কুখ্যাত ২০ ওয়ার্ম, ভাইরাস ও বটনেট

তাসনুভা মাহ্‌মুদ

কমপিউটার জগৎ-এর নিয়মিত বিভাগ পাঠশালা সাধারণত ব্যবহারকারীদের ব্যবহারগত প্রয়োজনীয়তা ও চাহিদার প্রতি লক্ষ রেখে বিভিন্ন বিষয়ের ওপর লেখা প্রকাশ করে আসছে। তারই ধারাবাহিকতা থেকে একটু ভিন্ন দৃষ্টিকোণে এবার পাঠশালায় উপস্থাপন করা হয়েছে কুখ্যাত ২০ ওয়ার্ম, ভাইরাস ও বটনেক সম্পর্কে প্রাথমিক ধারণা। কেননা গত চার দশক ধরে অসংখ্য ম্যালওয়্যারের ব্যাপক বিস্তারের ঘটনা পরিলক্ষিত হয়। প্রথম দিকে ওয়ার্ম ও ভাইরাস সৃষ্টি বা তৈরি করা হয় কৌতূহলের বশে এবং তা খুব সামান্যই ক্ষতি বা বিরক্ত করত। কিন্তু এখন সময় অনেক বদলে গেছে। এ লেখায় ব্যবহারকারীদের জ্ঞাতার্থে ২০ ওয়ার্ম, ভাইরাস এবং বটনেটের ক্রমবিকাশ সম্পর্কে আলোকপাত করা হয়েছে, যেগুলোর মধ্যে আছে ক্রিপার নামের ভাইরাস থেকে শুরু করে সাম্প্রতিকের আলোচিত ফ্লেম ম্যালওয়্যার পর্যন্ত।

ক্রিপার

প্রথম প্রকৃত কমপিউটার ভাইরাস ক্রিপার অবমুক্ত হয় ১৯৭১ সালে, ল্যাবে। 'FortiGuard Labs'-এর সিনিয়র ডিরেক্টর গুইলাম লোভেট (Guillaume Lovet)-এর মতে, কোম্পানির একজন কর্মী ইন্টারনেটের আদি সংস্করণ Arpanet তৈরির কাজ করার সময় ক্রিপার অবমুক্ত হয়। ক্রিপার নেটওয়ার্কে একটি মেশিন অনুসন্ধান করে এতে ট্রান্সফার হয় এবং 'I'am the creeper, catch me if you can।' মেসেজ প্রদর্শন করে মনিটরে এবং ওপরে শুরু করে। এভাবে এক সিস্টেম থেকে আরেক সিস্টেমে লাফিয়ে লাফিয়ে চলতে শুরু করে।

Elk Cloner

Elk Cloner নামের ভাইরাসটি রচিত হয় ১৯৮২ সালে। ১৫ বছরের এক তরুণ তার বন্ধুর অ্যাপল টু কমপিউটার সিস্টেমে ফিজিক্যাল অ্যাক্সেস ছাড়াই অ্যাক্সেসের জন্য বুবি ট্র্যাপ হিসেবে এটি তৈরি করে। FortiGuard Lab-এর সিনিয়র ডিরেক্টর গুইলাম লোভেটের মতে, Elk Cloner বিস্তৃত হয় ফ্লপি ডিস্কের মাধ্যমে। এ ক্ষেত্রে সংক্রমিত মেশিন প্রদর্শন করে এক ক্ষতিহীন কবিতা, যা ভাইরাসের চমৎকারিত্বে উৎসর্গ করা হয়।

মরিস ওয়ার্ম

ব্লু কোট সিস্টেমসের ম্যালওয়্যার ল্যাব আর্কিটেক ক্রিশ লারসেনের মতে, মরিস (Morris) ওয়ার্ম ১৯৮৮ সালে কর্নেল বিশ্ববিদ্যালয়ের (Cornell University) ছাত্র রবার্ট তাপ্পন (Robert Tappan) তৈরি করেন, যা প্রথম ইন্টারনেট ওয়ার্ম হিসেবে পরিচিত।

সিমেনটেক সিকিউরিটি রেসপন্স বিভাগের ডিরেক্টর ক্যাভিন হ্যালি বলেন, মরিস ওয়ার্ম হলো প্রথম ওয়ার্ম, যা সবার মনোযোগ আকৃষ্ট করতে সক্ষম হয় এবং বিশৃঙ্খলা সৃষ্টির জন্য সম্ভাব্য কমপিউটার ম্যালওয়্যারকে ডেমোনেস্ট্রেট করে।

