএস ফাইন্যান্স মিনিস্ট্রি এর বাস্তব দৃষ্টান্ত।



ইনফেক্টেড : হ্যাকার ম্যানিপুলেট ওয়েবসাইট
হ্যাকার কোড চুরি করে তিন ধরনের বৈধ ওয়েবসাইটে যাতে সেগুলো ম্যালওয়্যার হোস্টের সাথে যুক্ত হতে পারে।

রিডাইরেক্ট : সবচেয়ে সহজ পদ্ধতি। এইচটিএমএল কোড ভিজিটরদের সরাসরি রিডাইরেক্ট করে ক্লোন করা ম্যালওয়্যার হোস্টে, যা নিম্নরূপ দেখা যায় : <meta http-equiv="refresh" content=0;url=http://www.malware.com">

আইফ্রেম : ওয়েবসাইটের ভেতরে ওয়েবসাইটের মতো অদৃশ্য iframe ফাংশন যা ইউজারকে না জানিয়ে লোড হয়। আইফ্রেম উপাদান সরাসরি টার্গেট ওয়েবসাইটে রেফার করে।

জাভাস্ক্রিপ্ট : হ্যাক সাইটে জাভাস্ক্রিপ্ট কোড অ্যামবেড্ড করা তুলনামূলকভাবে কঠিন, কেননা সিকিউরিটি পরিমাপ করা অত্যন্ত উন্নত হয়েছে। বেশিরভাগ সময়ে এই কোড কনসিল্ড থাকে।

অটোমেটেড : সুযোগ গ্রহণকারী কিটস পিসিতে অ্যাক্সেস করছে
স্বতন্ত্র ভাইরাসের পরিবর্তে অপরাধীরা এখন তৈরি করছে সুযোগের সদ্ব্যবহারকারী কিটস যা প্রসেসকে স্বয়ংক্রিয় করে। এই কিটস টার্গেট পিসিকে আক্রান্ত করে স্বয়ংক্রিয়ভাবে। এই আক্রমণের ভিত্তি হলো ব্রাউজার আর প-াইনের বিপুলসংখ্যক সিকিউরিটি লুপহোল।

ওয়েবে যেভাবে আপনার কমপিউটার প্রোটেক্ট করবেন

সিকিউরিটি স্যুট : সিকিউরিটি স্যুটে সম্পৃক্ত থাকে অ্যান্টিভাইরাস এবং ফায়ারওয়াল কম্পোনেন্ট যা কমপিউটারকে ম্যালওয়্যার থেকে রক্ষা করে। উইন্ডোজ এবং ব্রাউজার উভয়কে আপডেট হতে হবে।

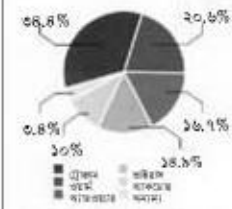
লিঙ্কস : সার্ফিংয়ের সময় মারাত্মক ওয়েবসাইটকে এড়িয়ে যাবার জন্য ইনস্টল করুন লিঙ্ক চেকার। ফিশিং ফিল্টার যাতে নিষ্ক্রিয় না থাকে সেদিকে খেয়াল রাখা উচিত।

জাভাস্ক্রিপ্ট : Add ons যেমন–AdBlock বা NoScript আপনাকে ক্ষতিকর স্ক্রিপ্ট থেকে রক্ষা করবে। সম্পূর্ণ নিরাপত্তার জন্য নিশ্চিত করুন যে আপনার ব্রাউজারে জাভাস্ক্রিপ্ট নিষ্ক্রিয় থাকে।

পিডিএফ : ভাইরাস স্ক্যানার বেশিরভাগ ভাইরাস কোড শনাক্ত করতে পারে। এ কারণেই হ্যাকাররা কোড ভেঙে ফেলে এবং এগুলো ডিস্ট্রিবিউট করে এনক্রিপ্টেড অবস্থায়। সাধারণত এই এনক্রিপ্টেড কোডগুলো হলো পিডিএফ ডকুমেন্টের ক্ষুদ্র ইউনিট।

