র‍্যানসামওয়্যার কী এবং যেভাবে তা অপসারণ করবেন

তাসনুভা মাহ্‌মুদ

আপনার কমপিউটার স্ক্রিন একটি পপআপ ম্যাসেজসহ ফ্রিজ হয়ে আছে। ধরুন, ম্যাসেজটি এসেছে এফবিআই অথবা অন্য ফেডারেল এজেন্সি থেকে। এতে উল্লেখ করা হয়েছে– যেহেতু আপনি কমপিউটারের ফেডারেল তথা চুক্তি সংক্রান্ত আইন ভঙ্গ করেছেন, তাই আপনার কমপিউটার লক হয়ে থাকবে যতক্ষণ পর্যন্ত না জরিমানা দিচ্ছেন। অথবা আপনার পপআপ ম্যাসেজে উল্লেখ করা হয়েছে যে, আপনার পার্সোনাল ফাইল এনক্রিপ্ট হয়ে আছে। তাই আপনার ফাইল ডিক্রিপ্ট করার জন্য প্রয়োজনীয় কী পেতে চাইলে কিছু অর্থ দিতে হবে। মূলত এ দৃশ্যপট হলো র‍্যানসামওয়্যার স্ক্যামের কিছু উদাহরণ। এতে সম্পৃক্ত রয়েছে এক ধরনের ম্যালওয়্যার, যা কমপিউটারকে আক্রান্ত করে এবং ব্যবহারকারীকে তাদের ফাইলে অ্যাক্সেসকে বাধা দেয় অথবা তথ্য স্থায়ীভাবে ধ্বংস করার হুমকি দেয়, যদি না মুক্তিপণ দেয়া হয়।

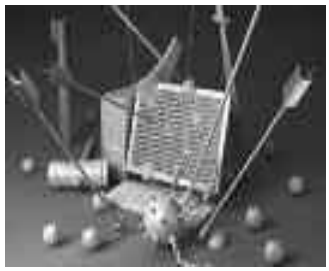
র‍্যানসামওয়্যার শুধু হোম কমপিউটারকে আঘাত করে না, বরং ব্যবসায়, ফিন্যান্সিয়াল ইনস্টিটিউশন, সরকারের এজেন্সি, অ্যাকাডেমিক ইনস্টিটিউশন ও অন্যান্য অর্গানাইজেশনও আক্রান্ত হতে পারে এবং ফলাফল হিসেবে সংবেদনশীল অথবা প্রোপাইটরি তথ্য হারাতে পারে অথবা নিয়মিত অপারেশনে বাধা দেয়।

র‍্যানসামওয়্যার কী?

সাধারণ জ্ঞান, ব্যাকআপ, প্রোঅ্যাক্টিভ প্রোটেকশন ও অটোমেটেড রিমুভাল টুলের সমন্বয়ে গড়ে তোলা যায় খুব দ্রুত বর্ধনশীল র‍্যানসামওয়্যারের বিরুদ্ধে কার্যকর প্রতিরোধ। র‍্যানসামওয়্যার গতানুগতিক সাধারণ ম্যালওয়্যারের মতো গুপ্তভাবে আপনার পিসিতে বিচরণ করে গুরুত্বপূর্ণ তথ্য হাতিয়ে নেয় না, বরং এটি হঠাৎ করে ব্যবহারকারীর সিস্টেমে ঢুকে পড়ে এবং কমপিউটার সিস্টেমে অ্যাক্সেসকে ব্লক করে দেয় যতক্ষণ পর্যন্ত না কিছু অর্থ দেয়া হচ্ছে। সুতরাং র‍্যানসামওয়্যার হলো এক ধরনের ম্যালওয়্যার, যা ব্যবহারকারীকে তাদের সিস্টেমে অ্যাক্সেস করতে বাধাদান কিংবা সীমিত করে সিস্টেমের স্ক্রিন লক করার মাধ্যমে অথবা ইউজার ফাইল লক করার মাধ্যমে যতক্ষণ পর্যন্ত না এ বন্দিত্বমোচনের জন্য মুক্তিপণ দেয়া হচ্ছে। অধিকতর আধুনিক র‍্যানসামওয়্যার ফ্যামিলি সমষ্টিগতভাবে ক্যাটাগরাইজ করা হয় ক্রিপ্টো-র‍্যানসামওয়্যার হিসেবে, আক্রান্ত সিস্টেমে নির্দিষ্ট কিছু ফাইল টাইপ এনক্রিপ্ট করে এবং ব্যবহারকারীকে নির্দিষ্ট কিছু অনলাইন পেমেন্ট মেথোডে নগদ অর্থ প্রদানে বাধ্য করে বন্দিত্বমোচনের মুক্তিপণ হিসেবে। যদি এমন অবস্থা থেকে নিজেকে রক্ষা করতে না জানেন, তাহলে বারবার র‍্যানসামওয়্যারে আক্রান্ত হতে পারে।