মাইকেল অ্যাঞ্জেলো

রেনেসিয়ান্স যুগের শিল্পী মাইকেল অ্যাঞ্জেলোর নামে এক ঘুমন্ত ভাইরাসকে ১৯৯১ সালে ডিজাইন করা হয়। লোভেটের মতে, এ ভাইরাসকে এমনভাবে ডিজাইন করা হয়, যা ঘুমন্ত অবস্থা থেকে জাগ্রত হবে অর্থাৎ সক্রিয় হবে শিল্পী মাইকেল অ্যাঞ্জেলোর জন্মদিন ৬ মার্চে এবং আক্রান্ত কমপিউটারের হার্ডডিস্কের জটিল অংশ মুছে ফেলবে।

এটি সিস্টেমে ক্ষতি করার জন্য অবজ্ঞাভরে সাময়িকভাবে প্রবল উত্তেজনা সৃষ্টি করে। ৬

চিত্র-১

মার্চের আগেই মিডিয়ায় প্রকাশিত হয় বিশেষজ্ঞদের ভবিষ্যদ্বাণী। এতে উল্লেখ করা হয়, আনুমানি ৫০ লাখ কমপিউটার এতে অবশ্যই ক্ষতিগ্রস্ত হবে। এখনও মাঝেমধ্যে ৬ মার্চে কয়েক হাজার ডাটা হারানোর ঘটনার কথা শোনা যায়।

ম্যালিশা

১৯৯৯ সালে ম্যালিশা ভাইরাস প্রথম শনাক্ত হয়। লোভেটের মতে, এই ভাইরাস বংশবিস্তার করে আক্রান্ত মাইক্রোসফট ওয়ার্ড ডকুমেন্টের মাধ্যমে এবং আউটলুক কন্টাক্টে নিজেকে মেইল করে ব্যবহারকারীকে সংক্রমিত করে। এটি ইন্টারনেটে কোনো কোনো গুরুত্বপূর্ণ মেইলিং সিস্টেমে আঘাত হেনে নিষ্ক্রিয় বা অসাড় করে ফেলতে পারে। ম্যালিশা ভাইরাসের স্রষ্টা ম্যালিশা নামের এক স্ট্রিপারের সম্মানে এটি তৈরি করা হয়, যার সাথে এর দেখা হয়েছিল ফ্লোরিডায়।


চিত্র-২

অসম্ভব কিছুই নয়, এর মাধ্যমে হয়তো সে কোনোভাবে ম্যালিশার হৃদয় জয় করতেও পারে কিংবা নাও পারে। তবে যাই হোক, লোভেটের মতে, এ ক্ষতিকর কোড সৃষ্টি করার কারণে তাকে ২০ মাসের জন্য কারাদণ্ড ভোগসহ ৫ হাজার ডলার জরিমানাও দিতে হয়েছিল। তা নিশ্চিত করে বলা যায়।

আই লাভ ইউ

'I Love you' বা 'Love Letter' নামের ম্যালওয়্যার প্রথম শনাক্ত হয় ২০০০ সালে। সোশ্যাল ইঞ্জিনিয়ারিং ব্যবহার করে কমপিউটারকে আক্রান্ত করার ম্যালওয়্যারের প্রথম সফল দৃষ্টান্ত এটি নয়। এর আগে এ ধরনের অনেক আক্রান্তের ঘটনা ঘটেছে, তবে সেগুলো তেমন ক্ষতিকর ছিল না।

এ ভাইরাস কমপিউটারকে আক্রান্ত করার পাশাপাশি সাইবার সোশ্যাল ইঞ্জিনিয়ারিংয়ের জন্য দেয় এক ভিত্তি, যা এখনও কাজ করে। সবাই চায় কেউ তাদেরকে ভালোবাসুক। কিন্তু এর বিপরীত দিকও রয়েছে। তাই কমপিউটার ব্যবহারকারীদের উচিত সবকিছুতে বিশ্বাস করা না করা, যা কিছুই অনলাইনে দেখা যায়, বিশেষ করে তাদের ইনবক্সে যেসব ই-মেইল মেসেজ দেখা যায়।

