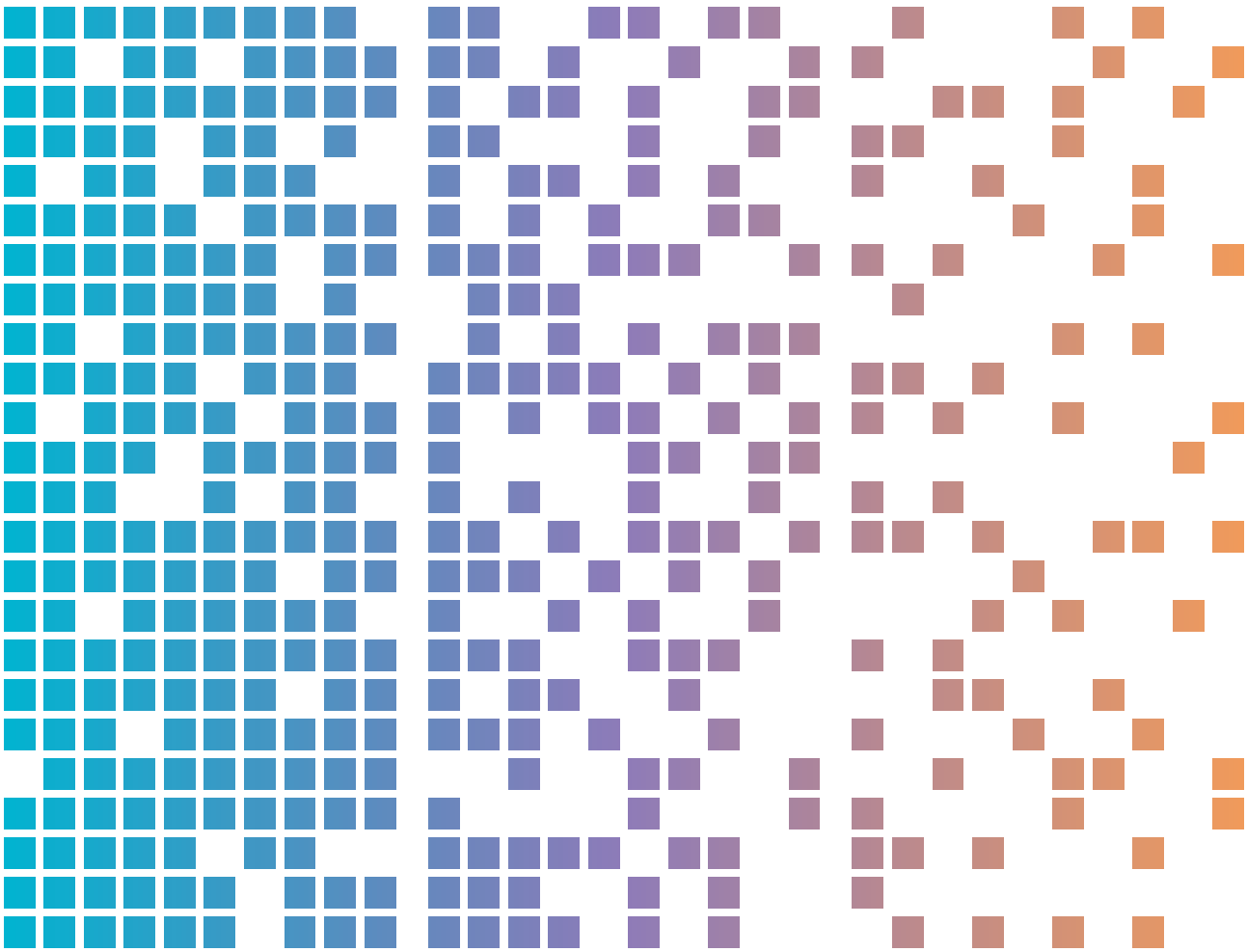
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

নীরব ডাকাতি: সাইবার অপরাধীরা ইনফো স্টিলার ম্যালওয়্যার ব্যবহার করে কর্পোরেট নেটওয়ার্কে হানা দেয়



কন্টেন্ট এর জটিলতা
মাঝারি

সূচিপত্র

প্রেক্ষাপট

ইনফরমেশন স্টিলার ম্যালওয়্যার ব্যবহার করে সাইবার অপরাধীরা ব্যবহারকারীর লগইন তথ্য ও সিস্টেম সম্পর্কিত তথ্য চুরি করে, যা তারা সাধারণত অর্থ উপার্জনের উদ্দেশ্যে ব্যবহার করে। বিশ্বজুড়ে, অস্ট্রেলিয়ায় সহ, বিভিন্ন প্রতিষ্ঠান ও খাতে এই ধরনের সাইবার আক্রমণের ঘটনা দেখা গেছে। এই প্রকাশনায় ইনফরমেশন স্টিলার ম্যালওয়্যার সম্পর্কে সাইবার নিরাপত্তা নির্দেশনা দেওয়া হয়েছে, যার মধ্যে প্রতিষ্ঠান ও কর্মীদের জন্য হুমকির ধরন ও প্রতিরোধমূলক পরামর্শ রয়েছে।