ইনফেকটেড : ম্যালওয়্যার কমপিউটারের নিয়ন্ত্রণ গ্রহণ করে

ম্যানিপুলেটেড পিডিএফের মাধ্যমে বিভিন্ন ধরনের ম্যালওয়্যার পিসিতে পৌঁছে। যেমন–ট্রোজান, জিওস, জেটনট ইত্যাদি সবচেয়ে খারাপ ধরনের ভাইরাস।



এক্সিকিউট : মেমরিকে চূর্ণবিচূর্ণ করে

এক্সিকিউট করা ম্যালওয়্যার অপ্রয়োজনীয় কোড দিয়ে রিডারের মেমরি এরিয়াকে পরিপূর্ণ করে ফেলে যাতে ক্ষতিকর কোড পরবর্তী মেমরি এরিয়াতে অবস্থান করে এবং সেখানে ট্রুপার ফাংশন হিসেবে সবসময় এক্সিকিউট করে, যা ওয়েব থেকে অন্যান্য ম্যালওয়্যার লোড করে।

হিডেন কোড পিডিএফ ফাইলে ডিস্ট্রিবিউট

পিডিএফ ডকুমেন্ট গঠিত হয় অবজেক্টের মতো টেক্সট, ফন্ট, স্পেস, ফরম এবং ইমেজ দিয়ে। প্রতিটি পেজে ন্যূনতম ১০ হাজার অবজেক্ট থাকে। হ্যাকাররা এগুলো ভেঙে ফেলে এবং ডিস্ট্রিবিউট করে কিছু অবজেক্টে ক্ষতিকর কোড, যাতে সেগুলো ভাইরাস স্ক্যানার শনাক্ত করতে না পারে।

```
/Type/Action/S/Launch/Win<<F(cmd.exe)/
f=fso.OpenTextFile("doc.pdf",1,True)>>
script.vbs&&echo>=InStr(pf."SS")>>
batscript.vbs Click the "open" button to
view this document:)
```

যুক্ত হওয়া রিডার পিডিএফ লোড ও কোড অ্যাসেম্বল করে

পাঠক পিডিএফ ওপেন, বিভিন্ন পিডিএফ অবজেক্ট অ্যাসেম্বল এবং অবজেক্টে প্যারামিটারের মানানসই কনটেন্ট প্রদর্শন করেন। এভাবে পাঠক স্ক্রিপ্ট এক্সিকিউশনে প্রলুব্ধ হন, যা অবস্থান করে অবজেক্টে। যেমন–জাভাস্ক্রিপ্ট বা ভিজ্যুয়াল বেসিক স্ক্রিপ্ট ইত্যাদি। স্ক্রিপ্ট কমান্ড বিভিন্ন অবজেক্ট থেকে কোড ইউনিট অ্যাসেম্বল করে এবং সেগুলো চালনা করে, যা পরবর্তী সময়ে বাফার ওভার ফ্লো করে।

শতকরা ৫৭ ভাগ ম্যালওয়্যার পিডিএফ রিডারের টার্গেট গুলনিয়ারিবিলিটিস

পিডিএফ সংক্রমণ থেকে যেভাবে কমপিউটার রক্ষা করবেন

স্ক্রিপ্ট : অ্যাডোবি রিডারে স্ক্রিপ্টকে নিষ্ক্রিয় করার জন্য Edit→ Performances→JavaScript-এ নেভিগেট করুন। ফলে মেনু আইটেমে 'Authorizations' লিখুন করে এক্সটারনাল প্রোগ্রামের এক্সিকিউশন।

বিকল্প : যেহেতু বেশিরভাগ পিডিএফ টার্গেট করে অ্যাডোবি রিডারকে, তাই বিকল্প হিসেবে ব্যবহার করতে পারেন Foxit Reader যা বেশি নিরাপদ। অবশ্যই এটি নিয়মিতভাবে আপডেট করতে হবে।