২০১১ সালে টেনিস তারকা আনা কুর্নিকোভার নামের এক ভাইরাস বিদ্যুৎচমকের মতো ছড়িয়ে পড়ে। ই-মেইলের মাধ্যমে এ

চিত্র-৩

ভাইরাস দ্রুতগতিতে বিস্তৃত হওয়ার প্রধান কারণ ছিল ই-মেইলে ব্যবহারকারীদের প্রলুব্ধ করার জন্য আনা কুর্নিকোভার আকর্ষণীয় ছবির কথা উল্লেখ ছিল। সোশ্যাল নেটওয়ার্কে এটি অনেকটা সেক্স সেলের বিজ্ঞাপনের মতো।

কোড রেড

কোড রেড নামের ভাইরাসটি প্রথম শনাক্ত হয় ২০০১ সালে। এ ভাইরাসটি ওয়েব সার্ভারকে আক্রান্ত করে এবং স্বয়ংক্রিয়ভাবে বিস্তৃত হয়। লোভেটের মতে, মাইক্রোসফট IIS ▸

সার্ভারের ভালনারেবিলিটিকে সদ্ব্যবহার করে কোড রেড ভাইরাস স্বয়ংক্রিয়ভাবে বিস্তৃত হয়।

এক সপ্তাহের কম সময়ের মধ্যে কোড রেড ভাইরাস প্রায় ৪ লাখ সার্ভারকে আক্রান্ত করে এবং তাদের হোস্ট করা ওয়েবসাইটের হোমপেজ প্রতিস্থাপিত হয় 'Hacked By Chinese' মেসেজ দিয়ে।

লোভেট আরও উল্লেখ করেন, কোড রেডের রয়েছে স্বতন্ত্র বৈশিষ্ট্য বা ফিচার, যা ডিজাইন করা হয়েছে আক্রান্ত সার্ভার থেকে হোয়াইট হাউস ওয়েবসাইটকে ট্রাফিক দিয়ে প্লাবিত করা। সম্ভবত এটি হলো প্রথম কেস, যার ওপর ভিত্তি করে ব্যাপক বিস্তৃত পরিসরে হ্যাকটিভিজমের ডকুমেন্ট তৈরি হয়।

চিত্র-৪

এসকিউএল স্লামার

এসকিউএল স্লামার ২০০৩ সালের মাঝামাঝিতে তৈরি হয়। সিমেনটেকের শীর্ষস্থানীয় কর্মকর্তা হ্যালির মতে, এই ওয়ার্ম তাৎক্ষণিকভাবে ১৫ মিনিটের মধ্যে প্রায় সব সিস্টেমের ভালনারেবিলিটিকে সংক্রমিত করার জন্য আক্রমণ করে। এটি কোনো কোনো ইন্টারনেট হোস্টে ডিন্যায়েল অব সার্ভিসের কারণ হয়ে দাঁড়ায় এবং নাটকীয়ভাবে সাধারণ ইন্টারনেট ট্রাফিককে ধীরগতিসম্পন্ন করে দেয়, খুব দ্রুতগতিতে বিস্তৃত হতে থাকে এবং মাত্র ১০ মিনিটের মধ্যে এর ৭৫ হাজার শিকারের মধ্যে বেশিরভাগকেই সংক্রমিত করে।

সিমেনটেকের এক শীর্ষ কর্মকর্তা বলেন, ইতোপূর্বে কেউ এত দ্রুতগতিতে ম্যালওয়্যারকে বিস্তৃত হতে দেখেনি। এ ওয়ার্মের ভিত্তি হলো প্রুফ অফ কনসেপ্ট কোড।

সাসার

সাসার নামের ম্যালওয়্যার প্রথম শনাক্ত হয় ২০০৪ সালে। এটি মাইক্রোসফট উইন্ডোজের ভালনারেবিলিটিকে কাজে লাগিয়ে বংশবিস্তার করে, যা বিশেষভাবে খুবই ক্ষতিকর হিসেবে প্রতিষ্ঠিত করেছে। এ ছাড়া বিশেষজ্ঞ লোভেটের মতে, ওয়ার্ম কোডের ভেতরে বাগ তথা ত্রুটি থাকার কারণে আক্রান্ত সিস্টেম কয়েক মিনিট পরপর বন্ধ হয়ে যায়।