মূল বিষয়সমূহ

- ইনফরমেশন স্টিলার ম্যালওয়্যার, যা "ইনফো স্টিলার" নামেও পরিচিত, এটি এমন এক ধরনের ম্যালওয়্যার যা ভুক্তভোগীর ডিভাইস থেকে তথ্য সংগ্রহ করার জন্য তৈরি করা হয়েছে। এই তথ্যের মধ্যে থাকতে পারে ইউজারনেম ও পাসওয়ার্ড, ক্রেডিট কার্ডের তথ্য, ক্রিপ্টোকারেন্সি ওয়ালেট, লোকাল ফাইল, কুকি সহ ব্রাউজার ডেটা, ব্যবহারকারীর ইতিহাস ও অটোফিল ফর্মের তথ্য।
- সাইবার অপরাধীরা এসব চুরি করা ইউজার ক্রেডেনশিয়াল কিনে নিয়ে কর্পোরেট অ্যাকাউন্টে প্রবেশ করে ভিকটিমের কর্মস্থল, ক্লায়েন্ট বা অন্যান্য এন্টারপ্রাইজ সিস্টেমে প্রাথমিক অ্যাক্সেস পায়। এর ফলে প্রতিষ্ঠানগুলো র‍্যানসমওয়্যার, চাঁদাবাজি, ব্যবসায়িক ইমেইল হ্যাক এবং বুদ্ধিবৃত্তিক সম্পত্তি চুরির মতো গুরুতর সাইবার হামলার শিকার হতে পারে।
- ASD-এর ACSC লক্ষ্য করেছে যে অনেক কর্পোরেট নেটওয়ার্ক হ্যাক হয়েছে, কারণ কর্মীরা ব্যক্তিগত ডিভাইস থেকে কাজের রিসোর্সে অ্যাক্সেস করেছে—যেগুলো আগে থেকেই হ্যাক করা ছিল। অনেক ক্ষেত্রে, চুরি করা বৈধ ব্যবহারকারীর লগইন তথ্য ব্যবহার করে সাইবার অপরাধীরা কর্পোরেট নেটওয়ার্কে প্রবেশ করেছে। আমাদের তদন্তে দেখা গেছে, সাইবার অপরাধীরা যখন উচ্চ পর্যায়ের ব্যবহারকারীর অ্যাকাউন্টে সফলভাবে প্রবেশ করে, তখনই সবচেয়ে বড় ধরনের নিরাপত্তা লঙ্ঘনের ঘটনা ঘটে।
- যেসব প্রতিষ্ঠান কর্মী, কনট্রাক্টর, ম্যানেজড সার্ভিস প্রোভাইডার বা অন্যান্য পক্ষকে রিমোটলি নেটওয়ার্কে অ্যাক্সেস করার সুযোগ দেয়—বিশেষ করে BYOD (নিজস্ব ডিভাইস ব্যবহারের অনুমতি) থাকলে—তাদের ইনফো স্টিলার ম্যালওয়্যারের ঝুঁকি সম্পর্কে সচেতন থাকা এবং নিজেদের সুরক্ষিত রাখা জরুরি। সাইবার অপরাধীরা বিভিন্ন কৌশল ব্যবহার করে ইনফো স্টিলার ম্যালওয়্যার ছড়িয়ে দেয়, যেমন, ফিশিং ইমেইল, পাইরেটেড সফটওয়্যার ডাউনলোড, সার্চ ইঞ্জিন অপ্টিমাইজেশন (SEO) কৌশল, ক্ষতিকর বিজ্ঞাপন, কিংবা সোশ্যাল মিডিয়ায় পোস্ট করা ক্ষতিকর লিংক। সাধারণভাবে, যেসব ডিভাইস ব্যক্তিগত ও কর্মসংক্রান্ত কাজে একসাথে ব্যবহার করা হয়, সেগুলোতে ইনফো স্টিলার ম্যালওয়্যার সংক্রমণের ঝুঁকি বেশি—এর পেছনে কারণ হলো ব্যবহারকারীর আচরণ ও দুর্বল সিকিউরিটি কন্ট্রোল।
- ইনফো স্টিলার ম্যালওয়্যার সাইবার অপরাধীদের জন্য একটি আকর্ষণীয় মডেল, কারণ এটি সহজে আর্থিক লাভ এনে দেয়, বিশেষ করে নতুন অপরাধীদের জন্য, যাদের প্রযুক্তিগত দক্ষতা সীমিত। কিছু কিছু সাইবার অপরাধী "Malware-as-a-Service (MaaS)" স্টাইলের প্রোগ্রামের মাধ্যমে ইনফো স্টিলার বিক্রি করে—যেখানে মাসিক সাবস্ক্রিপশন ফি দিয়ে এই ম্যালওয়্যার ব্যবহার করা যায়।

পটভূমি

সাইবার অপরাধীরা যখন ইনফো স্টিলার ম্যালওয়্যার ব্যবহার করে, তখন তা অস্ট্রেলিয়ান প্রতিষ্ঠানগুলোর নিরাপত্তা ও স্থিতিশীলতার জন্য হুমকি হয়ে দাঁড়ায়। ইনফো স্টিলার সংক্রমণ সাধারণত বড় সাইবার নিরাপত্তা ঘটনার পূর্বাভাস হিসেবে দেখা যায়, কারণ অপরাধীরা এগুলো ব্যবহার করে ব্যবহারকারীর লগইন তথ্য সংগ্রহ করে। ব্যবহারকারীর এই লগইন তথ্য, বিশেষ করে যেগুলো ইন্টারনেটে যুক্ত রিমোট সার্ভিস বা উচ্চ পর্যায়ের অ্যাকাউন্টে অ্যাক্সেস দেয়, সেগুলো ব্যবহার করে অপরাধীরা কর্পোরেট সিস্টেম ও ডেটায় প্রাথমিক প্রবেশ করে।

> **নোট:** ইনিশিয়াল অ্যাক্সেস ব্রোকাররা চুরি করা ব্যবহারকারীর লগইন তথ্য কেনা ও যাচাই করার মাধ্যমে সাইবার অপরাধ জগতে একটি বিশেষ ভূমিকা পালন করে। এরপর তারা উচ্চমানের ইউজার ক্রেডেনশিয়াল—বিশেষ করে কর্পোরেট পরিবেশে ব্যবহৃত অ্যাকাউন্ট—অন্যান্য সাইবার অপরাধীদের কাছে নিলামে বিক্রি করে, যারা এই ক্রেডেনশিয়াল ব্যবহার করে প্রতিষ্ঠানের নেটওয়ার্কে প্রবেশ করে।

চুরি করা বৈধ ইউজার ক্রেডেনশিয়াল সাইবার অপরাধীদের কাছে অত্যন্ত মূল্যবান, কারণ এগুলো ব্যবহার করে তারা দ্রুত ও সহজে কর্পোরেট সিস্টেমে প্রবেশ করতে পারে। চুরি হওয়া বৈধ ক্রেডেনশিয়াল ব্যবহার করে সাইবার অপরাধীরা নিচের কিছু সাধারণ কৌশল এড়িয়ে যেতে পারে:

- টার্গেটকে শনাক্ত করে তার সম্পর্কে তথ্য সংগ্রহ
- টার্গেটের নেটওয়ার্কের দুর্বলতা খুঁজে বের করা
- প্রাথমিক অ্যাক্সেসের জন্য সম্ভাব্য পথ তৈরি করা, যেমন:
  - ফিশিং কনটেন্ট তৈরি
  - সফটওয়্যারের দুর্বলতা কাজে লাগানো
  - রিমোট ডেস্কটপ প্রোটোকল (RDP) বা ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN) সার্ভিসসহ রিমোট সার্ভিসগুলোকে লক্ষ্য করে সাইবার আক্রমণ চালানো।
  - ব্যবহারকারীর লগইন তথ্য আন্দাজ (পাসওয়ার্ড অনুমান) করে বারবার চেষ্টা চালানো।

এই ধাপগুলো সম্পন্ন করতে সময় ও প্রযুক্তিগত দক্ষতা দরকার হয়, যা অনেক সাইবার অপরাধীর জন্য বাধা হয়ে দাঁড়ায়। বিশেষ করে, যারা কর্পোরেট নেটওয়ার্কের প্রতিরক্ষা ভেদ করতে পারে না, তারা ইনফো স্টিলার সংক্রমণ থেকে সরাসরি লাভবান হয়—কারণ এই সংক্রমণগুলো কর্পোরেট নেটওয়ার্কে প্রবেশের জন্য দ্রুত ও সহজ ইউজার ক্রেডেনশিয়াল আক্সেস সরবরাহ করে।