ফাইল চেক : অপরাধীরা ই-মেইলের মাধ্যমে সংক্রমিত পিডিএফ ফাইল পাঠায়। এ ধরনের ফাইল চেক করার জন্য VirusTotal Uploaderসহ এগুলো আপলোড করুন (www.virustotal.com) অথবা অন্য কোনো স্ক্যানার ব্যবহার করুন।

ভাইরাস থেকে রক্ষা পাওয়ার ক্ষেত্রেও সর্বজনীন।

প্রায় দুই বিলিয়ন লোক ইন্টারনেট ব্যবহার করে অর্থাৎ প্রায় দুই বিলিয়ন লোক ম্যালওয়্যারের সম্ভাব্য শিকার। ব্যবহারকারীদের মূল্যবান ডাটা যেমন–পাসওয়ার্ড, পিন নাম্বার এবং ক্রেডিট কার্ড নাম্বার ক্ষতিকর হ্যাকারদের কাছে খুবই গুরুত্বপূর্ণ। ডাটা চুরির সবচেয়ে সহজ পথ হচ্ছে সংক্রমিত ওয়েবসাইট ও ফাইল, প্রাথমিকভাবে পিডিএফ ডকুমেন্ট। এছাড়া সবচেয়ে কম গুরুত্ব দেয়া উৎসও রয়েছে ভয়ের অরেকটি কারণ, যেমন–ডাটা ক্যারিয়ার তথা পেনড্রাইভ এবং অন্যান্য ইউএসবি স্টোরেজ ডিভাইস। এ লেখায় ব্যবহারকারীদের উদ্দেশে দেখানো হয়েছে কীভাবে সংক্রমিত ওয়েবসাইট, ক্ষতিকর পিডিএফ ফাইল এবং আক্রান্ত ইউএসবি ডিভাইস আপনার কমপিউটারকে সংক্রমিত করে এবং এ থেকে সুরক্ষার সেরা উপায় কী হতে পারে?

সিকিউরিটি ভেন্ডর ক্যাসপারস্কি গত জানুয়ারি থেকে মার্চ পর্যন্ত রেজিস্টার করে যে, এ সময়ের মধ্যে কমপিউটার সংক্রমণের প্রচেষ্টা শতকরা ২৬ দশমিক ৮ ভাগ বেড়েছে, যার বেশিরভাগই ম্যানিপুলেটেড ওয়েবসাইটের মাধ্যমে সংঘটিত হয়। সন্দেহজনক পর্নো বা পাইরেট ও ক্র্যাক সাইট ভিজিট করা থেকে বিরত থাকার মাধ্যমেই ক্ষতিকর ট্র্যাপ এড়িয়ে যেতে পারবেন তা কিন্তু নয়। অ্যান্টিভাইরাস ভেন্ডর অ্যাভাস্টের মতে, শতকরা ৯৯ ভাগ ক্ষতিকর ওয়েবসাইটই বৈধ ওয়েব পোর্টাল যারা আপোস করে আছে। ম্যালওয়্যার নিজেই এক্সটারনাল সাইট থেকে লোড হয়, যা ম্যালওয়্যার হোস্ট হিসেবে বিবেচিত। ক্যাসপারস্কির মতে, এ মুহূর্তে এ ধরনের আনুমানিক ১২০ মিলিয়ন হোস্ট ওয়েবসাইট সক্রিয় রয়েছে। এমন অবস্থায় সফটওয়্যারের লুপহোল কাজে লাগিয়ে স্বার্থ হাসিল করার ক্ষেত্রে অ্যাডোবি রিডার অন্য সবার চেয়ে এগিয়ে। সিকুনিয়ার সিকিউরিটি অ্যানালিস্ট ২০০৯-১০ সালের মধ্যে সর্বমোট ৬৯টি লুপহোল রেজিস্টার করে। অ্যাডোবি এখন তার ব্যবহারকারীদের উদ্দেশে চূড়ান্তভাবে আরও বেশি নিরাপত্তা বিধান করতে চাচ্ছে অ্যাক্রোবেট ভার্সন ১০ থেকে পরবর্তী ভার্সনগুলোতে। রিডার প্রোটেকটেড পরিবেশে সব কোড রান করবে যাতে সিস্টেমে অ্যাক্সেসের সুযোগ কমে যায়।