সাসার ওয়ার্মের কারণে ১ মিলিয়নের বেশি সিস্টেম সংক্রমিত হয়। এএফপির কমিউনিকেশন স্যাটেলাইটের কার্যক্রম কয়েক ঘণ্টার জন্য বিঘ্নিত হয়, ডেল্টা এয়ারলাইন্স ফ্লাইট বাতিল করতে বাধ্য হয়, ব্রিটিশ কোস্টগার্ড ম্যাপ প্রিন্ট করতে ফিরে যেতে বাধ্য হয়েছিল এবং একটি হাসপাতাল তার ইমার্জেন্সি রুমকে রিডাইরেক্ট করতে বাধ্য হয়েছিল, কেননা এর রেডিওলজি ডিপার্টমেন্টকে ভাইরাস সম্পূর্ণরূপ প্যারালাইজ তথা অসাড় করে ফেলেছিল। এ ভাইরাস আক্রমণের ফলে ক্ষতির পরিমাণ আনুমানিক ১৮ বিলিয়ন ডলারের বেশি।

মাইক্রোসফট এ ভাইরাস রচয়িতাকে ধরিয়ে দেয়ার জন্য ২,৫০,০০০ ডলারের পুরস্কার ঘোষণা দেয়, যিনি ১৮ বছরের এক জার্মান ছাত্র।

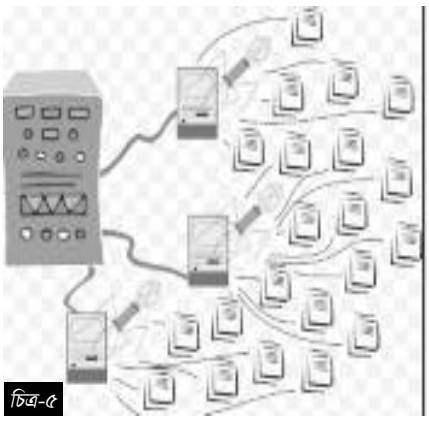
মাইটব

মাইটব হলো এমন এক ভাইরাস, যা ম্যালওয়্যারের অন্যতম প্রথম অংশ, যা বট (একটি কমপিউটার প্রোগ্রাম, যা পারফর্ম করে বিশেষ কোনো কাজকে বারবার করে অনেকবার করে) এবং মাস-মেইলার ফিচারকে সমন্বিত করে। লোভেটের মতে, ২০০৫ সালে মাইটবকে চিহ্নিত করা হয় বটনেট এবং সাইবার ক্রাইমের যুগের সূচনা হিসেবে।

ইদানীং বিজনেস মডেল ডিজাইন করা হয় মুদ্রারূপে চালু করার জন্য। এর ফলে অনেক বটনেট আবির্ভূত হতে শুরু করে, ইনস্টল হতে থাকে স্পাইওয়্যার, সবদিকে ছড়িয়ে পড়ে স্প্যাম। অবৈধ কনটেন্ট হোস্টিং হয়, ব্যাংকিংয়ে বিশ্বস্ততায় ব্যাঘাত সৃষ্টি করে, ব্ল্যাকমেইলিং ইত্যাদি।

স্টর্ম বটনেট

স্টর্ম বটনেট ইন্টারনেটে প্রথম শনাক্ত হয় ২০০৭ সালের জানুয়ারিতে এবং ই-মেইলের মাধ্যমে দ্রুতগতিতে ছড়িয়ে পড়ে। স্টর্ম বটনেট বা স্টর্ম ওয়ার্ম বটনেট হলো প্রত্যন্ত অঞ্চল থেকে নিয়ন্ত্রিত জম্বি কমপিউটারের নেটওয়ার্ক, যা স্টর্ম ওয়ার্ম, ট্রোজান হর্স ইত্যাদির সাথে লিঙ্ক হয়ে ই-মেইলের মাধ্যমে দ্রুত ছড়িয়ে পড়ে।