রিমোট কাজের পরিবেশে, কিছু কর্মী ব্যক্তিগত ডিভাইস ব্যবহার করে কাজ ও ব্যক্তিগত ব্রাউজিং—দুইই করে। এতে তারা ওয়েব ব্রাউজারের পাসওয়ার্ড স্টোর বা এক্সটেনশন-এ তাদের ইউজার ক্রেডেনশিয়াল সংরক্ষণ করতে পারে, অথবা ওয়েব ব্রাউজারের অটোফিল ফিচার ব্যবহার করতে পারে। ইনফো স্টিলার ম্যালওয়্যার ওয়েব ব্রাউজারে সংরক্ষিত পাসওয়ার্ড স্টোর, অথেনটিকেশন কুকিজ এবং অন্যান্য ব্যক্তিগত তথ্যকে লক্ষ্যবস্তু করে।

কর্পোরেট ডিভাইসের তুলনায় ব্যক্তিগত ডিভাইসে সাধারণত এন্টারপ্রাইজ সিকিউরিটি পলিসি প্রয়োগ করা হয় না, যার ফলে প্রতিষ্ঠানগুলোর জন্য ঝুঁকি বেড়ে যায়। উদাহরণস্বরূপ, কর্মীরা পাইরেটেড সফটওয়্যার ডাউনলোড বা উচ্চ-ঝুঁকিপূর্ণ ব্রাউজিং-এ জড়িয়ে পড়তে পারে, যা তাদের সাইবার হুমকি ও ম্যালওয়্যার সংক্রমণের ঝুঁকিতে ফেলতে পারে।

ইনফো স্টিলার, ডিস্ট্রিবিউটর, ইনিশিয়াল অ্যাক্সেস ব্রোকার এবং র‍্যানসমওয়্যার অ্যাফিলিয়েটরা এখন আর্থিক লাভের উদ্দেশ্যে পরিচালিত একটি সাইবার অপরাধ ইকোসিস্টেমের মূল অংশ। এই ইকোসিস্টেম আরও কার্যকর হয়ে ওঠে যখন সাইবার অপরাধীরা আক্রমণের নির্দিষ্ট ধাপগুলোতে সক্ষমতা অর্জন করে এবং সেই সক্ষমতা সার্ভিস হিসেবে অন্য অপরাধীদের কাছে বিক্রি করে।

হুমকি প্রদানকারী কার্যকলাপ

ASD-এর ACSC অস্ট্রেলিয়ান নেটওয়ার্কগুলোর জন্য একটি বাড়তে থাকা হুমকি হিসেবে বিশ্বব্যাপী ইনফো স্টিলার ক্রমবর্ধমান কার্যকলাপ পর্যবেক্ষণ ও নজরদারি করছে। শিল্প-ভিত্তিক রিপোর্ট অনুযায়ী, ২০২৩ সালে ইনফো স্টিলার ছিল সাইবার অপরাধে ব্যবহৃত সবচেয়ে জনপ্রিয় ম্যালওয়্যার ভ্যারিয়েন্ট। ডার্ক ওয়েব মার্কেটপ্লেসে চুরি হওয়া ডেটার বিক্রয় বৃদ্ধি এবং এই ডেটা ব্যবহার করে ইনিশিয়াল অ্যাক্সেস ব্রোকারদের কার্যকলাপ বৃদ্ধি—এই ক্রমবর্ধমান প্রবণতাকে প্রতিফলিত করে, যা ২০২৪ সালে আরও তীব্র হয়েছে।

তথ্য চুরি-ভিত্তিক সাইবার অপরাধের পরিকাঠামো

ষ্টেজ ১: ম্যালওয়্যার সংগ্রহ করা

ইনফো স্টিলার সাধারণত সাইবার অপরাধীদের মার্কেটপ্লেসে MaaS বা Stealer-as-a-Service হিসেবে অফার করা হয়, অথবা সোর্স কোড আকারে বিক্রি করা হয়। MaaS বলতে বোঝায় এমন একটি ব্যবসায়িক মডেল, যেখানে ম্যালওয়্যার ডেভেলপাররা একটি ওয়েব-ভিত্তিক প্ল্যাটফর্মের মাধ্যমে তাদের ক্ষতিকর সফটওয়্যার অন্যদের কাছে সাবস্ক্রিপশন ভিত্তিতে বিক্রি করে, যা দেখতে অনেকটা বৈধ Software-as-a-Service এর মতো। MaaS মডেলটি সাইবার অপরাধে প্রবেশের বাধা কমিয়ে দিয়েছে, কারণ এটি প্রযুক্তিগত দক্ষতা ছাড়াই সাইবার অপরাধীদের ম্যালওয়্যার ছড়াতে ও চুরি করা তথ্য সংগ্রহ করতে সক্ষম করে।

MaaS হিসেবে অফার করা ইনফো স্টিলার সাধারণত কম খরচে মাসিক ফিতে বিজ্ঞাপন দেওয়া হয়, এবং এতে একটি ইনফো স্টিলার ড্যাশবোর্ডে অ্যাক্সেস দেওয়া হয়—যার মাধ্যমে সাইবার অপরাধীরা ম্যালওয়্যার তৈরি, চুরি করা ডেটা সংগঠিত এবং সংক্রমিত সিস্টেম ট্র্যাক করতে পারে। ড্যাশবোর্ডের মাধ্যমে ইনফো স্টিলার ম্যালওয়্যার তৈরি করা, চুরি করা ডেটা সংগঠিত করা এবং সংক্রমিত সিস্টেমের সংখ্যা ট্র্যাক করা যায়। MaaS অপারেটররা নিয়মিত ফিচার আপডেট, টুলস ও টেকনিক্যাল সাপোর্ট প্রদান করে, যাতে তারা অ্যান্টিভাইরাস সফটওয়্যার দ্বারা ধরা পড়া এড়াতে পারে এবং গ্রাহকদের আকৃষ্ট ও ধরে রাখতে পারে। অনেক ইনফো স্টিলার ম্যালওয়্যার ডেটা চুরি করার পর নিজেই ভিকটিমের ডিভাইস থেকে মুছে যেতে সক্ষম।

ষ্টেজ ২: বিতরণ

যেসকল সাইবার অপরাধী ইনফো স্টিলার ম্যালওয়্যার ছড়ায় এবং সংক্রমিত ডিভাইস থেকে তথ্য সংগ্রহ করে, তাদের ‘ট্র্যাফার’ (traffic distributors) বলা হয়। ট্র্যাফাররা ভিকটিমদের ম্যালিশাস লিংকে রিডাইরেক্ট করে, যার মাধ্যমেবিস্তৃত ক্যাম্পেইনের অংশ হিসেবে ইনফো স্টিলার ছড়ানো হয় । বেশিরভাগ ক্যাম্পেইন অবিকল্পিত ও সুযোগসন্ধানী সংক্রমণের উপর নির্ভর করে। তবে কিছু ক্যাম্পেইন নির্দিষ্ট ইন্ডাস্ট্রি বা সেক্টরের জন্য কাস্টমাইজড হয় এবং এতে নির্দিষ্ট ভিকটিমদের লক্ষ্য করে স্পিয়ার-ফিশিং ব্যবহার করা হয় । ট্র্যাফাররা এই ধরনের গ্রাহকের চাহিদা অনুযায়ী টার্গেটেড ক্যাম্পেইন চালায় — যেমন, যখন ক্রেতারা উচ্চ-মূল্যবান প্রতিষ্ঠান বা সেক্টরে প্রবেশের জন্য অ্যাক্সেস খুঁজে থাকে।