পক্ষান্তরে ইউএসবি ডিভাইসগুলো ম্যালওয়্যার ট্রান্সমিশনের পথ হিসেবে কম পরিচিত। এর ফলে হ্যাকাররা স্বতন্ত্র বা কোম্পানিসমূহকে টার্গেট করতে পারে বিশেষভাবে ডিজাইন করা ট্রোজান দিয়ে। এক্ষেত্রে বেশিরভাগ সময় উইন্ডোজের অটোরান ফাংশনের সুবিধা গ্রহণ করে ম্যালওয়্যার, যেগুলো এখন নিষ্ক্রিয় করা হয়েছে।

ভাইরাস এখন অনেক বেশি কৌশলী যা টার্গেট করতে পারে সুনির্দিষ্ট স্বতন্ত্র ফাইল ও ফোল্ডারকে। আগের যেকোনো সময়ের চেয়ে এখন এটি বেশি গুরুত্বপূর্ণ যে ভাইরাসের জন্য আগে থেকে সতর্কতামূলক ব্যবস্থা গ্রহণ করা। ▶

ইউএসবি ডিভাইসসমূহ : সংক্রমণের সবচেয়ে বেশি ঝুঁকিতে থাকে

ক্যামেরা, এমপিথ্রি প্লে-য়ার বা ইউএসবি পেনড্রাইভ ইত্যাদি খুব সহজেই ম্যালওয়্যারের মাধ্যমে সংক্রমিত হয়। এই ভাইরাস পরে অন্যান্য কমপিউটারকে সংক্রমিত করে।

ম্যানিপুলেট হওয়া ম্যালওয়্যার শনাক্ত করে ইউএসবি ডিভাইসকে যখনই তা প-াগ করা হয়

কয়েক ধরনের ম্যালওয়্যার এক্সটারনাল ড্রাইভকে শনাক্ত করে উইন্ডোজ অটোরান ফাংশন মনিটর করার মাধ্যমে। যখনই ম্যালওয়্যার সংক্রমিত ইউএসবি ডিভাইসকে শনাক্ত করে, তখনই এটি ড্রাইভে নিজে নিজেই কপি হয় এবং একটি কমান্ড রাইট করে Autorun.inf ফাইলে, যা প্রায় প্রতিটি এক্সটারনাল ড্রাইভে রুট ডিরেক্টরিতে লুকানো থাকে।

ট্রিগার করে : অটোরান ফাংশন উইন্ডোজকে সংক্রমিত করে

যখনই কোনো সংক্রমিত ড্রাইভ অন্য কোনো কমপিউটারে ঢুকানো হয়, তখন উইন্ডোজ Autorun-inf কমান্ড এক্সিকিউট করে যা এক্ষেত্রে ম্যালওয়্যার হিসেবে পরিচিত। উপরন্তু EXE ফাইল হতে পারে HTML ফাইল, যা ব্রাউজারে ওপেন করা হলে ইউজারকে ভিজাইটেড করে ম্যালওয়্যার সাইটে।

ম্যানুফ্যাকচারারসহ অন্যান্য মাধ্যমে ভাইরাস সরবরাহ করা

ম্যালওয়্যার বিস্তৃত হওয়ার সবচেয়ে সহজ মাধ্যম হলো ইউএসবি ডিভাইস যা প্রস্তুতের সময় থেকে বা 'trust worthy' সোর্সে ডিস্ট্রিবিউট করার সময় থেকে সংক্রমিত থাকে। এখানে কিছু দৃষ্টান্ত দেয়া হলো–