র‍্যানসামওয়্যার কেন ভীতিকর?

ডিজিটাল চৌর্যবৃত্তির সশস্ত্র দুর্বৃত্ত তথ্যের মহাসাগরে বিচরণ করে অনেকটাই উত্তেজিত অ্যাকশন মুভির মতো। এর সত্যতার প্রমাণ পাওয়া যায় র‍্যানসামওয়্যারের হামলার সংখ্যা দেখে। ২০১৫ সালে র‍্যানসামওয়্যার হামলার সংখ্যা যেখানে ছিল মাত্র ৩.৮ মিলিয়ন, সেখানে ২০১৬ সালে এ হামলার সংখ্যা উন্নীত হয় ৬৩৮ মিলিয়নে। অর্থাৎ র‍্যানসামওয়্যার হামলা গত এক বছরে বেড়েছে ১৬৭ গুণ। পক্ষান্তরে এ সময়ে ম্যালওয়্যার হামলার সংখ্যা কমেছে। কেননা, যেখানে নগদ অর্থ দাবি করে পাওয়া যায়, সেখানে তো চুরি করার দরকারই হয় না।



অতি সম্প্রতি প্রথমবারের মতো সানফ্রান্সিসকোর আরএসএ সিকিউরিটি কনফারেন্সে র‍্যানসামওয়্যারের ওপর হয়ে গেল দিনব্যাপী এক কম্প্রেহেনসিভ সেমিনার। যেখানে বিস্তারিত তুলে ধরা হয়– কে আক্রান্ত হতে যাচ্ছে, তারা কতটুকু নিচ্ছে, সবচেয়ে গুরুত্বপূর্ণ হলো কীভাবে ব্লক করা যায়, কীভাবে অপসারণ ও অসৎ লোকের সাথে আপস-মীমাংসা করা যায় যে আপনার ডাটাকে হোস্টেজ করে রেখেছে। ব্যবহারকারীরা তথ্য-সম্পদ ব্যবহার করতে পারেন অ্যান্টি-র‍্যানসামওয়্যার স্ট্র্যাটেজি ফর্মুলেট করার জন্য।

অ্যান্টি-র‍্যানসামওয়্যার সলিউশন যেমন ম্যালওয়্যারবাইট নামের টুলটি নির্ভরযোগ্য হলেও শতভাগ নির্ভরযোগ্য বা ফুল প্রুফ বলা যায় না।

র‍্যানসামওয়্যারের প্রকারভেদ

র‍্যানসামওয়্যার হলো সফিস্টিকেটেড ধরনের ম্যালওয়্যার, যা ব্যবহারকারীকে তাদের ফাইলে অ্যাক্সেস করতে বাধাদান কিংবা সীমিত করে সিস্টেমের স্ক্রিন লক করার মাধ্যমে অথবা ইউজার ফাইল লক করার মাধ্যমে যতক্ষণ পর্যন্ত না এ বন্দিত্বমোচনের জন্য মুক্তিপণ দেয়া হচ্ছে। সার্কুলেশনে মূলত দুই ধরনের র‍্যানসামওয়্যার রয়েছে। র‍্যানসামওয়্যারের শিকার হওয়ার আগে নিজেকে প্রস্তুত রাখতে চাইলে শত্রুকে জেনে নিন। ইন্টেল সিকিউরিটির EMEA বিজনেসের চিফ টেকনোলজি অফিসার রাজ সামানির মতে, ম্যাক ওএস ও লিনঅ্যাক্সসহ প্রায় চারশ'র বেশি র‍্যানসামওয়্যার ফ্যামিলি রয়েছে।