ট্র্যাফাররা ইনফো স্টিলার ম্যালওয়্যার ভিকটিমদের ডিভাইসে ছড়িয়ে দিতে বিভিন্ন কৌশল ব্যবহার করে, যার মধ্যে রয়েছে:

- **বটনেট**: সাইবার অপরাধীদের দ্বারা নিয়ন্ত্রিত সংক্রমিত কম্পিউটার সিস্টেমের নেটওয়ার্ক, যা ফিশিং বার্তা বা ম্যালওয়্যার পাঠানোর মতো ক্ষতিকর কাজ করতে ব্যবহৃত হয়

- **ফিশিং**: প্রতারণার মাধ্যমে সংবেদনশীল তথ্য সংগ্রহের চেষ্টা—যেমন ইমেইল, সোশ্যাল মিডিয়া, ফোরাম বা মেসেজিং অ্যাপে পাঠানো বার্তার মাধ্যমে—যা সাইবার অপরাধীদের জন্য প্রবেশের বাধা কমিয়ে দিয়েছে:
  - ইমেইলে সরাসরি ক্ষতিকর ফাইল সংযুক্ত না করে এই ধরনের বার্তাগুলোতে সাধারণত ক্ষতিকর লিংক থাকে, ।
- **ম্যালিশাস সার্চ রেজাল্ট**: সার্চ ইঞ্জিন অপ্টিমাইজেশন (SEO) কৌশল ব্যবহার করে ভিকটিমদের এমন ওয়েবসাইটে পাঠানো হয়, যেখানে ম্যালওয়্যারকে বৈধ সফটওয়্যার বা কনটেন্ট হিসেবে ছদ্মবেশে উপস্থাপন করা হয়।
- **ম্যালভারটাইজিং**: বৈধ অনলাইন বিজ্ঞাপনে ক্ষতিকর কোড ইনজেক্ট করে ম্যালওয়্যার ছড়ানো হয়।
- **ক্র্যাকড বা পাইরেটেড সফটওয়্যার**: যেমন ভিডিও গেমস, YouTube ভিডিওর মাধ্যমে শেয়ার করা হয়, যেখানে ভিডিওর বিবরণ বা কমেন্টে ম্যালিশাস লিংক থাকে, অথবা অবিশ্বস্ত ডাউনলোড সাইট থেকে।
- **সোশ্যাল মিডিয়া বিজ্ঞাপন ও পোস্ট**: ভিকটিমদের ছদ্মবেশী ম্যালওয়্যার ফাইলে রিডাইরেক্ট করে।
- **ক্ষতিকর সফটওয়্যার আপডেট**: সাধারণত ওয়েব ব্রাউজার আপডেটের ছদ্মবেশে থাকে।

ষ্টেজ ৩: তথ্য সংগ্রহের প্রক্রিয়া

একবার ইনফো স্টিলার ম্যালওয়্যার ভিকটিমের ডিভাইসে কার্যকর হলে, এটি সংক্রমিত মেশিন থেকে সংবেদনশীল তথ্য সংগ্রহ শুরু করে। ব্যবহারকারীর লগইন তথ্য চুরি ছাড়াও, যদি ইনফো স্টিলার বটনেটের অংশ হয়, তাহলে সাইবার অপরাধীরা রিমোটলি ডিভাইস নিয়ন্ত্রণ করতে পারে—যেমন কনফিগারেশন কমান্ড পাঠিয়ে অতিরিক্ত ফিচার চালু করা বা অন্য ম্যালওয়্যার ডেলিভারি করা। সাধারণভাবে, ইনফো স্টিলার ম্যালওয়্যার নিচের তথ্য চুরি করতে সক্ষম:

- ইউজারনেম ও পাসওয়ার্ড বিশেষ করে যেগুলো ওয়েব ব্রাউজারে সংরক্ষিত MFA (মাল্টি-ফ্যাক্টর অথেনটিকেশন) সেশন / টোকেন আকারে থাকে
- অথেনটিকেশন কুকিজ
- ওয়েব ব্রাউজারের অটোফিল ফর্ম তথ্য
- ইমেইল ক্রেডেনশিয়াল, ইমেইলের বিষয়বস্তু ও ঠিকানা
- ওয়েব ব্রাউজিং এর ইতিহাস
- ইউজার ডকুমেন্ট
- ক্রেডিট কার্ডের তথ্য
- ডেস্কটপ মেসেজিং অ্যাপের চ্যাট লগ
- সিস্টেম সম্পর্কিত তথ্য
- ক্রিপ্টোকারেন্সি ওয়ালেট
- VPN বা ফাইল ট্রান্সফার প্রোটোকল (FTP) ক্রেডেনশিয়াল

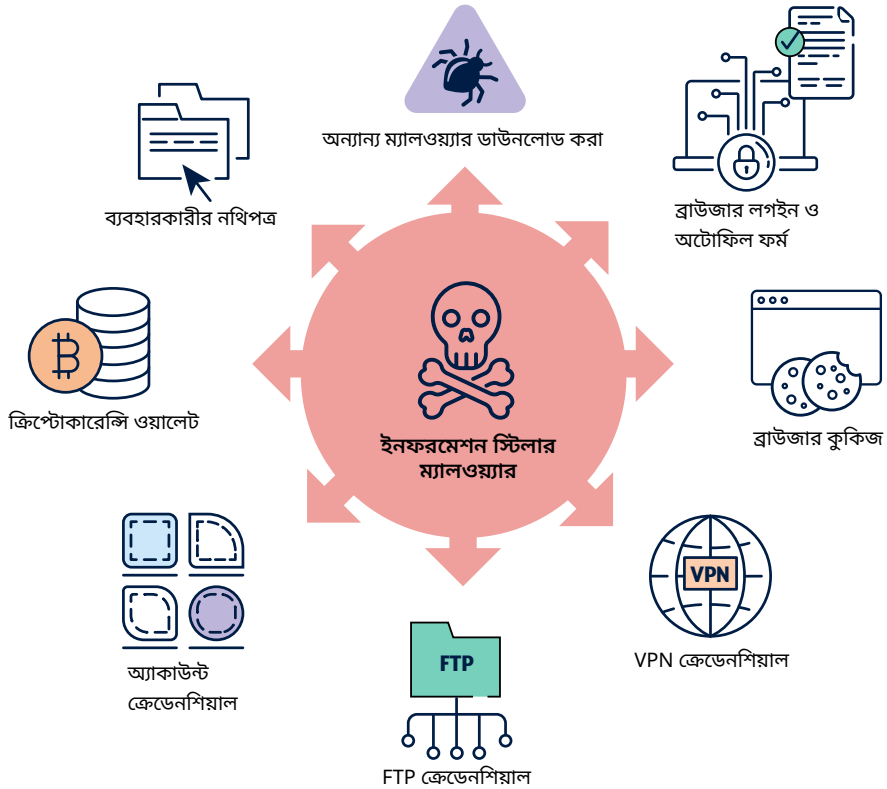


Figure 1. ইনফো স্টিলারের সক্ষমতা

কিছু ওয়েব ব্রাউজার অথেনটিকেশন কুকিজ ব্যবহারকারীকে একাধিক দিন ধরে লগইন অবস্থায় রাখে, যাতে বারবার লগইন করতে না হয়। যদি এই কুকিজ চুরি হয়ে যায়, তাহলে তা মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) এড়িয়ে সাইবার অপরাধীদের ভিকটিমের অ্যাকাউন্ট, কর্পোরেট নেটওয়ার্ক এবং এন্টারপ্রাইজ সিস্টেমে প্রবেশের সুযোগ দিতে পারে।

