APT40 সতর্কতামূলক পরামর্শ

PRC MSS এর গোয়েন্দা কৌশলের ব্যবহার চলছে

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

সূচিপত্র

সারসংক্ষেপ

পটভূমি

এই সতর্কতামূলক পরামর্শ, অস্ট্রেলিয়ান সিগন্যাল ডিরেক্টরেটের অস্ট্রেলিয়ান সাইবার সিকিউরিটি সেন্টার (ASD এর ACSC), যুক্তরাষ্ট্রের সাইবার সিকিউরিটি অ্যান্ড ইনফ্রাস্ট্রাকচার সিকিউরিটি এজেন্সি (CISA), যুক্তরাষ্ট্রের জাতীয় নিরাপত্তা সংস্থা (NSA), যুক্তরাষ্ট্রের ফেডারেল ব্যুরো অব ইনভেস্টিগেশন (FBI), যুক্তরাজ্যের ন্যাশনাল সাইবার সিকিউরিটি সেন্টার (NCSC-UK), কানাডিয়ান সেন্টার ফর সাইবার সিকিউরিটি (CCCS), নিউজিল্যান্ড ন্যাশনাল সাইবার সিকিউরিটি সেন্টার (NCSC-NZ) যৌথভাবে এই পরামর্শ তৈরি করেছে। জার্মান ফেডারেল ইন্টেলিজেন্স সার্ভিস (BND) এবং সংবিধান সুরক্ষার জন্য ফেডারেল অফিস (BfV), কোরিয়া প্রজাতন্ত্রের জাতীয় গোয়েন্দা পরিষেবা (NIS) এবং NIS এর জাতীয় সাইবার সুরক্ষা কেন্দ্র এবং জাপানের জাতীয় ঘটনা প্রস্তুতি ও কৌশল কেন্দ্র (NISC) এবং জাতীয় পুলিশ সংস্থা (NPA) – যাদেরকে এখন থেকে "নির্দেশিকা প্রস্তুতকারী সংস্থা" হিসাবে উল্লেখ করা হয়েছে – গণপ্রজাতন্ত্রী চীন (পিআরসি) রাষ্ট্র সমর্থিত একটি সাইবার গ্রুপ এবং অস্ট্রেলিয়ার নেটওয়ার্কের প্রতি তাদের বর্তমান হুমকির রূপরেখা দেয়। এই সতর্কতামূলক পরামর্শটি তৈরি করা হয়েছে নির্দেশিকা প্রস্তুতকারী সংস্থাগুলোর যৌথ বোঝাপড়া এবং ASD-এর ACSC-র তদন্ত প্রতিবেদনগুলোর ভিত্তিতে।

চীনের রাষ্ট্রীয় পৃষ্ঠপোষকতায় পরিচালিত সাইবার গ্রুপটি এর আগে অস্ট্রেলিয়া এবং মার্কিন যুক্তরাষ্ট্র সহ বিভিন্ন দেশের সংস্থাগুলিকে লক্ষ্যবস্তু করেছে এবং নীচে উল্লিখিত কৌশলগুলি বিশ্বব্যাপী অন্যান্য চীন রাষ্ট্র সমর্থিত হ্যাকার গ্রুপ দ্বারা নিয়মিত ব্যবহৃত হয়। অতএব, নির্দেশিকা প্রস্তুতকারী সংস্থাগুলো বিশ্বাস করে যে গ্রুপটি এবং অনুরূপ কৌশলগুলি তাদের দেশের নেটওয়ার্কগুলির জন্যও হুমকি হিসাবে রয়ে গেছে।

নির্দেশিকা প্রস্তুতকারী সংস্থাগুলো মূল্যায়ন করে যে এই গোষ্ঠীটি পিআরসি রাষ্ট্রীয় সুরক্ষা মন্ত্রকের (এমএসএস) জন্য দূষিত সাইবার অপারেশন পরিচালনা করে। এই কার্যকলাপ ও প্রযুক্তিগুলো এমন একটি সাইবার হুমকি গোষ্ঠীর সঙ্গে সাদৃশ্যপূর্ণ, যেটিকে শিল্প প্রতিবেদনে APT 40 নামে শনাক্ত করা হয়েছে—যা ক্রিপটোনাইট পান্ডা, গিংহাম টাইফুন, লেভিয়াথান এবং ব্রোঞ্জ মোহক নামেও পরিচিত। এই দলটি এর আগে চীনের হাইনান প্রদেশের হাইকৌ শহরে অবস্থান করছে বলে রিপোর্ট করা হয়েছিল এবং তারা চীনের রাষ্ট্রীয় নিরাপত্তা সংস্থা—হাইনান স্টেট সিকিউরিটি ডিপার্টমেন্ট থেকে কাজের নির্দেশনা পেয়ে থাকে বলে জানা যায়।[2] নিম্নোক্ত সতর্কতামূলক পরামর্শটিতে এই সাইবার দুর্বৃত্তদের কৌশল ব্যবহারের উল্লেখযোগ্য কিছু ঘটনার উদাহরণ তুলে ধরা হয়েছে, যা দুটি ভুক্তভোগী নেটওয়ার্কের বিরুদ্ধে পরিচালিত হয়েছে। এই কেস স্টাডিগুলি সাইবার নিরাপত্তা বিশেষজ্ঞদের তাদের নিজস্ব নেটওয়ার্কে APT40 এর অনুপ্রবেশ সনাক্তকরণ, প্রতিরোধ এবং প্রতিকারের ক্ষেত্রে গুরুত্বপূর্ণ। যে ঘটনাগুলোর বিশ্লেষণ এখানে উপস্থাপন করা হয়েছে, সেগুলোর ক্ষেত্রে যথাযথ প্রতিকারমূলক ব্যবস্থা নেওয়া হয়েছে—ফলে এই সাইবার দুর্বৃত্ত কিংবা অন্য কোনও গোষ্ঠীর দ্বারা পুনরায় এই দুর্বলতাগুলোর অপব্যবহারের আশঙ্কা কমে গেছে। এই কারণে উপস্থাপিত ঘটনাগুলো স্বভাবতই কিছুটা পুরনো—যাতে সংশ্লিষ্ট প্রতিষ্ঠানগুলোকে যথাযথ প্রতিকারমূলক ব্যবস্থা নেওয়ার জন্য প্রয়োজনীয় সময় দেওয়া যায়।