চিত্র-৫

স্টর্ম বটনেট ই-মেইলের মাধ্যমে ছড়িয়ে পড়ে, যার সাবজেক্ট হলো '230 dead as storm batters Eurrope', যা এ ওয়ার্মকে ব্যাপক পরিচিতি দেয়। স্টর্ম বটনেট ১০ থেকে ৫০ লাখ কমপিউটার সিস্টেমকে আক্রান্ত করে, যা হিসেব অনুযায়ী সারাবিশ্বে রানিং ম্যালওয়্যারের ৮ শতাংশ। বটনেটকে সম্পূর্ণরূপে নিষ্ক্রিয় করা যায় ইউনিট কন্ট্রোল সেন্টার নিউট্র্যালাইজ করার মাধ্যমে। ২০১২ সালের ডিসেম্বরের পর স্টর্ম ওয়ার্মের শনাক্তের কোনো তথ্য পাওয়া যায়নি।

কুবফেস

কুবফেস হলো একটি মাল্টি-প্ল্যাটফরম কমপিউটার ওয়ার্ম, যা মূলত টার্গেট করে ব্যবহারকারীর সামাজিক নেটওয়ার্কিং ওয়েবসাইট ফেসবুক ই-মেইল। এটি ফেসবুকের জন্য একটি অ্যানাগ্রাম। কুবফেস প্রথম শনাক্ত হয় ২০০৮ সালের ডিসেম্বর মাসে।

কুবফেস মূলত বিস্তৃত হয় জনগণের কাছে ফেসুবক মেসেজ ডেলিভারির মাধ্যমে যারা ফেসবুক ব্যবহারকারীর বন্ধু এবং যাদের কমপিউটার আক্রান্ত। কুবফেসকে ডিজাইন করা হয়েছে মাইক্রোসফট উইন্ডোজ এবং ম্যাক ওএস এক্সকে সংক্রমিত করার জন্য। তবে লিনআক্সেও কাজ করে। কুবফেস কোনো সংবেদনশীল ফিন্যান্সিয়াল ডাটাকে আক্রান্ত করে না। কুবফেস সোশ্যাল নেটওয়ার্কে আক্রান্ত ব্যবহারকারীদেরকে প্রম্পট করে ভালোভাবে ভিডিও উপভোগ করার জন্য ফ্ল্যাশ প্লেয়ারের আপডেট ভার্সন ডাউনলোড করার জন্য প্ররোচিত করে। মূলত এই আপডেট কপিই হলো ভাইরাস।

জিইউএস বটনেট

জিইউএস বটনেট ২০০৭ সালে প্রথম শনাক্ত হয় যখন এটি ইউনাইটেড স্টেটস ডিপার্টমেন্ট অব ট্রান্সপোর্টেশনের তথ্য চুরি করতে ব্যবহার হয়। এটি ২০০৯ সালের মার্চে আরও বিস্তৃত হয়। ব্লু কোট সিস্টেমসের ম্যালওয়্যার ল্যাব আর্কিটেক্ট ক্রিশ লারমেনের মতে, এটি হলো 'King of the botnet kits'।

ম্যালওয়ার প্লাটফরম নিজের মধ্যে ট্রোজান হর্স তৈরির জন্য ব্যবহার হয়, যা ব্যাংকিং তথ্য চুরি করে। জিইউএস বটনেট বিস্তৃত হয় তথা চালিত হয় ডাউনলোড ও ফিশিং স্কিমের মাধ্যমে। বিশ্বে ১৯৬টি দেশে জিইউএস নিয়ন্ত্রিত মেশিন রয়েছে। জিইউএসের ট্যার্গেট হলো মাইক্রোসফট উইন্ডোজ মেশিন। এটি অ্যাপল ম্যাক ওএস এক্স বা লিনআক্সে কাজ করে না। সারাবিশ্বে ২৪২১টি কোম্পানি ও সংস্থা আক্রান্ত হয় এই বটনেটের মাধ্যমে।

আইকি

সি ল্যাঙ্গুয়েজ প্রোগ্রাম দিয়ে লেখা অ্যাপল আইফোনের জন্য প্রথম ওয়ার্মের নাম আইকি। এটি তৈরি করেন ২১ বছর বয়েসী অস্ট্রেলিয়ার এক অনুসন্ধিৎসু প্রোগ্রামার একঘেয়েমির কারণে বিরক্ত হয়ে।

ওয়ার্ম আইপি আইফোনের স্বত্বাধিকারীর ওয়ালপেপার বদলে ফেলে এবং প্রতিস্থাপন করে আশির দশকের পপস্টার রিক অ্যাশলের (Rick Astley) ছবি দিয়ে এবং মেসেজ দেয়। 'ikee is never going to give you up' আইপি ওয়ার্ম প্রথম আবির্ভূত হয় ২০০৯ সালে।