ষ্টেজ ৪: ডেটা সংগ্রহ ও অর্থায়ন

ইনফো স্টিলার ম্যালওয়্যার ভিকটিমের তথ্য যা ‘লগ’ নামে পরিচিত, চুরি করে ক্ষতিকর কমান্ড-অ্যান্ড-কন্ট্রোল সার্ভারে পাঠায়। সাধারণভাবে, ইনফো স্টিলাররা টেলিগ্রাম ও ডিসকর্ড-এর মতো জনপ্রিয় মেসেজিং অ্যাপ ব্যবহার করে সাইবার অপরাধীদের সঙ্গে লগ শেয়ার করে।

টেলিগ্রাম ও ডার্ক ওয়েবে লগ বিক্রি ও বিনিময়ের জন্য বিশেষায়িত মার্কেটপ্লেস রয়েছে। সাইবার অপরাধীরা বিভিন্নভাবে লগ থেকে অর্থ উপার্জন করে, যেমন:

- অবৈধ মার্কেটপ্লেসে লগগুলি বিক্রি করা, যেমন ইনিসিয়াল অ্যাক্সেস ব্রোকারদের কাছে
- পরিচয় চুরি ও ব্ল্যাকমেইলের মাধ্যমে ভিকটিমকে সরাসরি ফাঁদে ফেলা
- কর্পোরেট নেটওয়ার্কে প্রবেশের জন্য তথ্য ব্যবহার করে র‍্যানসমওয়্যার আক্রমণ চালানো।

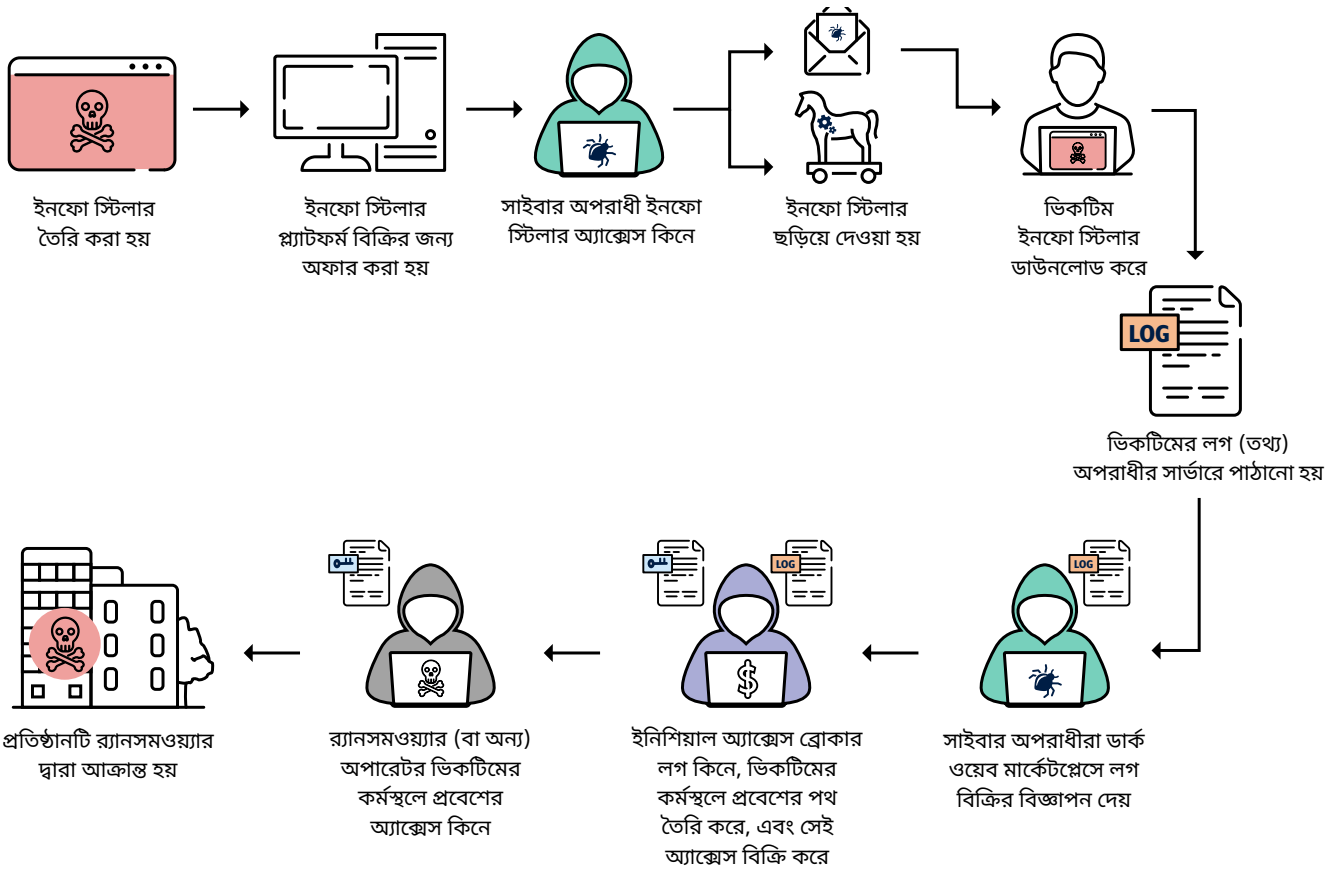


Figure 2. ইনফো স্টিলার ইকোসিস্টেম এবং একটি প্রতিষ্ঠানের উপর সম্ভাব্য প্রভাব

প্রভাব

ইনফো স্টিলার ম্যালওয়্যার ব্যক্তি ও প্রতিষ্ঠানের জন্য গুরুতর প্রভাব ফেলতে পারে। যেখানে ইনফো স্টিলার ইউজার ক্রেডেনশিয়াল সংগ্রহ করে, সেখানে সাইবার অপরাধীরা সেই বৈধ ইউজার অ্যাকাউন্ট ব্যবহার করে কর্পোরেট নেটওয়ার্ক বা এন্টারপ্রাইজ সিস্টেমে প্রবেশ করতে পারে, যা সিস্টেম মালিকদের পক্ষে শনাক্ত করতে দেরি করিয়ে দেয়।