কার্যক্রমের সংক্ষিপ্ত বিবরণ

APT40 বারবার অস্ট্রেলিয়ান নেটওয়ার্কসহ এই অঞ্চলের সরকারি ও বেসরকারি খাতের নেটওয়ার্ককে লক্ষ্যবস্তু করেছে, এবং আমাদের নেটওয়ার্কের প্রতি তারা যে হুমকি সৃষ্টি করেছে তা এখনও অব্যাহত রয়েছে। এই নির্দেশিকায় বর্ণিত কৌশলগুলো অস্ট্রেলিয়ার নেটওয়ার্কের বিরুদ্ধে নিয়মিতভাবে ব্যবহার হতে দেখা গেছে।

বিশেষভাবে উল্লেখযোগ্য যে, APT40 নতুন দুর্বলতাগুলোর প্রুফ-অফ-কনসেপ্ট (POC) দ্রুত পরিবর্তন ও অভিযোজিত করার সক্ষমতা রাখে এবং সংশ্লিষ্ট দুর্বলতাযুক্ত অবকাঠামো রয়েছে এমন নেটওয়ার্কগুলোর বিরুদ্ধে তাৎক্ষণিকভাবে ব্যবহার করতে পারে। APT40 নিয়মিতভাবে তাদের লক্ষ্যে থাকা নেটওয়ার্কগুলোর ওপর গোয়েন্দা নজরদারি চালায়—যার মধ্যে এই নির্দেশিকায় প্রস্তুতকারী সংস্থাগুলোর দেশের নেটওয়ার্কও অন্তর্ভুক্ত রয়েছে—যেখানে তারা দুর্বলতা খুঁজে বের করে লক্ষ্যে আঘাত হানার সুযোগ খোঁজে। এই নিয়মিত গোয়েন্দা নজরদারির মাধ্যমে দলটি তাদের লক্ষ্যে থাকা নেটওয়ার্কে দুর্বল, মেয়াদোত্তীর্ণ অথবা আর রক্ষণাবেক্ষণ করা হয় না—এমন ডিভাইস শনাক্ত করতে, এবং এসব দুর্বলতার ওপর দ্রুত হামলা চালাতে সক্ষম হয়। ২০১৭ সাল থেকে শুরু হওয়া দুর্বলতাগুলোর সুযোগ কাজে লাগিয়ে APT40 এখনও সফলভাবে সাইবার হামলা চালিয়ে যাচ্ছে।

APT40 দ্রুততার সাথে নতুন প্রকাশিত দুর্বলতাগুলোকে কাজে লাগায়, যা বহুল ব্যবহৃত সফটওয়্যার যেমন Log4J (CVE 2021 44228), অ্যাটলাসিন কনফ্লুএন্স (CVE-2021-31207, CVE-2021-26084) এবং Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473) -এ পাওয়া যায়। ASD-এর ACSC এবং নির্দেশিকা প্রস্তুতকারী সংস্থাগুলো আশা করছে যে, এই গোষ্ঠী নতুন ও গুরুত্বপূর্ণ দুর্বলতাগুলোর প্রুফ-অফ-কনসেপ্ট সমূহ (POC) জনসমক্ষে প্রকাশের কয়েক ঘণ্টা বা কয়েক দিনের মধ্যেই তা ব্যবহার করা শুরু করবে।

2 যুক্তরাষ্ট্র ডিপার্টমেন্ট অব জাস্টিস 2021. রাষ্ট্রীয় নিরাপত্তা মন্ত্রণালয়ের সহযোগিতায় কাজ করা চারজন চীনা নাগরিককে বৈশ্বিক কম্পিউটার অনুপ্রবেশ অভিযানের অভিযোগে অভিযুক্ত করা হয়েছে—যাদের লক্ষ্য ছিল বুদ্ধিবৃত্তিক সম্পদ ও সংবেদনশীল ব্যবসায়িক তথ্য, যার মধ্যে সংক্রামক রোগ সংক্রান্ত গবেষণা অন্তর্ভুক্ত ছিল।