০১. এনক্রিপ্টিং র‍্যানসামওয়্যার : এটি ইনকর্পোরেট তথা সংঘবদ্ধ করে অ্যাডভান্সড এনক্রিপ্টশন অ্যালগরিদম। এটিকে ডিজাইন করা হয়েছে সিস্টেম ফাইলকে ব্লক করার জন্য ও পেমেন্ট ডিমান্ড করে ভিকটিমকে প্রয়োজনীয় কী প্রদান করতে, যা ব্লক করা কনটেন্টকে ডিক্রিপ্ট করার জন্য। উদাহরণস্বরূপ– ক্রিপ্টোলকার, লকি, ক্রিপ্টোওয়ালসহ আরও কিছু টুল।

০২. লকার র‍্যানসামওয়্যার : এটি অপারেটিং সিস্টেমের বাইরে ভিকটিমকে লক করে এবং ডেস্কটপ ও যেকোনো অ্যাপে অথবা ফাইলে অ্যাক্সেসকে অসম্ভব করে তোলে। এ ক্ষেত্রে ফাইলগুলো এনক্রিপ্ট করা থাকে না। তবে হামলাকারীরা এখনও মুক্তিপণ দাবি করে আক্রান্ত কমপিউটারকে আনলক করার জন্য। যেমন– পুলিশ দি ম্যাড র‍্যানসামওয়্যার অথবা উইনলকার।

০৩. মাস্টার বুট রেকর্ড (MBR) : মাস্টার বুট রেকর্ড র‍্যানসামওয়্যার হলো এ ধরনের সম্পর্ক যুক্ত আরেকটি ভার্সন। এমবিআর হলো পিসির হার্ডড্রাইভের সেক্টর, যা অপারেটিং সিস্টেমকে এনাবল করে পিসি বুটআপ করার জন্য। যখন এমবিআর র‍্যানসামওয়্যার স্ট্রাইক করে, বুট প্রসেস স্বাভাবিকভাবে সম্পন্ন হতে পারে না এবং একটি র‍্যানসাম তথা মুক্তিপণ নোট স্ক্রিনে ডিসপ্লে করার জন্য প্রম্পট করে। উদাহরণস্বরূপ– Satana ও Petya র‍্যানসামওয়্যার।

যেভাবে র‍্যানসামওয়্যার হুমকি থেকে রক্ষা পেতে পারেন

তবে যাই হোক, সবচেয়ে ব্যাপক-বিস্তৃতি ধরনের র‍্যানসামওয়্যার হলো ক্রিপ্টো-র‍্যানসামওয়্যার অথবা এনক্রিপ্টিং র‍্যানসামওয়্যার, যা এ লেখায় তুলে ধরা হয়েছে। সাইবার সিকিউরিটি কমিউনিটি একমত হয়েছে যে, এটি সবচেয়ে লক্ষণীয় ও ঝামেলাপূর্ণ সাইবার হামলা।

সাধারণ জ্ঞান : বিশেষজ্ঞদের অভিমত, সাধারণ কিছু জ্ঞানের অভ্যাস ব্যবহারকারীকে সহায়তা করতে পারে ম্যালওয়্যার এবং র‍্যানসামওয়্যারের তীব্রতা হ্রাস ও প্রকাশ করতে। এ জন্য নিচে বর্ণিত ধাপগুলোর প্রতি বিশেষভাবে নজর দিতে হবে।

উইন্ডোজ আপডেটের মাধ্যমে আপনার পিসিকে আপডেট রাখুন।

নিশ্চিত করুন, আপনি ব্যবহার করছেন অ্যাক্টিভ ফায়ারওয়াল ও অ্যান্টিম্যালওয়্যার সলিউশন্স। উইন্ডোজ ফায়ারওয়াল ও উইন্ডোজ ডিফেন্ডার মোটামুটিভাবে যথেষ্ট বলা যায়। তবে ভালো মানের একটি থার্ডপার্টি অ্যান্টিম্যালওয়্যার সলিউশন্স ব্যবহার করা আরও অনেক ভালো।