ইনফো স্টিলার দ্বারা আক্রান্ত **প্রতিষ্ঠানগুলোর** জন্য সম্ভাব্য পরিণতির মধ্যে রয়েছে:

- র‍্যানসমওয়্যার
- ডেটা লিক বা তথ্য ফাঁস
- বিজনেস ইমেইল হ্যাক
- মেধাস্বত্ব চুরি
- সংবেদনশীল তথ্য চুরি।

ইনফো স্টিলার দ্বারা আক্রান্ত **ব্যক্তির** জন্য সম্ভাব্য পরিণতির মধ্যে রয়েছে:

- ব্যক্তিগত ইমেইল বা সোশ্যাল মিডিয়া অ্যাকাউন্টে অননুমোদিত প্রবেশ
- পরিচয় চুরির ঝুঁকি বৃদ্ধি
- ফিশিং আক্রমণের ঝুঁকি বৃদ্ধি
- আর্থিক ক্ষতি বা অর্থ সংক্রান্ত অ্যাকাউন্টে অননুমোদিত প্রবেশ
- গোপনীয়তা হারানো।

কেইস স্টাডিঃ

এই কেস স্টাডিটি জনসাধারণের জন্য প্রকাশযোগ্য করার উদ্দেশ্যে বেনামী করা হয়েছে। এটি ASD-এর ACSC-তে রিপোর্ট করা একাধিক সাইবার নিরাপত্তা ঘটনার উপর ভিত্তি করে তৈরি, যা অস্ট্রেলিয়ান সংস্থাগুলিকে ক্ষতিগ্রস্ত করেছে। ক্ষতিগ্রস্ত প্রতিষ্ঠানটিকে এখানে 'সংস্থা' নামে উল্লেখ করা হয়েছে। এই কেস স্টাডিতে ব্যক্তিদের নাম কাল্পনিক এবং ভিকটিমদের পরিচয় রক্ষার্থে কিছু তথ্য সরিয়ে ফেলা হয়েছে।

সংস্থাটি একটি অস্ট্রেলিয়ান ব্যবসা প্রতিষ্ঠান, যেখানে কর্মীরা ব্যক্তিগত ডিভাইস ব্যবহার করে কর্পোরেট সিস্টেমে প্রবেশ করতে পারে। অ্যালিস একটি প্রতিষ্ঠানের কর্মচারী, যিনি দূর থেকে কাজ করেন। বাসা থেকে কাজ করার সময়, অ্যালিস তার ব্যক্তিগত ল্যাপটপ ব্যবহার করে প্রতিষ্ঠানের কর্পোরেট নেটওয়ার্কে প্রবেশ করেন। অ্যালিস তাঁর কাছে বৈধ মনে হয়েছে এমন একটি ওয়েবসাইট থেকে Notepad++ নামক নোট নেওয়ার সফটওয়্যারের একটি সংস্করণ **নিজের ল্যাপটপে ডাউনলোড** করেন। Notepad++ সফটওয়্যারের ইনস্টলার হিসেবে ছদ্মবেশে একটি **ইনফো স্টিলার** (তথ্য চুরি করার ম্যালওয়্যার) লুকানো ছিল। অ্যালিস যখন সফটওয়্যারটি ইনস্টল করার চেষ্টা করেন, তখন ইনফো স্টিলার সক্রিয় হয়ে তার ল্যাপটপ থেকে **ইউজার ক্রেডেনশিয়াল সংগ্রহ করতে** শুরু করে। এর মধ্যে ছিল তার কর্মস্থলের ইউজারনেম ও পাসওয়ার্ড, যা তিনি ওয়েব ব্রাউজারের সেভড লগইন ফিচারে সংরক্ষণ করেছিলেন। ইনফো স্টিলার সেই ইউজার ক্রেডেনশিয়াল একটি দূরবর্তী কমান্ড-অ্যান্ড-কন্ট্রোল সার্ভারে পাঠিয়ে দেয়, যা একটি সাইবার অপরাধী গোষ্ঠীর নিয়ন্ত্রণে ছিল।

চুরি করা লগগুলো অন্যান্য লগের সঙ্গে একত্রিত করে ডার্ক ওয়েব মার্কেটপ্লেসে **সাইবার অপরাধীদের কাছে বিক্রি করা হয়**। 'বব' নামক এক সাইবার অপরাধী অ্যালিসের ইউজার ক্রেডেনশিয়াল কিনে নেয়, যা তার প্রতিষ্ঠানের নেটওয়ার্কে ব্যবহৃত বিভিন্ন পরিষেবার জন্য ছিল। অ্যালিসের প্রতিষ্ঠান ঐ পরিষেবাগুলোর জন্য **মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) কনফিগার করেনি**, ফলে বব শুধুমাত্র চুরি করা ইউজার ক্রেডেনশিয়াল ব্যবহার করেই সফলভাবে কর্পোরেট নেটওয়ার্কে **অথেনটিকেট এবং প্রবেশ** করতে পারে। বব চুরি করা **বৈধ ইউজার ক্রেডেনশিয়াল** ব্যবহার করে অ্যালিসের প্রতিষ্ঠানের কর্পোরেট নেটওয়ার্কে অজান্তে প্রবেশ করে। এরপর বব প্রতিষ্ঠানের নেটওয়ার্কের অন্যান্য অংশে প্রবেশ করে সংস্থার সংবেদনশীল তথ্য শনাক্ত করে এবং তা চুরি করে কোম্পানিকে ব্ল্যাকমেইল করার উদ্দেশ্যে ব্যবহার করে। সংবেদনশীল তথ্য চুরি করার পর, বব প্রতিষ্ঠানের **ডেটাবেস ও ফাইল সিস্টেম এনক্রিপ্ট** করে অপ্রবেশযোগ্য করে তোলে।

প্রতিকার ব্যবস্থা

প্রতিষ্ঠানগুলো তাদের কর্পোরেট নেটওয়ার্কে সংযুক্ত ডিভাইসগুলোর উপর নিয়ন্ত্রণ আরোপ করতে নাও পারতে পারে, বিশেষ করে যেসকল কর্মী দূর থেকে কাজ করেন তাদের ব্যক্তিগত ডিভাইসের ক্ষেত্রে। ASD-এর ACSC সুপারিশ করে যে প্রতিষ্ঠানগুলো যেন ইনফো স্টিলার দ্বারা ইউজার ক্রেডেনশিয়াল চুরির ঝুঁকি থেকে নিজেদের রক্ষা করার জন্য নিয়ন্ত্রণ ব্যবস্থা বাস্তবায়নে মনোযোগ দেয়। এই প্রতিকারমূলক পদক্ষেপগুলোর মধ্যে রয়েছে:

কর্মীদের জন্য সাইবার নিরাপত্তা সচেতনতা প্রশিক্ষণ প্রদান

- কর্মীদের কার্যকর প্রশিক্ষণের মাধ্যমে লক্ষ্যভিত্তিক সোশ্যাল ইঞ্জিনিয়ারিং ও ক্ষতিকর ফাইল ডাউনলোড করা থেকে বিরত রাখা।
- ইনফো স্টিলার, তাদের বিতরণ পদ্ধতি এবং আপনার প্রতিষ্ঠানের জন্য ফিশিং হুমকি সম্পর্কে সচেতনতা বৃদ্ধি।