চিত্র ১: APT40 কার্যকলাপের TTP ধারা-চিত্র

এই গোষ্ঠী সাধারণত ব্যবহারকারীর সক্রিয় অংশগ্রহণ পছন্দ করে, যেমন ফিশিং প্রচারণা কৌশলের চেয়ে দুর্বল, প্রকাশ্য অবকাঠামোকে কাজে লাগাতে বেশি আগ্রহী। তারা বৈধ ব্যবহারকারী পরিচয়পত্র (ক্রেডেনশিয়াল) সংগ্রহকে অত্যন্ত গুরুত্ব দিয়ে থাকে, যাতে পরবর্তী বিভিন্ন কর্মকাণ্ড চালানো যায়। APT40 বিশেষ করে হামলার প্রাথমিক পর্যায়েই তাদের অনুপ্রবেশ বজায় রাখার জন্য নিয়মিতভাবে 'ওয়েব শেল' (T1505.003) ব্যবহার করে। সাধারণভাবে দেখা যায়, প্রাথমিকভাবে সফলভাবে প্রবেশ করার পর APT40 আক্রান্তের নেটওয়ার্কে স্থায়ীভাবে অবস্থান নিশ্চিত করার চেষ্টায় থাকে, যাতে তাদের প্রবেশাধিকার বজায় থাকে। তবে যেহেতু অনুপ্রবেশের শুরুতেই স্থায়ীত্ব (পার্সিস্টেন্স) ঘটে, তাই এটি প্রায় সব ধরনের অনুপ্রবেশেই লক্ষ্য করা যায়—আক্রমণের গভীরতা বা পরবর্তী পদক্ষেপ যাই হোক না কেন।

উল্লেখযোগ্য কর্মকৌশল

যদিও APT40 অতীতে তাদের কার্যক্রম পরিচালনার জন্য হ্যাক করা অস্ট্রেলিয়ান ওয়েবসাইটকে কমান্ড ও কন্ট্রোল (C2) হোস্ট হিসেবে ব্যবহার করেছে, তবে তারা এখন এই কৌশলটি আরও উন্নত করেছে (T1594)।

APT40 এখন এমন এক বৈশ্বিক কৌশল অনুসরণ করছে, যেখানে হ্যাকাররা আক্রান্ত যন্ত্রপাতি ব্যবহার করে—বিশেষ করে বাসা বা ছোট অফিসে ব্যবহৃত SOHO ডিভাইস—যেগুলোকে তারা অস্ট্রেলিয়ায় তাদের সাইবার হামলা এবং শেষ ধাপের রিডাইরেক্টার হিসেবে (T1584.008) ব্যবহার করছে। এর ফলে নির্দেশিকা প্রস্তুতকারী সংস্থাগুলো এই গোষ্ঠীর কার্যকলাপকে আরও স্পষ্টভাবে বিশ্লেষণ ও পর্যবেক্ষণ করতে সক্ষম হয়েছে

এই SOHO ডিভাইসগুলোর অনেকটাই মেয়াদোত্তীর্ণ বা নিরাপত্তা আপডেটবিহীন, ফলে সেগুলো N-ডে দুর্বলতা কাজে লাগিয়ে আক্রমণের জন্য সহজ টার্গেট হয়ে দাঁড়ায়। একবার আক্রান্ত হলে, SOHO ডিভাইসগুলো সাইবার হামলার জন্য এমন এক সূচনা-স্থানে পরিণত হয়—যেখান থেকে বৈধ ট্রাফিকের সাথে মিশে গিয়ে আক্রমণ চালানো হয়, যাতে তা নেটওয়ার্ক সুরক্ষার দায়িত্বে থাকা ব্যক্তিদের জন্য শনাক্ত করা কঠিন হয় (T1001.003)।

এই কৌশলটি চীনা (PRC) রাষ্ট্র-সমর্থিত বিশ্বের অন্যান্য গোষ্ঠীগুলোও নিয়মিতভাবে ব্যবহার করে থাকে, এবং নির্দেশিকা প্রস্তুতকারী সংস্থাগুলো এটিকে একটি যৌথ হুমকি হিসেবে বিবেচনা করে। আরও তথ্যের জন্য, এই যৌথ পরামর্শনামাগুলো দেখুন: গণপ্রজাতন্ত্রী চীন রাষ্ট্র সমর্থিত সাইবার গোষ্ঠী নেটওয়ার্ক প্রদানকারী এবং ডিভাইসগুলিতে হামলা চালাচ্ছে এবং তারা যুক্তরাষ্ট্রের গুরুত্বপূর্ণ অবকাঠামোতে অনুপ্রবেশ করে সেখানে দীর্ঘমেয়াদে তাদের অবস্থান বজায় রাখছে।

APT40 মাঝে মাঝে আক্রান্তদের সামনে থাকা C2 (Command and Control) অবকাঠামো হিসেবে কেনা বা ভাড়া নেওয়া অবকাঠামো ব্যবহার করে; তবে এই কৌশলটির ব্যবহার তুলনামূলকভাবে কমে যাচ্ছে বলে মনে হচ্ছে।

টুলিং

ASD-এর ACSC নিচে তালিকাভুক্ত তদন্তে শনাক্ত করা কিছু ক্ষতিকর ফাইল শেয়ার করছে। এই ফাইলগুলো VirusTotal-এ আপলোড করা হয়েছে, যাতে বিস্তৃত নেটওয়ার্ক সুরক্ষা এবং সাইবার নিরাপত্তা সম্প্রদায় আরও ভালোভাবে বুঝতে পারে তারা কোন ধরনের হুমকির বিরুদ্ধে প্রতিরক্ষা গড়ে তুলতে হবে।

কেস স্টাডি

সাইবার হুমকি প্রদানকারী গোষ্ঠীগুলো কীভাবে তাদের টুলস এবং কৌশল ব্যবহার করে, সে বিষয়ে সচেতনতা বৃদ্ধির উদ্দেশ্যে ASD-এর ACSC দুটি বেনামি তদন্ত প্রতিবেদন শেয়ার করছে।

MD5	ফাইলের নাম	অতিরিক্ত তথ্য
26a5a7e71a601be991073c78d513dee3	horizon.jsp	১ kB | জাভা সোর্স
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	৫৯৭ B | জাভা বাইটকোড
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	৫ kB | জাভা বাইটকোড
64454645a9a21510226ab29e01e76d39	Index_jsp.java	৫ kB | জাভা সোর্স
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	৪ kB | জাভা বাইটকোড
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	৩ kB | জাভা বাইটকোড
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	১ kB | জাভা বাইটকোড
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	৭ kB | জাভা বাইটকোড
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	৮ kB | জাভা বাইটকোড
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	১৫ kB | জাভা সোর্স

কেস স্টাডি ১

এই প্রতিবেদনটিকে বেনামি (anonymised) করা হয়েছে, যাতে তা বিস্তৃতভাবে ছড়িয়ে দেওয়া সম্ভব হয় আক্রান্ত সংস্থাকে এখন থেকে 'সংস্থা' নামে উল্লেখ করা হবে। ভিকটিমের পরিচয় এবং ASD-এর ACSC এর হামলা মোকাবেলার কৌশল রক্ষার্থে কিছু নির্দিষ্ট তথ্য সরিয়ে ফেলা হয়েছে।

মূল সারসংক্ষেপ

এই প্রতিবেদনটি জুলাই থেকে সেপ্টেম্বর ২০২২-এর মধ্যে একটি সংস্থার নেটওয়ার্ক সফলভাবে হ্যাকিং এর উপর ASD-এর ACSC-এর তদন্তের ফলাফল তুলে ধরে। পর্যবেক্ষণ করা ক্ষতিকর কার্যকলাপের সারসংক্ষেপ প্রদান এবং প্রতিকারমূলক সুপারিশ প্রদানের উদ্দেশ্যে এই তদন্ত প্রতিবেদনটি সংস্থাটিকে সরবরাহ করা হয়েছে। তদন্তের ফলাফল ইঙ্গিত করে যে এই অনুপ্রবেশ APT40 গোষ্ঠী দ্বারাই পরিচালিত হয়েছে।

আগস্টের মাঝামাঝি সময়ে ASD-এর ACSC সংস্থাকে জানায় যে তাদের নেটওয়ার্কে একটি সম্ভব্য হ্যাক হওয়া ডিভাইসের মাধ্যমে ক্ষতিকর কার্যকলাপ ঘটেছে, যা ওই গোষ্ঠী আগস্টের শেষ দিকে ব্যবহার করেছে। সংস্থার সম্মতিতে ASD-এর ACSC সম্ভাব্য আক্রান্ত হোস্টে হোস্ট-ভিত্তিক সেন্সর স্থাপন করে। এই সেন্সরগুলো ASD-এর ACSC-এর বিশ্লেষকদের একটি পুঙ্খানুপুঙ্খ ডিজিটাল ফরেনসিক তদন্ত পরিচালনা করতে সক্ষম করে। বিদ্যমান সেন্সর ডেটা ব্যবহার করে ASD-এর ACSC বিশ্লেষকরা হুমকি পরিচালনাকারী গোষ্ঠীর কার্যকলাপ সফলভাবে চিত্রায়িত করেছে এবং পর্যবেক্ষণ করা ঘটনাগুলোর একটি বিস্তারিত টাইমলাইন তৈরি করেছে।

২০২২ সালের জুলাই থেকে আগস্ট পর্যন্ত ASD-এর ACSC যে গুরুত্বপূর্ণ হুমকি কার্যকলাপ পর্যবেক্ষণ করেছে তা নিচে তুলে ধরা হলোঃ

- হোস্ট এনুমারেশন: যা হুমকি পরিচালনাকারী গোষ্ঠীকে নেটওয়ার্কের মানচিত্র তৈরি করতে সক্ষম করে তোলে;
- ওয়েব শেল ব্যবহারের মাধ্যমে আক্রমণকারী নেটওয়ার্কে প্রাথমিক অবস্থান অর্জন করে এবং বিভিন্ন কমান্ড চালানোর সক্ষমতা লাভ করে; এবং
- ক্ষতিকর উদ্দেশ্যে ব্যবহার করার জন্য অন্যান্য টুল বা সরঞ্জাম স্থাপন করে।