আইকি বিদ্বেষপরায়ণ নয়, তারপরও এটি কিছু বিষয় মোডিফাই করে এবং পারফর্ম করে কিছু কাজ যেমন আইফোন ব্যবহারকারীর গুরুত্বপূর্ণ তথ্য চুরি করে। এ ওয়ার্ম SSH (Secure Shell) নামের এক ইউনিক্স ইউটিলিটি রান করে প্রভাবিত করতে পারে জেলব্রোকেন আইফোনকে যেখানে আইফোনের ডিফল্ট পাসওয়ার্ড 'alpine' ব্যবহার হয়।

ইদানীং মোবাইল ডিভাইসগুলো সাধারণ ▸

কমপিউটারের মতো কাজ করে। তাই সাইবার হুমকি থেকে একে রক্ষা করা উচিত অন্যান্য কমপিউটারের মতো।

কনফ্লিকার

কনফ্লিকার নামের ওয়ার্মের প্রথম আবির্ভাব ঘটে ২০০৮ সালের নভেম্বর মাসে। এ ওয়ার্মের প্রধান টার্গেট হলো মাইক্রোসফট উইন্ডোজ অপারেটিং সিস্টেম। এটি উইন্ডোজ সফটওয়্যার এবং ডিকশনারির ত্রুটিকে কাজে লাগিয়ে অ্যাডমিনিস্ট্রেটর পাসওয়ার্ডে আক্রমণ করে বংশবিস্তার করে বটনেট গঠন করার সময়। এটি প্রতিরোধ করা বেশ জটিল। কেননা এটি অনেক অ্যাডভান্স ম্যালওয়্যারের সমন্বিত কৌশল ব্যবহার করে। কনফ্লিকার ওয়ার্ম ২০০ দেশের বেশি সরকারি-বেসরকারি ব্যবসায়ী ও হোম কমপিউটারকে আক্রান্ত করে ২০১৩ সাল পর্যন্ত সময়ের মধ্যে সবচেয়ে বেশি মারাত্মক কমপিউটার ওয়ার্ম হিসেবে পরিচিতি পায়। এ ওয়ার্মে আক্রান্ত কমপিউটারের সংখ্যা আনুমানিক ৯০ লাখ থেকে দেড় কোটির মতো।

অপারেশন অরোরা

অপারেশন অরোরা হলো এক সাইবার হামলা, যা শুরু হয় ২০০৯ সালের মাঝামাঝিতে এবং তা অব্যাহত থাকে ডিসেম্বরের মাঝামাঝি সময় পর্যন্ত।

২০১০ সালের ১২ জানুয়ারিতে গুগল জনসাধারণের সামনে ব্লগ পোস্টের মাধ্যমে প্রথম সাইবার হামলার কথা প্রকাশ করে, যা আসে চীন থেকে।

এ হামলায় যুক্তরাষ্ট্রের ৩০টির বেশি প্রতিষ্ঠানে আঘাত হানা হয়। এ সাইবার হামলায় ব্যবহার করা হয় খুব অগ্রসর মানের কৌশল, যা দীর্ঘদিন ধরে শনাক্ত করা সম্ভব হয়নি। আর এ দীর্ঘ সময়ের মধ্যে সোর্স কোড ও মেধাস্বত্ব সম্পদসহ গুরুত্বপূর্ণ অনেক তথ্যই চুরি করে নিতে সক্ষম হয় অপরাধীরা।

ফ্ল্যাশব্যাক

ফ্ল্যাশব্যাক ট্রোজান প্রথম শনাক্ত হয় ২০১১ সালে। এটি ম্যাক ওএস এক্স কমপিউটারকে আক্রান্ত করে এবং সিকিউরিটি ত্রুটিকে কাজে লাগিয়ে জাভায় নিজেকে ইনস্টল করায় ম্যাক কমপিউটারে।

জাভা ভালনারেবিলিটি ছাড়া ফ্ল্যাশব্যাক ম্যালওয়্যার নির্ভর করে হোস্ট করা কমপিউটার সার্ভারের মাধ্যমে। ফলে ম্যালওয়্যার অথরকে পারফর্ম করতে হয় এর অনেক জটিল ফাংশন। অ্যাপল আইএসপিগুলোর সাথে কাজ করছে সারা বিশ্বে, যাতে এই কমান্ড ডিজ্যাবল হয় এবং নেটওয়ার্কে নিয়ন্ত্রণ করা যায়।