- **অলিম্পাস µTough 6010** : কোয়ালিটি কন্ট্রোল সিস্টেমে ত্রুটি থাকা অবস্থায় অলিম্পাস কোম্পানি জাপানে সংক্রমিত ক্যামেরা বিক্রি করে।
- **আইবিএম পেনড্রাইভ** : অস্ট্রেলিয়ান সিকিউরিটি কনফারেন্সে আইবিএম তাদের স্টলে ডিজিট করা দর্শকদের সংক্রমিত ইউএসবি স্টিক বিতরণ করে।
- **ক্রিয়েটিভ সাউন্ড ব-াস্টার X-Fi Go :** এই ডিভাইসটি বিক্রি করা হয় ট্রোজান ও ওয়ার্মসহ যা মারাত্মক হুমকিস্বরূপ। Trojan CorelinK.D ইনস্টল করে রুটকিট এজেন্ট THK, লোড করে Trojan Almanahe.V এবং ম্যানিপুলেট করে অটোরান ফাংশন। ওয়ার্ম RJump.AJ লোড করে Trojan Agent JXU এবং শনাক্ত করা প্রতিটি ইউএসবি ডিভাইসে নিজে নিজেই কপি হয়।

ইউএসবিভিত্তিক সংক্রমণ থেকে নিজেকে যেভাবে রক্ষা করবেন

অটোরান : অটোরান ফাংশন নিষ্ক্রিয় করতে হবে। এ কাজটি করতে পারে পান্ডা ইউএসবি ভ্যাকসিন নামের প্রোগ্রাম। বিকল্প হিসেবে স্বতন্ত্র ইউএসবি ডিভাইস ব-ক করা যেতে পারে।

ভাইরাস চেক : আপনার সিকিউরিটি স্যুটের 'Scan removable storage' অপশন সিলেক্ট করুন এ ধরনের ডিভাইস স্ক্যানে যুক্ত করার জন্য। এই অপশন সাধারণত পাওয়া যায় অ্যাডভান্স সেটিংয়ে।

অনলাইন, পিডিএফ এবং ইউএসবি ডিভাইসের মাধ্যমে ভাইরাস যেভাবে বিস্তৃত হয় এবং তার প্রতিরোধের উপায় চিত্রের মাধ্যমে দেখানো হলো।

শেষ কথা

ভাইরাস থেকে রক্ষা পেতে চাইলে প্রথমেই জানতে হবে ভাইরাস কীভাবে বিস্তৃত হয়। কেননা ভাইরাস সংক্রমণের উৎস যদি জানা না থাকে তাহলে তার প্রতিকার করা সম্ভব হবে না কোনো মতেই। ভাইরাস প্রতিরোধে বিভিন্ন টুল রয়েছে ঠিকই, তবে সেগুলো সবসময় শতভাগ ভাইরাস প্রতিরোধে সফল হয় না বিভিন্ন কারণে। মনে রাখা উচিত কোনো সিস্টেমে একের অধিক অ্যান্টিভাইরাস টুল থাকা উচিত নয়। অ্যান্টিভাইরাস টুল যেন সবসময় আপডেটেড থাকে সেদিকে খেয়াল রাখতে হবে। তাছাড়া অ্যান্টিভাইরাস টুলই যে আপনাকে সুরক্ষিত রাখতে পারবে তেমন নিশ্চয়তাও নেই। সুতরাং মনে রাখা উচিত প্রতিরোধমূলক ব্যবস্থা গ্রহণ করাই হচ্ছে সুরক্ষিত থাকার একমাত্র উপায়। আর তাই ভাইরাস সংক্রমণের উৎস সম্পর্কে জেনে নিয়ে প্রতিরোধমূলক ব্যবস্থা গ্রহণ করা উচিত।

ফিডব্যাক :
swapan52002@yahoo.com