কর্পোরেট অ্যাকাউন্টগুলো সুরক্ষিত করা

- MFA বাস্তবায়ন করুন:
- বাহ্যিক ও অভ্যন্তরীণ পরিষেবা, সিস্টেম এবং সংবেদনশীল ডেটা রিপোজিটরিতে MFA বাস্তবায়ন করুন, বিশেষ করে ওয়েবমেইল, VPN এবং গুরুত্বপূর্ণ সিস্টেমে প্রবেশকারী উচ্চ পর্যায়ের ইউজার অ্যাকাউন্ট-এ। সর্বোত্তম পদ্ধতি হলো সব অ্যাকাউন্টে ফিশিং প্রতিরোধী MFA বাস্তবায়ন করা।
- ব্যবহার না হলে ইউজার অ্যাকাউন্ট নিষ্ক্রিয় করে দিন।
- অ্যাডমিনিস্ট্রেটর সুযোগ-সুবিধা সীমিত করুন:
- নেটওয়ার্ক প্রশাসন ও অন্যান্য প্রিভিলেজড কাজ শুধুমাত্র একটি নির্দিষ্ট, লকড-ডাউন ওয়ার্কস্টেশন (যেমন সিকিউর অ্যাডমিন ওয়ার্কষ্টেশন) ব্যবহার করে সম্পাদন করুন।
- সর্বনিম্ন-অধিকার নীতির অনুসরণে প্রশাসকদেরকে নির্দেশ দিন যেন তারা শুধুমাত্র সিস্টেম ব্যবস্থাপনার জন্য বিশেষাধিকারপ্রাপ্ত ইউজার অ্যাকাউন্ট ব্যবহার করেন এবং সাধারণ কাজের জন্য সাধারণ ব্যবহারকারী অ্যাকাউন্ট ব্যবহার করেন।
- বিশেষাধিকারপ্রাপ্ত ইউজার অ্যাকাউন্টগুলো (যেগুলো অনলাইন পরিষেবায় প্রবেশের জন্য স্পষ্টভাবে অনুমোদিত নয়) যেন ইন্টারনেট, ইমেইল ও ওয়েব পরিষেবায় প্রবেশ করতে না পারে, তা নিশ্চিত করুন।
- সিস্টেম ও অ্যাপ্লিকেশনের জন্য জাস্ট-ইন-টাইম প্রশাসন বাস্তবায়নের কথা বিবেচনা করুন।
- বিশেষাধিকারপ্রাপ্ত ইউজার অ্যাকাউন্টগুলোর পরিচালনা ও অডিটিং নিশ্চিত করুন।
- পাসওয়ার্ড নিয়মিত আপডেট করুন, বিশেষ করে বাহ্যিকভাবে সংযুক্ত রিমোট-অ্যাক্সেস অ্যাকাউন্টগুলোর জন্য।
- সেশন টোকেন ও কুকিজে নির্দিষ্ট সময়সীমা ও সানসেট নীতিমালা প্রয়োগ করুন।

এন্টারপ্রাইজ মোবিলিটি শক্তিশালী করুন

- প্রতিষ্ঠানের মোবিলিটি ঝুঁকি মূল্যায়ন করুন এবং এন্টারপ্রাইজ মোবিলিটি শক্তিশালীকরণ নির্দেশিকা বাস্তবায়ন করুন।
- যদি আপনি কর্মীদের ব্যক্তিগত ডিভাইস ব্যবহার করার অনুমতি দেন, তাহলে ব্রিং ইউর অউন ডিভাইস (BYOD) নীতিমালা বাস্তবায়ন করুন, কারণ প্রতিষ্ঠানের নিয়ন্ত্রিত ডিভাইস অনিয়ন্ত্রিত ব্যক্তিগত ডিভাইসের চেয়ে বেশি নিরাপদ।

আপনার নেটওয়ার্কে অ্যাক্সেস থাকা সরবরাহকারী, সফটওয়্যার-অ্যাস-এ-সার্ভিস (SaaS) ভেন্ডর এবং ম্যানেজড সার্ভিস প্রভাইডার এর সরবরাহ চেইনের ঝুঁকি পর্যালোচনা ও মূল্যায়ন করুন। ম্যানেজড সার্ভিস প্রভাইডার -এর সাথে যুক্ত হলে নিরাপত্তা কীভাবে পরিচালনা করবেন তা নিশ্চিত করুন।

কর্পোরেট নেটওয়ার্ক সুরক্ষিত করুন

- অ্যাপ্লিকেশন এবং অপারেটিং সিস্টেমসমূহ সর্বদা আপডেট রাখুন।
- অ্যাপ্লিকেশন কন্ট্রোল প্রয়োগ করার জন্য স্থানীয় নিরাপত্তা নীতিমালা প্রয়োগ করুন এবং কঠোর অ্যালাউ লিস্ট ব্যবহার করুন।
- ভূমিকা ও কার্যকারিতা অনুযায়ী নেটওয়ার্ক অংশগুলো আলাদাভাবে ভাগ করতে 'নেটওয়ার্ক সেগমেন্টেশন' বাস্তবায়ন করুন।
- ব্যবহারকারীর, বিশেষ করে দূরে কাজ করা কর্মীদের কার্যকলাপ নিরীক্ষণ ও পর্যবেক্ষণ করুন।
- প্রিভিলেজড অ্যাকাউন্ট মনিটরিং করলে সংবেদনশীল ডেটায় অননুমোদিত অ্যাক্সেস বা অস্বাভাবিক ডেটা ট্রান্সফার—যেমন বিশাল পরিমাণ ডেটা বাহ্যিক নেটওয়ার্কে আপলোড—উন্মোচিত হতে পারে।
- অননুমোদিত ডেটা ট্রান্সফার প্রতিরোধ করতে ডেটা-লস প্রিভেনশন নীতিমালা এবং টুলস বাস্তবায়ন করুন।

ASD-এর সাইবার সিকিউরিটি নেটওয়ার্ক পার্টনার হোন এবং ASD-এর সাইবার থ্রেট ইনটেলিজেন্স শেয়ারিং (CTIS) সার্ভিসে যোগ দিন।

- CTIS একটি দ্বিপাক্ষিক তথ্য আদান-প্রদান প্ল্যাটফর্ম যা সরকার ও শিল্পখাতের পার্টনারদের ক্ষতিকর সাইবার কার্যক্রম সম্পর্কিত তথ্য গ্রহণ এবং শেয়ার করার সুযোগ দেয়।
- ASD-এর ACSC ইনফো স্টিলার কার্যক্রম পর্যবেক্ষণ করছে এবং CTIS প্ল্যাটফর্মের মাধ্যমে সক্রিয় কমান্ড ও কন্ট্রোল ইনফ্রাস্ট্রাকচারের বিস্তারিত তথ্য শেয়ার করছে।
- পার্টনার হিসেবে নিবন্ধন করুন এবং সাইবার অপরাধের হুমকি থেকে আপনার প্রতিষ্ঠান ও গ্রাহকের তথ্য সুরক্ষিত করুন।