চিত্র-৬

স্টাক্সনেট

স্টাক্সনেট নামের কমপিউটার ওয়ার্ম শনাক্ত হয় ২০১০ সালের জুনে। কথিত আছে, ইরানের নিউক্লিয়ার স্থাপনায় আক্রমণ করার জন্য যুক্তরাষ্ট্র এবং ইসরায়েল এ ওয়ার্ম তৈরি করে। স্টাক্সনেট ওয়ার্ম প্রাথমিকভাবে বিস্তৃত হয় মাইক্রোসফট উইন্ডোজের মাধ্যমে এবং টার্গেট করে সিমেন্স ইন্ডাস্ট্রিয়াল কন্ট্রোল সিস্টেমসে।

স্টাক্সনেটের উইন্ডোজের বেশ কিছু জটিল ভালনারেবিলিটিকে কাজে লাগিয়ে নিজের স্বার্থ হাসিল করে, যা এখনও অজানাই রয়ে গেছে। এর সাথে সম্পৃক্ত রয়েছে আক্রান্ত ইউএসবি কী-কে টার্গেট সিস্টেমে ঢোকানো মাত্রই এক্সিকিউশনের ব্যাপারে নিশ্চয়তা, যদি কোনো সিস্টেমে অটোরান সক্ষমতাকে ডিজ্যাবল করা হয় তাহলেও তা কার্যকর হবে।

আক্রান্ত সিস্টেম থেকে স্টাক্সনেট অভ্যন্তরীণ নেটওয়ার্কে বিস্তৃত হতে সক্ষম হয়। যতক্ষণ পর্যন্ত না এটি কাঙ্ক্ষিত লক্ষ্যে পৌঁছছে। আর

চিত্র-৭

এটি সিমেন্সের তৈরি একটি ইন্ডাস্ট্রিয়াল কন্ট্রোল সিস্টেম। স্টাক্সনেট জানে সুনির্দিষ্ট কন্ট্রোলারের দুর্বল দিক এবং বেশিরভাগ ক্ষেত্রে তা ধ্বংস করা, যা ইন্ডাস্ট্রিয়াল সিস্টেমকে নিষ্ক্রিয় করে দেয়।

ফ্লেম ম্যালওয়্যার

২৮ মে ২০১২ সালে ফ্লেম নামের কমপিউটার মডিউলার ম্যালওয়্যার শনাক্ত হয়, যা মাইক্রোসফট উইন্ডোজ অপারেটিং সিস্টেমচালিত কমপিউটারে আক্রমণ করে। ফ্লেমের টার্গেট করা বেশিরভাগ কমপিউটারই হলো মধ্যপ্রাচ্যের। এ প্রোগ্রামটি ব্যবহার করা হয় সাইবার গোয়েন্দা হিসেবে।

ফ্লেম লোকাল নেটওয়ার্ক অথবা ইউএসবি স্টিকের মাধ্যমে অন্যান্য সিস্টেমে বিস্তৃত হতে পারে। এটি অডিও, স্ক্রিনশট, কীবোর্ড অ্যাক্টিভিটি এবং নেটওয়ার্ক ট্রাফিক রেকর্ড করে রাখতে পারে। এটি স্কাইপি কথোপকথন রেকর্ড করতে পারে এবং ব্লু টুথে সংক্রমিত কমপিউটারে রূপান্তর হতে পারে, যা চেষ্টা করে কাছাকাছি ব্লুটুথ এনাবল ডিভাইস থেকে কন্টাক্ট তথ্য ডাউনলোড করতে চেষ্টা করে।

চিত্র-৮

ক্যাসপারস্কির মতে, ২০১২ সালের মে মাসের মধ্যে প্রাথমিকভাবে আনুমানিক ১০০০ মেশিনকে আক্রান্ত করে, যার বেশিরভাগই ইরান, ইসরায়েল, সুদান, সিরিয়া, লেবানন, সৌদি আরব, মিসরে।

এরপর কী

উপরের আলোচনা পর্যালোচনা করলে দেখা যায়, সাইবার অপরাধীদের পরবর্তী টার্গেট স্মার্টফোন কজ

ফিডব্যাক : mahmood_sw@yahoo.com