তবে যাই হোক, অ্যান্টিম্যালওয়্যারের ওপর আস্থা রাখবেন না, যা আপনাকে রক্ষা করবে। RSA সেশনে উপস্থিত সুধী সমাজে বিশেষজ্ঞেরা বলেন, অ্যান্টিভাইরাস কোম্পানিগুলো র‍্যানসামওয়্যার সম্পর্কে সচেতন করে আসছে ▶

এবং তাদের প্রোটেকশন ব্যবস্থার কোনো গ্যারান্টি নেই।

অ্যাডোবি ফ্ল্যাশ যেন বন্ধ থাকে অথবা একটি ব্রাউজার দিয়ে সার্ফ করুন, যেমন– গুগল ক্রোম। এটি যেন বাইডিফল্ট বন্ধ থাকে, তা নিশ্চিত করুন।

অফিস ম্যাক্রো যদি এনাবল থাকে, তাহলে তা বন্ধ রাখুন (অফিস ২০১৬-এর ক্ষেত্রে Trust Center → Macro Settings গিয়ে নিশ্চিত করতে পারবেন যে সেগুলো বন্ধ) অথবা সার্চ বক্সে 'macros' টাইপ করুন এবং 'Security' বক্স ওপেন করুন।

সন্দেহজনক কোনো লিঙ্ক ওপেন করবেন না, হতে পারে তা একটি ওয়েবপেজ অথবা একটি ই-মেইলের। র‍্যানসামওয়্যারের মুখোমুখি হওয়ার সবচেয়ে সাধারণ ও সহজ উপায় হলো খারাপ লিঙ্কে ক্লিক করা। সবচেয়ে উদ্বেগের বিষয় হলো র‍্যানসামওয়্যারের হামলার শিকার হওয়া দুই-তৃতীয়াংশের বেশি হলো খারাপ লিঙ্কে ক্লিক করা।

অনুরূপভাবে ইন্টারনেটের খারাপ প্রান্ত থেকে দূরে সরে থাকুন। একটি বৈধ সাইটের খারাপ অ্যাডও ম্যালওয়্যার ইনজেক্ট তথা উদ্বুদ্ধ করতে পারে, যদি না এ ব্যাপারে সতর্ক থাকেন। তবে ঝুঁকি বাড়তে পারেন যদি আপনি ওইসব সাইটে সার্ফ করতে থাকেন, যেখানে সার্ফ করা উচিত নয়।

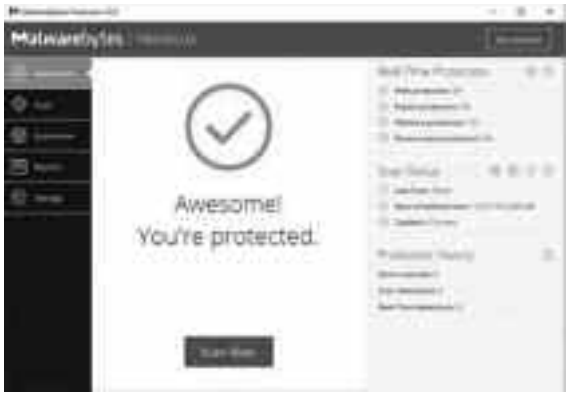
ডেডিকেটেড অ্যান্টি-ম্যালওয়্যার প্রোটেকশনের জন্য ম্যালওয়্যারবাইট ৩-কে বিবেচনা করতে পারেন। কেননা, এটি র‍্যানসামওয়্যারের বিরুদ্ধে প্রতিরোধ গড়ে তুলতে সক্ষম এমনটি বলা হয় প্রতিষ্ঠানটির বিজ্ঞাপনে। র‍্যানসামফ্রি নামের টুলটি ডেভেলপ করা হয়, যাকে বলা হয় অ্যান্টি-র‍্যানসামওয়্যার প্রোটেকশন। যাই হোক, অ্যান্টি-ম্যালওয়্যার প্রোগ্রাম তাদের পেইড বা বাণিজ্যিক স্যুটে সংরক্ষণ করে অ্যান্টি-র‍্যানসামওয়্যার। আপনি ইচ্ছে করলে ডাউনলোড করে নিতে পারবেন ফ্রি অ্যান্টি-র‍্যানসামওয়্যার প্রোটেকশন, যেমন– বিটডিফেন্ডারের অ্যান্টি-র‍্যানসামওয়্যার টুল। তবে লক্ষণীয়, আপনি মাত্র চার ধরনের কমন বা সাধারণ র‍্যানসামওয়্যার থেকে সুরক্ষিত থাকতে পারবেন।