সম্ভাব্য তথ্য চুরির ঘটনা মোকাবেলার জন্য প্রস্তুত থাকুন।

- তথ্য চুরির ঘটনা ঘটলে ব্যবহারযোগ্য সাইবার নিরাপত্তা ঘটনার প্রতিক্রিয়া পরিকল্পনা তৈরি করুন। কর্মচারীরা যদি সন্দেহজনক ফাইল ডাউনলোড করেছেন বলে ধারণা করেন, তাহলে কী করতে হবে এবং কার সাথে যোগাযোগ করতে হবে তা তারা যেন জানেন তা নিশ্চিত করুন।

ASD-এর ACSC-এর এসেনশিয়াল এইট বাস্তবায়ন করুন।

- উপরে উল্লিখিত প্রতিরোধমূলক ব্যবস্থা ছাড়াও, ASD-এর ACSC দৃঢ়ভাবে পরামর্শ দেয় যেন ASD-এর ACSC-এর এসেনশিয়াল এইট -এর বাকি অংশসমূহও বাস্তবায়ন করা হয়।

রিমোটভাবে কাজ করার সময় কর্মচারীদের জন্য পরামর্শ।

- ব্যক্তিগত ডিভাইসে আপনার তথ্য সুরক্ষিত রাখুন।
  - ভালো সাইবার হাইজিন অনুশীলন করুন এবং সন্দেহজনক লিংকে ক্লিক করা, পপ-আপে সাড়া দেওয়া অথবা অজানা বা অবিশ্বস্ত উৎস থেকে ফাইল বা সফটওয়্যার ডাউনলোড করা থেকে বিরত থাকুন।
  - কাজ ও ব্যক্তিগত অ্যাকাউন্টের জন্য আলাদা পাসওয়ার্ড ব্যবহার করুন। সম্ভব হলে ব্যক্তিগত অ্যাকাউন্টে মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) ব্যবহার করুন।
  - কর্মস্থলের অনুমতি না থাকলে ব্যক্তিগত পাসওয়ার্ড ম্যানেজারে আপনার কাজের ক্রেডেনশিয়াল সংরক্ষণ করবেন না। এর মধ্যে আপনার ওয়েব ব্রাউজারের পাসওয়ার্ড ম্যানেজারও অন্তর্ভুক্ত। **সন্দেহ হলে, কর্পোরেটভাবে সমর্থিত পাসওয়ার্ড ম্যানেজার সরবরাহ করার জন্য আপনার কর্মস্থলকে অনুরোধ করুন।**
  - শেয়ার করা বা কমিউনাল ওয়ার্কস্টেশন থেকে কাজের অ্যাকাউন্টে লগইন করবেন না।
  - আপনার ওয়েব ব্রাউজারের অটোফিল ফিচারে কী কী সংরক্ষিত হচ্ছে সে সম্পর্কে সচেতন থাকুন। ইনফো স্টিলাররা ওয়েব ব্রাউজারের অটোফিল ফিচারে সংরক্ষিত ডেটাগুলি লক্ষ্য করে। ওয়েব ফর্ম পূরণ করার সময় ক্রেডিট কার্ড নম্বরের মতো সংবেদনশীল তথ্য ব্রাউজারে সংরক্ষণ না করে ম্যানুয়ালি এন্ট্রি করার বিষয়টি বিবেচনা করুন।
  - ব্রাউজিং সেশন শেষ হলে সব অনলাইন সার্ভিস থেকে লগআউট করুন এবং ওয়েব ব্রাউজারের কুকিজ ক্লিয়ার করুন, যাতে ইনফো স্টিলারদের পাওয়ার মতো তথ্য কম থাকে।
  - আপনার অপারেটিং সিস্টেমে বিল্ট-ইন অ্যান্টিভাইরাস সল্যুশন সক্রিয় রয়েছে কিনা তা নিশ্চিত করুন। আপনি যদি তৃতীয় পক্ষের অ্যান্টিভাইরাস সল্যুশন ব্যবহার করেন, তাহলে এটি আপডেট রাখা এবং খ্যাতনামা কোনো ভেন্ডরের কাছ থেকে নেওয়া হয়েছে কি না তা নিশ্চিত করুন।

সাহায্য

অস্ট্রেলিয়ান প্রতিষ্ঠানসমূহ যারা ইনফো স্টিলার সংক্রান্ত ঘটনায় ক্ষতিগ্রস্ত হয়েছে বা সহায়তা প্রয়োজন, তারা ASD-এর ACSC-এর সাথে **1300 CYBER1 (1300 292 371)** নম্বরে অথবা cyber.gov.au/report ওয়েবসাইটে রিপোর্ট জমা দিয়ে যোগাযোগ করতে পারে।

ASD-এর ACSC ইনফো স্টিলার সম্পর্কিত সন্দেহজনক নেটওয়ার্ক কার্যকলাপ এবং কম্প্রোমাইজ-এর লক্ষণ রিপোর্ট করার জন্য প্রতিষ্ঠানগুলিকে উৎসাহ দেয়, এমনকি ঘটনাটি নিয়ন্ত্রিত বলে মনে হলেও। আপনার প্রদান করা তথ্য সাইবার হুমকিসমূহের কার্যপ্রণালী, কৌশল এবং পদ্ধতি সম্পর্কে আমাদের ধারণাকে উন্নত করতে সহায়তা করে, যা একইভাবে লক্ষ্যবস্তু হওয়া অন্যান্য অস্ট্রেলিয়ান প্রতিষ্ঠানকে সতর্ক করতে সাহায্য করে।

দাবিত্যাগ

এই নির্দেশিকার তথ্য সাধারণ প্রকৃতির এবং কোনও বিশেষ পরিস্থিতিতে বা জরুরি পরিস্থিতিতে আইনি পরামর্শ হিসেবে বিবেচনা করা উচিত নয় অথবা সহায়তার জন্য এর উপর নির্ভর করা উচিত নয়। যেকোনো গুরুত্বপূর্ণ বিষয়ে, আপনার নিজের পরিস্থিতির ভিত্তিতে উপযুক্ত স্বাধীন পেশাদার পরামর্শ নেওয়া উচিত।

এই নির্দেশিকায় থাকা তথ্যের উপর নির্ভর করার কারণে যে কোনও ক্ষয় ক্ষতি বা ব্যয়ের জন্য কমনওয়েলথ কোনও দায়বদ্ধতা বা দায় স্বীকার করে না।

আরও তথ্যের জন্য, অথবা সাইবার নিরাপত্তা সংক্রান্ত কোনও ঘটনার প্রতিবেদন করতে, আমাদের সাথে যোগাযোগ করুন:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

এই নম্বরটি শুধুমাত্র অস্ট্রেলিয়ার মধ্যে ব্যবহারের জন্য উপলব্ধ।

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre