ক্রিপ্টোকারেন্সি মাইনিং নমুনা বিশ্লেষণ

দেবাশীষ পাল
ইনফরমেশন সিকিউরিটি স্পেশালিস্ট, বিজিডি ই-গভ সার্ট

ক্রিপ্টোকারেন্সি মাইনিং একটি প্রক্রিয়া, যা ক্রিপ্টোকারেন্সির বিভিন্ন ধরনের লেনদেন যাচাই করা হয় এবং ব্লকচেইন ডিজিটাল অ্যাকাউন্টে যোগ করা হয়। প্রতিটি ক্রিপ্টোকারেন্সি লেনদেন করার সময় লেনদেন তথ্যটির সত্যতা নিশ্চিত করার জন্য এবং লেনদেনের সাথে জড়িত ব্লকচেইন লেজার আপডেট করার জন্য একটি ক্রিপ্টোকারেন্সি মাইনিং প্রক্রিয়া শুরু হয়। এই প্রক্রিয়া সম্পন্ন করতে জটিল গাণিতিক সমস্যা সমাধান করতে হয়। এই গাণিতিক সমস্যা সমাধানের সাথে জড়িত ব্যক্তি বা কমপিউটারকে সাধারণত মাইনার বলা হয়। এই গাণিতিক সমস্যা প্রথম যে সমাধান করতে পারবে, সে বিজয়ী হিসেবে ক্রিপ্টোকারেন্সি পাবে (কমিশন পাবে)।

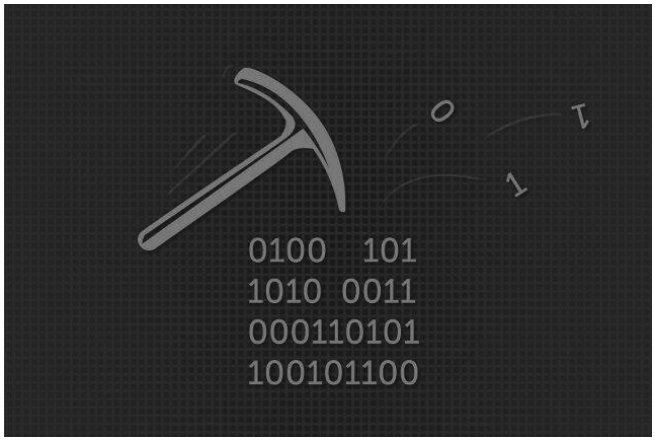


Image source : https://sensorstechforum.com/

একটি সফল ক্রিপ্টোকারেন্সি মাইনিংয়ের জন্য একজন মাইনারকে অন্য ক্রিপ্টোমাইনারদের সাথে প্রতিদ্বন্দ্বিতা করতে হয় ও দ্রুত সমাধানের জন্য অনেক কমপিউটিং রিসোর্সের প্রয়োজন হয়ে থাকে। যেহেতু এ ধরনের ক্রিপ্টোকারেন্সি মাইনিং করতে প্রচুর কমপিউটিং প্রসেসিং দরকার হয়, তাই সাইবার অপরাধীরা ক্রিপ্টোমাইনিং ম্যালওয়্যার দিয়ে সাধারণ কমপিউটার ব্যবহারকারীদের কমপিউটার আক্রান্ত কমপিউটারের প্রসেসিং ক্ষমতা ব্যবহার করে থাকে।

সাধারণত সাইবার অপরাধীরা নিচের যেকোনো পদ্ধতি ব্যবহার করে সাধারণ কমপিউটারের ব্যবহারকারীদের কমপিউটারকে আক্রান্ত করে থাকতে পারে। যেমন-

০১. অবিশ্বস্ত/জাল ডাউনলোড পোর্টাল থেকে সফটওয়্যার ডাউনলোডের মাধ্যমে।

০২. স্প্যাম প্রচারণা/ফিশিং ই-মেইলের মাধ্যমে। কমপিউটর ব্যবহারকারীকে তাদের প্রেরিত ফিশিং ই-মেইলে ডকুমেন্ট ফাইল ওপেন অথবা লিঙ্কে ক্লিক করতে প্ররোচিত করার মাধ্যমে।

০৩. আক্রান্ত ওয়েবসাইট ভিজিট করাবার মাধ্যমে।

সাইবার সচেতনতা বাড়ানোর লক্ষ্যে এই প্রবন্ধটি তৈরি করা হয়েছে। এই প্রবন্ধে দুটি ক্রিপ্টোকারেন্সি মাইনিং ম্যালওয়্যার নমুনা বিশ্লেষণ করা হয়েছে। নমুনা দুটি BGD e-GOV CIRT তার trusted source থেকে সংগ্রহ করেছে।

বিশ্লেষণ-১

নমুনা ফাইল নাম : window.exe

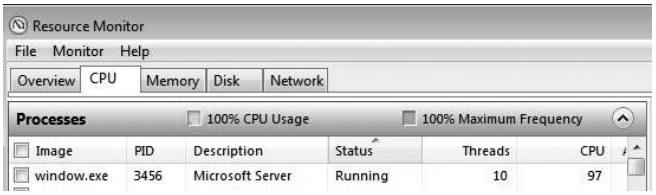
MD5: d14888fa2e40a0ebef641233a9 72c6f1

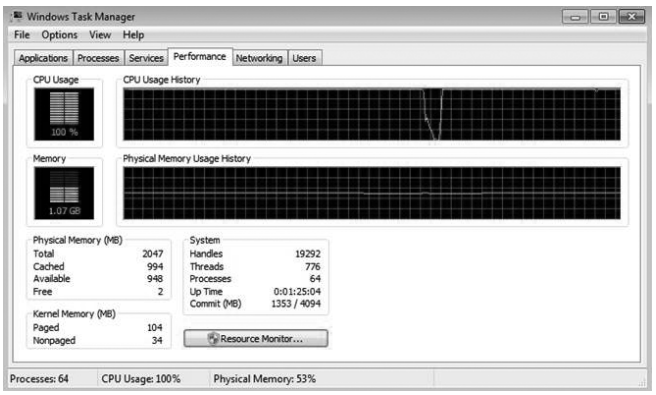
SHA-1: 42c2805bfbd78e651b6b9ba9 bdba5ed33b57318f

সাধারণত সাইবার অপরাধীরা ফিশিং ই-মেইলে ডকুমেন্ট ফাইল অথবা লিঙ্ক প্রেরণ করে সেই ডকুমেন্ট ফাইলটি ক্ষতিকারক ম্যাক্রোকোড দিয়ে সংযুক্ত থাকে। যদি এ ফাইলটি ওপেন তবে powershell বা vbs script চালু হতে পারে, যা সাইবার অপরাধীর নিয়ন্ত্রিত সার্ভারের সাথে যুক্ত হয়ে ম্যালওয়্যার ফাইল ডাউনলোড হয় ও কমপিউটার ব্যবহারকারীর অজান্তে চালু হয়ে যেতে পারে।

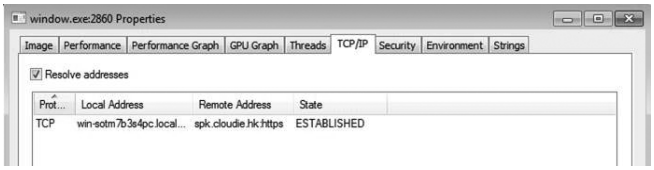
সাধারণত ক্রিপ্টোকারেন্সি মাইনিং ম্যালওয়্যার অন্যান্য ম্যালওয়্যারের মতো আক্রান্ত কমপিউটারের তথ্য ক্ষতিগ্রস্ত করে না, কিন্তু এটি আক্রান্ত কমপিউটারের প্রসেসিং ক্ষমতা ব্যবহার করে। ফলে কমপিউটারের পারফরম্যান্স অনেক ধীরগতি হিসেবে অনুভূত হয়।

০১. আমাদের বিশ্লেষিত নমুন window.exe চালু করার সাথে সাথে আক্রান্ত কমপিউটারের প্রসেসিং ক্ষমতা ১০০ শতাংশ পর্যন্ত ব্যবহার করতে থাকে।





০২. আক্রান্ত কমপিউটারটি সম্ভবত একটি মাইনিং পুলের সাথে যোগাযোগ করে।



০৩. ক্রিপ্টোকারেন্সির জন্য আক্রান্ত কমপিউটারের সাথে মাইনিং পুল ডাটা আদান-প্রদান।

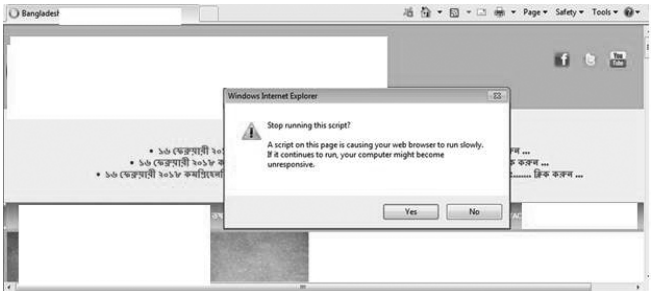
"jsonrpc":"2.0" = JSON-RPC প্রটোকল যা নেটওয়ার্ক সকেট বা HTTP-এর মাধ্যমে সহজভাবে ডাটা আদান-প্রদান করার জন্য ব্যবহার করা যেতে পারে। Params = প্যারামিটার job_id = মাইনার ও সার্ভার মাঝে ফলাফলের ইন্ডেক্সিং যা proof-of-work অ্যালগরিদম হিসেবে ব্যবহার হয়।

বিশ্লেষণ-২

ব্রাউজারভিত্তিক ক্রিপ্টোকারেন্সি মাইনিং : একটি ক্রিপ্টোকারেন্সি মাইনিং পদ্ধতি, যা জাভা স্ক্রিপ্টের সাহায্যে ব্রাউজার দিয়ে এক্সিকিউট হয়ে ওয়েব ব্যবহারকারীর কমপিউটারের প্রসেসিং ক্ষমতা ব্যবহার করে থাকে।

এ ক্ষেত্রে আমরা ক্রিপ্টোকারেন্সি মাইনিং স্ক্রিপ্ট দিয়ে আক্রান্ত একটি ওয়েবসাইট ভিজিট করব।

০১. যদি কোনো ওয়েব ব্যবহারকারী আক্রান্ত ওয়েবসাইটটি ব্রাউজ করে, তবে ব্যবহারকারীকে একটি পপআপ দেখায় ও একটি স্ক্রিপ্ট চালানোর অনুমতি চাইতে পারে।



০২. আক্রান্ত ওয়েবসাইটটির হোমপেজের সোর্স কোড দেখে আমরা একটি সন্দেহজনক জাভা স্ক্রিপ্ট খুঁজে পাই।

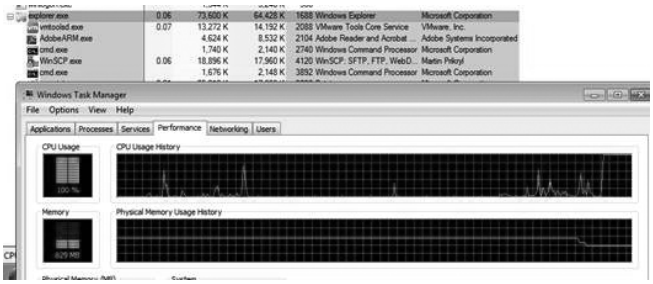
০৩. সন্দেহজনক ওয়েবসাইটটি ভিজিট করার পর আমরা একটি এনক্রিপ্ট কোড দেখতে পাই।

০৪. স্ক্রিপ্ট বোঝার জন্য আমরা ডিকোড করার চেষ্টা করি এবং

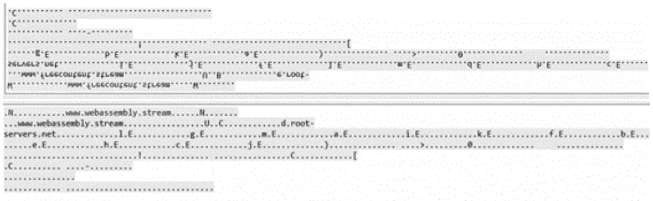
আংশিক ডিক্রিপ্টেড কোড খুঁজে পাই। যেমন-

এই জাভা স্ক্রিপ্ট বিভিন্ন ধরনের রেগুলার এক্সপ্রেমিন এবং RC4 এনক্রিপশন অ্যালগরিদম ব্যবহার করেছে।

০৫. রিয়েল টাইম বিশ্লেষণের জন্য আমরা আক্রান্ত ওয়েবসাইটটি ব্রাউজ করি ও জাভা স্ক্রিপ্টটি কার্যকর হতে দেই এবং লক্ষ করি যে, এটি কমপিউটারের প্রসেসিং ক্ষমতা ১০০ শতাংশ পর্যন্ত ব্যবহার করতে পারে।



০৬. আমরা এই স্ক্রিপটি ব্যবহারের সময় নিম্নোক্ত নেটওয়ার্ক যোগাযোগ দেখতে পাই।



০৭. আমরা আরো বিশ্লেষণ থেকে বুঝতে পারি, এ জাভা স্ক্রিপ্টটি একটি Monero জাভাস্ক্রিপ্ট ওয়েব মাইনার। কারণ coinimp ডকুমেন্টেশন থেকে আমরা একই ধরনের স্ক্রিপ্ট দেখতে পাই কজ