ব্যাকআপ

র‍্যানসামওয়্যার ফাইল এনক্রিপ্ট ও লকআপ করে, যেগুলো আপনার কাছে খুবই মূল্যবান। সুতরাং, সেগুলো ভলনিয়ারেবল অবস্থায় রেখে দেয়ার কোনো কারণ নেই। গুরুত্বপূর্ণ ফাইল ব্যাকআপ করা এক ভালো কৌশল।

বক্স, ওয়ানড্রাইভ, গুগলড্রাইভসহ অন্যান্য ফ্রি স্টোরেজ প্রোভাইডারের সুবিধা গ্রহণ করতে ও নিয়মিতভাবে ডাটা ব্যাকআপ নিতে পারেন। (সতর্ক থাকবেন, আপনার ক্লাউড সার্ভিস সংক্রমিত ফাইল ব্যাকআপ করতে পারে যদি আপনি যথেষ্ট তাড়াতাড়ি কার্যকর ভূমিকা রাখতে না পারেন)। আরও ভালো হয়, যদি একটি এক্সটারনাল হার্ডড্রাইভের জন্য বাড়তি কিছু খরচ বহন করতে পারেন, যেখানে ডাটা ব্যাকআপ থাকবে। মাঝেমধ্যে কার্যকর করুন ইনক্রিমেন্টাল ব্যাকআপ। ডাটা ব্যাকআপের পর ড্রাইভকে বিচ্ছিন্ন করে দিন আপনার ডাটার ওই কপিকে আলাদা করার জন্য। CIO.com সাইটের রয়েছে কিছু বাড়তি ব্যাকআপ উপদেশ, যা ব্যবহারকারীকে সহায়তা করতে পারে র‍্যানসামওয়্যারের বিরুদ্ধে প্রতিরোধ গড়ে তুলতে। এ ছাড়া অভিজ্ঞদের পরামর্শ নিতে পারেন র‍্যানসামওয়্যারের বিরুদ্ধে প্রতিরোধ গড়ে তোলার জন্য।

যদি আপনি সংক্রমিত হন, তাহলে এটি ঠিক কোন ফাইল আপনাকে হোস্টেজ করে রেখেছে, তা র‍্যানসামওয়্যার দেখার সুযোগ করে দেবে



ম্যালওয়্যারবাইটের মূল ইন্টারফেস

ডাটা ব্যাকআপ অনলাইন অফ

ফাইল এক্সপ্লোরারের মাধ্যমে। এ ক্ষেত্রে একটি লক্ষণ হতে পারে অ্যাটাচড অপরিচিত এক্সটেনশনসহ সাধারণ .DOC বা .DOCX ফাইল। অ্যাভাস্টের চিফ টেকনিক্যাল অফিসার Ondrej Vlcek অফার করে বেশ কিছু উপদেশ। যদি র‍্যানসামওয়্যার টাইম-লকড না হয়, তাহলে একটানা আপনার ফাইল দরকার হবে না। এ ক্ষেত্রে সেগুলো একাকী রেখে দেয়ার কথা বিবেচনা করতে পারেন। সম্ভবত আপনার অ্যান্টিভাইরাস সলিউশন্স সেগুলো আনলক করতে সক্ষম হবে, যেহেতু এটি ডেভেলপ করে কাউন্টারমেজার। যাই হোক, ব্যাকআপকে ফুল প্রুফ বলা যায় না।

র‍্যানসামওয়্যারে আক্রান্ত হলে করণীয়

কীভাবে বুঝতে পারবেন আপনি র‍্যানসামওয়্যারে আক্রান্ত হয়েছেন? যদি বুঝতে পারেন, তাহলে আতঙ্কিত হবেন না। যদি বুঝতে পারেন আপনি র‍্যানসামওয়্যারে আক্রান্ত হয়েছেন, তাহলে আপনার প্রথম প্রচেষ্টা হবে পুলিশ ও এফবিআইয়ের ইন্টারনেট ক্রাইম কমপ্লায়েন্ট সেন্টারসহ অন্যান্য অথরিটির সাথে যোগাযোগ করা। সমস্যা নির্ণয়ের লক্ষ্যবিন্দু স্থির করুন। ডিরেক্টরির মাধ্যমে এগিয়ে গিয়ে নির্দিষ্ট করুন আপনার কোন ফাইলটি আক্রান্ত হয়েছে। যদি খুঁজে পান যে আপনার ডকুমেন্টে রয়েছে বাজে এক্সটেনশন নেম, তাহলে সেগুলো পরিবর্তন করুন। কিছু র‍্যানসামওয়্যার ব্যবহার করে 'fake' এনক্রিপ্টশন, যা আসলে এনক্রিপ্ট না করেই শুধু ফাইল নেম পরিবর্তন করে।

পরবর্তী ধাপ হলো র‍্যানসামওয়্যার আইডেন্টিফিকেশন ও রিমুভাল। আপনার পেইড অ্যান্টি-ম্যালওয়্যার সলিউশন স্ক্যান করবে হার্ডড্রাইভ এবং আপনার ভেন্ডরের টেক সাপোর্ট ও হেল্প ফোরামের সাথে যোগাযোগের চেষ্টা করবে। আরেকটি চমৎকার রিসোর্স হলো NoMoreRansom.com-এর ক্রিপ্টো-শেরিফ। এটি হলো একটি রিসোর্সের কালেকশন এবং ইন্টেল, ইন্টারপোল ও ক্যাসপারস্কি ল্যাবের র‍্যানসামওয়্যার আনইনস্টলার প্রোগ্রাম, যা আইডেন্টিফাই করতে ও আপনার সিস্টেম থেকে সমূলে র‍্যানসামওয়্যার উৎপাটন করতে সহায়তা করে ফ্রি রিমুভাল টুল দিয়ে। NoMoreRansom.org-এর ক্রিপ্টো-শেরিফ সাইট সম্পৃক্ত করে এক সহজ টুল, যা আবিষ্কার করতে পারে কোন ধরনের র‍্যানসামওয়্যার আপনার পিসিকে আক্রান্ত করেছে।

যদি সবকিছু ব্যর্থ হয়

যদি র‍্যানসামওয়্যার রিমুভ করতে না পারেন, তাহলে আপনাকে বাধ্য হবে বিবেচনা করতে হবে ডাটা কত গুরুত্বপূর্ণ বা এর মূল্য কেমন হতে পারে এবং কত দ্রুত এটি আপনার দরকার হতে পারে। জরিপ প্রতিষ্ঠান Datto-এর তথ্য মতে, ২০১৬ সালে র‍্যানসামওয়্যারে আক্রান্ত ৪২ শতাংশ ক্ষুদ্র ব্যবসায়ীকে তাদের বন্দিত্বমোচনের জন্য মুক্তিপণ দিতে বাধ্য হয়েছে।

প্রত্যেক ব্যবহারকারীর মনে রাখা উচিত, ম্যালওয়্যারের অপর প্রান্তে এমন কেউ আছে যে আপনার কমপিউটিং জীবনকে অতিষ্ঠ করে ফেলতে পারে। বিশেষজ্ঞেরা পরামর্শ দেন, যদি কোনো উপায় থাকে র‍্যানসামওয়্যার অথারকে ম্যাসেজ দেয়ার, তাহলে চেষ্টা করে দেখতে পারেন। তবে কোনোভাবে আশা করবেন না যে, তারা ফ্রি-তে আপনার ফাইল এনক্রিপ্ট করে দেবে। র‍্যানসামওয়্যার রাইটার হলো অসাধু ব্যবসায়ী। তাদের সাথে আপস-মীমাংস করার চেষ্টা করুন কম র‍্যানসামে।

সুতরাং, প্রতিরোধের কৌশল ডাটার ডুপ্লিকেশন ও ব্যাকআপ হলো সেরা অপশন। যদি আপনার ডাটার আদি কপি অন্য কোথাও সেভ করা থাকে, তাহলে আপনাকে পিসি রিসেট, অ্যাপস রিইনস্টল ও ডাটা রিস্টোর করতে হতে পারে ব্যাকআপ থেকে কজ

ফিডব্যাক : mahmood_sw@yahoo.com