তদন্তে দেখা গেছে, আক্রমণকারীরা বিপুল পরিমাণ সংবেদনশীল তথ্যে অনুপ্রবেশ করেছে এবং নেটওয়ার্কের ভেতরে স্থানান্তরের প্রমাণ পাওয়া গেছে। (T1021.002). এই সাইবার আক্রমণের অনেকাংশই সম্ভব হয়েছে কারণ ওই দলটি নেটওয়ার্কে প্রবেশের একাধিক পথ (অ্যাক্সেস ভেক্টর) তৈরি করেছিল, নেটওয়ার্কের গঠন ছিল সমতল (ফ্ল্যাট), এবং অভ্যন্তরীণভাবে তৈরি করা নিরাপত্তাহীন সফটওয়্যার ব্যবহার করা হয়েছিল যা দিয়ে ইচ্ছামতো ফাইল আপলোড করা সম্ভব ছিল। চুরি হওয়া তথ্যের মধ্যে ছিল গুরুত্বপূর্ণ লগইন তথ্য, যার মাধ্যমে ওই দলটি নেটওয়ার্কে প্রবেশ করতে পেরেছিল। পাশাপাশি, তারা এমন নেটওয়ার্ক-সংক্রান্ত তথ্যও সংগ্রহ করেছিল, যা মূল প্রবেশপথ বন্ধ হয়ে গেলেও তদেরকে নতুন করে অবৈধভাবে প্রবেশ করতে সাহায্য করতে পারে। প্রাথমিকভাবে আক্রান্ত যন্ত্র ছাড়া অন্য কোনো ক্ষতিকর টুলস পাওয়া যায়নি; তবে ওই দলের হাতে বৈধ এবং উচ্চ-ক্ষমতাসম্পন্ন লগইন তথ্য থাকায় অতিরিক্ত টুলসের প্রয়োজনই ছিল না। তদন্তের ফলাফল ইঙ্গিত করে যে, সংস্থাটি সম্ভবত APT40 দ্বারা পরিকল্পিতভাবে লক্ষ্যবস্তুতে পরিণত হয়েছিল; এটি কোনো সর্বজনীনভাবে পরিচিত দুর্বলতার সুযোগ নিয়ে ঘটনাক্রমে আক্রান্ত হওয়ার বিষয় ছিল না।

তদন্তের ফলাফল

২০২২ সালের আগস্ট মাসের মাঝামাঝি সময়ে ASD-এর ACSC সংস্থাটিকে জানায় যে, একটি নিশ্চিতভাবে ক্ষতিকর IP ঠিকানা, যা সম্ভবত একটি রাষ্ট্র-সমর্থিত সাইবার গোষ্ঠীর সঙ্গে যুক্ত, জুলাই থেকে আগস্ট পর্যন্ত সময়ে সংস্থার কম্পিউটার নেটওয়ার্কের সঙ্গে সংযোগ স্থাপন করেছিল। আক্রান্ত যন্ত্রটি সম্ভবত কোনো ছোট ব্যবসায় প্রতিষ্ঠানের বা ব্যক্তিগত (বাসা-বাড়ির) ব্যবহারকারীর ছিল।

আগস্ট মাসের শেষ দিকে ASD-এর ACSC সংস্থাটির নেটওয়ার্কে আক্রান্ত হওয়া কম্পিউটারগুলোর ওপর একট 'হোস্ট ভিত্তিক এজেন্ট' স্থাপন করে।

তদন্তে সহায়ক হতে পারত এমন কিছু তথ্য বা ডেটা (আর্কাইভ) পাওয়া যায়নি, কারণ লগিংয়ের সেটআপ বা নেটওয়ার্ক ডিজাইনের ধরন সেগুলোর সংরক্ষণে সহায়ক ছিল না। তবে এর পরেও, সংস্থাটি যেহেতু সকল প্রাপ্য তথ্য সরবরাহে প্রস্তুত ছিল, ASD-এর ACSC-এর হামলা মোকাবেলাকারী দল একটি বিস্তৃত বিশ্লেষণ পরিচালনা করতে পেরেছে এবং নেটওয়ার্কে সম্ভাব্য APT40 কার্যকলাপ সম্পর্কে একটি ধারণা গড়ে তুলতে সক্ষম হয়েছে।

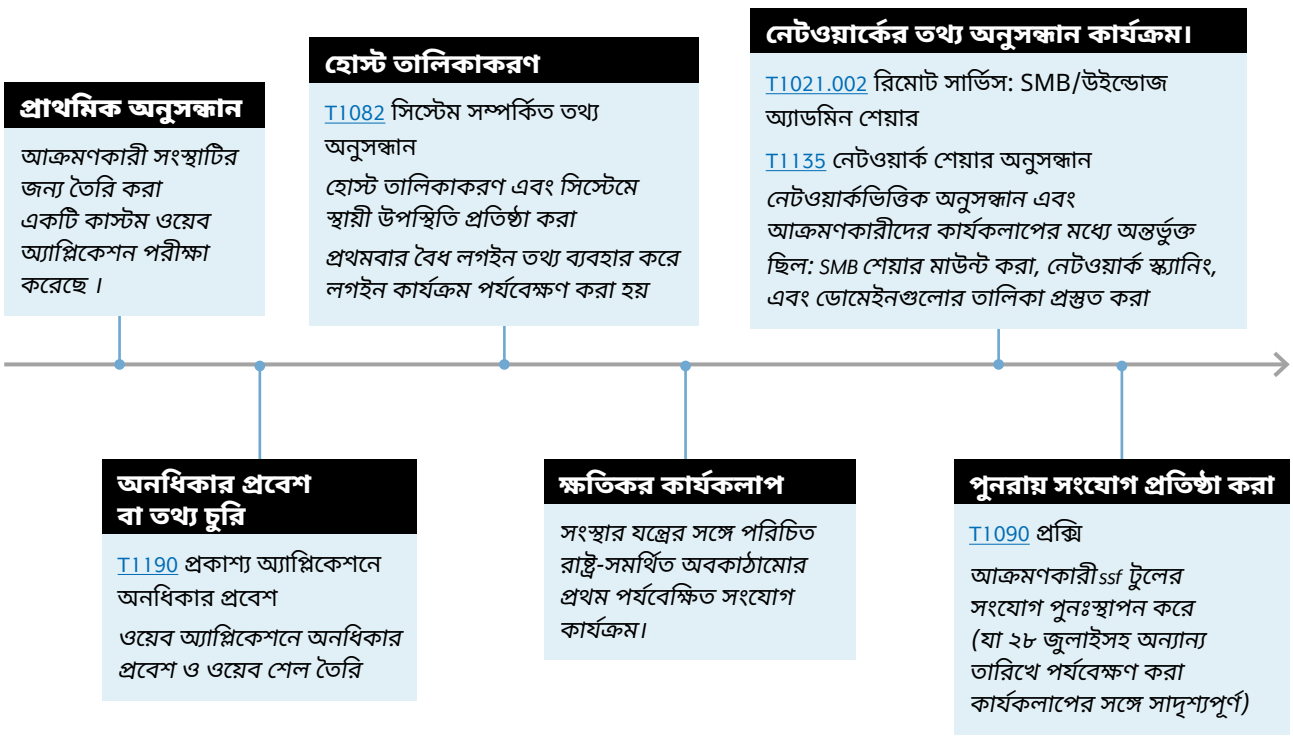
সেপ্টেম্বর মাসে ASD-এর ACSC-এর সঙ্গে পরামর্শের পর, সংস্থাটি প্রাথমিকভাবে শনাক্ত হওয়া IP ঠিকানাটিকে ব্লক করে দেয়ার করার সিদ্ধান্ত নেয়। অক্টোবর মাসে, সংস্থাটি পুনরুদ্ধার কার্যক্রম শুরু করে।

বিস্তারিত

জুলাই মাসের শুরুর দিকে, আক্রমণকারীরা `<webapp>2-ext` নামক একটি সিস্টেমে চলমান (T1190) কাস্টম ওয়েব অ্যাপ্লিকেশন পরীক্ষা ও তা ব্যবহার করতে সক্ষম হয়, যার মাধ্যমে তারা নেটওয়ার্কের ডিমিলিটারাইজড জোন (DMZ)-এ একটি প্রাথমিক অবস্থান তৈরি করে। এই সুবিধাটি কাজে লাগিয়ে আক্রমণকারীরা পুরো নেটওয়ার্ক এবং দৃশ্যমান সব ডোমেইনের তালিকা প্রস্তুত করে। আক্রান্ত লগইন তথ্য (T1078.002) ব্যবহার করে আক্রমণকারীরা Active Directory (T1018) থেকে তথ্য সংগ্রহ করে এবং DMZ-এ থাকা একাধিক যন্ত্রে ফাইল শেয়ার (T1039) মাউন্ট করে সেখান থেকে ডেটা চুরি করে নেয়। আক্রমণকারী একটি 'Kerberoasting' আক্রমণ চালায়, যাতে তারা সার্ভার থেকে বৈধ নেটওয়ার্ক লগইন তথ্য সংগ্রহ করতে পারে। (T1558.003). সংশ্লিষ্ট দলটি DMZ কিংবা অভ্যন্তরীণ নেটওয়ার্কে নতুন কোনো অবস্থান বা উপস্থিতি অর্জন করেছে—এমন কোনো প্রমাণ পাওয়া যায়নি।

দৃশ্যমান সময়রেখা

নিচের সময়রেখা সংস্থাটির নেটওয়ার্কে আক্রমণকারীদের কার্যকলাপের প্রধান পর্যায়গুলোর একটি সামগ্রিক পর্যালোচনা উপস্থাপন করে।



বিস্তারিত সময়রেখা

জুলাইঃ আক্রমণকারীরা সংস্থার জন্য তৈরি একটি কাস্টম ওয়েব অ্যাপ্লিকেশনের (T1190) এখানে 'ওয়েব অ্যাপ্লিকেশন' বা '*webapp*' নামে উল্লেখিত) ফ্রন্ট পেজে প্রথম সংযোগ স্থাপন করে, যা ট্রান্সপোর্ট লেয়ার সিকিউরিটি (TLS) সংযোগের মাধ্যমে সম্পন্ন হয় (T1102)। আর কোনো উল্লেখযোগ্য কার্যকলাপ পর্যবেক্ষণ করা হয়নি।

জুলাইঃ [2]আক্রমণকারীরা ওয়েব অ্যাপ্লিকেশনটির ওয়েবসাইটে বিভিন্ন এন্ডপয়েন্ট খুঁজে বের করার উদ্দেশ্যে তালিকাকরণ শুরু করে, যাতে তারা আরও তদন্ত চালাতে পারে।

জুলাইঃ আক্রমণকারীরা একটি নির্দিষ্ট এন্ডপয়েন্টে প্রবেশের চেষ্টা করার দিকে মনোযোগ কেন্দ্রীভূত করে।

জুলাইঃ আক্রমণকারীরা সম্ভবত অন্য একটি পেজে স্থাপন করা ওয়েব শেলের মাধ্যমে ওয়েব সার্ভারে সফলভাবে `POST` পাঠাতে সক্ষম হয়। এছাড়াও একটি দ্বিতীয় IP, যা সম্ভবত একই আক্রমণকারীদের দ্বারা ব্যবহৃত, একই URL-এ POST পাঠানো শুরু করে। আক্রমণকারীরা একাধিক সম্ভাব্য ওয়েব শেল তৈরি করে এবং সেগুলো পরীক্ষা করে।

যদিও এই অনধিকার প্রবেশের নির্দিষ্ট পদ্ধতি অজানা, তবে এটি স্পষ্ট যে `<webapp>2-ext` ফাইল তৈরি করার জন্য একটি নির্দিষ্ট এন্ডপয়েন্টকে লক্ষ্য করা হয়েছে।

ASD-এর ACSC মনে করে যে দুটি IP অ্যাড্রেস সংযোগ একই অনুপ্রবেশের অংশ ছিল, কারণ এগুলোর মধ্যে একটি অভিন্ন উদ্দেশ্য ছিল এবং প্রাথমিক সংযোগগুলো কয়েক মিনিটের ব্যবধানে ঘটেছিল।

জুলাইঃ দলটি এখনও কম্পিউটার হোস্ট শনাক্ত করার কাজ চালিয়ে যাচ্ছে, যেখানে তারা উচ্চ পর্যায়ের নিয়ন্ত্রণ নেয়ার সুযোগ খুঁজছে এবং একটি নতুন ধরনের ওয়েব শেল স্থাপন করছে। আক্রমণকারীরা চুরি হওয়া লগইন তথ্য `<firstname.surname>@<organisation domain>` ব্যবহার করে ওয়েব অ্যাপ্লিকেশনে প্রবেশ করে।

আক্রমণকারীদের কার্যক্রম দেখে মনে হচ্ছে তারা `<webapp>2-ext` সিস্টেমে উচ্চ পর্যায়ের নিয়ন্ত্রণ নিতে সফল হয়নি। এর পরিবর্তে, আক্রমণকারীরা নেটওয়ার্ক-ভিত্তিক কার্যকলাপে মনোনিবেশ করে।

জুলাইঃ আক্রমণকারী একটি সার্ভিস অ্যাকাউন্টের[3] জন্য চুরি হওয়া লগইন তথ্য পরীক্ষা করে, যা সম্ভবত তারা অভ্যন্তরীণভাবে সহজে প্রবেশযোগ্য সফটওয়্যার ফাইলের মধ্যে হার্ডকোড করা অবস্থায় খুঁজে পেয়েছিল।

জুলাইঃ আক্রমণকারীরা ওপেন সোর্স টুল 'Secure Socket Funnelling' ব্যবহার করে, যা তাদের ক্ষতিকর পরিকাঠামোর সঙ্গে সংযোগ স্থাপনে সহায়তা করে। এই সংযোগ ব্যবহার করে আক্রমণকারী তাদের আক্রমণের জন্য ব্যবহৃত কম্পিউটার থেকে সংস্থার অভ্যন্তরীণ নেটওয়ার্কে তথ্য পাঠানোর গোপন পথ তৈরি করে। তারা যখন সার্ভিস অ্যাকাউন্টের লগইন তথ্য ব্যবহার করার চেষ্টা করে, তখন ইভেন্ট লগে অভ্যন্তরীণ কম্পিউটারগুলোর নাম প্রকাশিত হয়।

আগস্টঃ আক্রমণকারীদের কিছু সীমিত কার্যকলাপ করতে দেখা গেছে, যার মধ্যে রয়েছে সার্ভিস অ্যাকাউন্ট ব্যবহার করে সংযোগ স্থাপন করতে ব্যর্থ হওয়া।

আগস্টঃ আক্রমণকারীরা ব্যাপক নেটওয়ার্ক এবং অ্যাক্টিভ ডিরেক্টরি অনুসন্ধানের কার্যক্রম পরিচালনা করে।[4] DMZ অঞ্চলের মধ্যে উইন্ডোজ মেশিনে শেয়ার সংযুক্ত করতে পরবর্তীতে একটি ভিন্ন হ্যাক হওয়া অ্যাকাউন্ট ব্যবহার করা হয়, এবং এর মাধ্যমে সফলভাবে সংবেদনশীল তথ্য বাইরে পাঠানো সম্ভব হয়।

এটিকে দেখে মনে হচ্ছে DMZ অঞ্চলের কিছু কম্পিউটার মেশিনে চুরি হওয়া লগইন তথ্যের সুযোগসন্ধানী ব্যবহার। তবে ফায়ারওয়াল অভ্যন্তরীণ নেটওয়ার্কে একই ধরনের কার্যকলাপ চালাতে আক্রমনকারীদের বাধা দেয়।

অগাস্ট-সেপ্টেম্বরঃ SSF নামক একটি টুল ক্ষতিকর IP-তে পুনরায় সংযোগ স্থাপন করে যতক্ষণ না সংস্থাটি ঐ গ্রুপটির অ্যাক্সেস ব্লক করে দেয় ততক্ষন তাদের কোনো অতিরিক্ত কার্যকলাপ দেখা যায়নি।

সেপ্টেম্বরঃ সংস্থাটি তাদের ফায়ারওয়ালে ক্ষতিকর আইপি ঠিকানাটিকে ব্লক করে দেয়।

2 এই প্রেক্ষাপটে, 'এন্ডপয়েন্ট' বলতে ওয়েব অ্যাপ্লিকেশনের একটি নির্দিষ্ট ফাংশন বা কার্যক্রমকে বোঝানো হয়েছে।

3 সার্ভিস অ্যাকাউন্টগুলি কোনো ব্যক্তিগত ব্যবহারকারীর সঙ্গে যুক্ত নয়, বরং সার্ভিসের সাথে যুক্ত । মাইক্রোসফট কর্পোরেট ডোমেইনে বিভিন্ন ধরনের অ্যাকাউন্ট থাকে।

4 শেয়ার সংযুক্তকরণ হল একটি প্রক্রিয়া, যেখানে ফাইল সিস্টেমের ফাইলগুলো কোনো ব্যবহারকারী বা ব্যবহারকারী দলের জন্য অ্যাক্সেসযোগ্য করে তোলা হয়।

আক্রমণকারীর কৌশল এবং পদ্ধতি

MITRE ATT&CK ফ্রেমওয়ার্ক হল অনলাইনে সাইবার হামলাকারীদের দ্বারা ব্যবহৃত কৌশল ও পদ্ধতিগুলির একটি সংগৃহীত নথি। এই ফ্রেমওয়ার্কটি তৈরি করেছে মার্কিন অলাভজনক সংস্থা 'The MITRE Corporation', এবং এটি সাইবার হামলাকারীদের কার্যক্রম বোঝাতে একটি বৈশ্বিক সাধারণ ভাষা হিসেবে কাজ করে।

ASD-এর ACSC মূল্যায়ন করেছে যে নিচে বর্ণিত কৌশল ও পদ্ধতিগুলো হামলাকারীদের ক্ষতিকর কার্যকলাপের সঙ্গে সম্পর্কিতঃ

পুনর্বিবেচনা

T1594 – আক্রান্তের মালিকানাধীন ওয়েবসাইট অনুসন্ধান

আক্রমণকারী কাস্টম ওয়েব অ্যাপ্লিকেশনের ওয়েবসাইট বিশ্লেষণ করেছে, যাতে নেটওয়ার্কে প্রবেশের সম্ভাব্য পথগুলো খুঁজে বের করতে পারে।

প্রাথমিক অ্যাক্সেস

T1190 – ইন্টারনেটে যুক্ত অ্যাপ্লিকেশনকে কাজে লাগানো (কাস্টম ওয়েব অ্যাপ্লিকেশনকে কাজে লাগানো সম্পর্কিত)

T1078.002 – বৈধ অ্যাকাউন্ট: ডোমেইন অ্যাকাউন্ট (চুরি হওয়া লগইন তথ্য ব্যবহার করে নেটওয়ার্কে প্রবেশ সম্পর্কিত)

ইন্টারনেটে উন্মুক্ত কাস্টম ওয়েব অ্যাপ্লিকেশনকে কাজে লাগিয়ে (এক্সপ্লয়েট করে) আক্রমণকারী তাদের প্রাথমিক প্রবেশ পথ তৈরি করে। পরে আক্রমণকারী চুরি করা লগইন তথ্য ব্যবহার করে নেটওয়ার্কে আরও গভীরভাবে প্রবেশ করতে সক্ষম হয়।

হামলা পরিচালনা

T1059 – কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার (ওয়েব শেল ব্যবহার করে কম্যান্ড পরিচালনা করা সম্পর্কিত)

T1072 – সফটওয়্যার ডিপ্লয়মেন্ট টুলস (আক্রমণকারী কর্তৃক কোন আইপির সাথে সংযুক্ত হতে সিকিউর সকেট ফানেলিং (SSF) ব্যবহার করা সম্পর্কিত)

সিস্টেমে স্থায়ী অনুপ্রবেশ

T1505.003 – সার্ভার সফটওয়্যার কম্পোনেন্ট: ওয়েব শেল (অ্যাক্সেস লাভের জন্য ওয়েব শেল এবং SSF ব্যবহার সম্পর্কিত)

ব্যবহারকারী নাম ও পাসওয়ার্ডের অননুমোদিত প্রবেশ

T1552.001 – পাসওয়ার্ড সংরক্ষণ ফাইল থেকে লগইন তথ্য সংগ্রহ (বিল্ডিং ম্যানেজমেন্ট সিস্টেম (BMS) এর সাথে সংশ্লিষ্ট পাসওয়ার্ড ফাইল সম্পর্কিত)

T1558.003 – কের্বেরোস টিকিট চুরি বা জালিয়াতি করা: কের্বেরোস (নেটওয়ার্কে লগইন তথ্য লাভের জন্য আক্রমণ সম্পর্কিত)

নেটওয়ার্কের ভেতরে ধাপে ধাপে অনুপ্রবেশ

T1021.002 – রিমোট সার্ভিসসমূহ: SMB শেয়ার (আক্রমণকারী কর্তৃক একাধিক ডিভাইস থেকে SMB শেয়ার সংযুক্ত করা সম্পর্কিত)

সংগ্রহ

T1213 –তথ্যভাণ্ডার থেকে তথ্য সংগ্রহ (BMS সার্ভারে পাওয়া ম্যানুয়াল/ডকুমেন্টেশন সম্পর্কিত তথ্য)

তথ্য পাচার

T1041 – (C2) চ্যানেলের মাধ্যমে তথ্য পাচার (আক্রমণকারী কর্তৃক একটিভ ডিরেক্টরি থেকে সংবেদনশীল তথ্য পাচার এবং শেয়ার সংযুক্তকরণ সম্পর্কিত)

কেস স্টাডি ২

আরও বিস্তৃতভাবে ছড়িয়ে দেয়ার উদ্দেশ্যে এই প্রতিবেদনটির পরিচয় গোপন করা হয়েছে। ক্ষতিগ্রস্ত সংস্থাটিকে এখন থেকে ‘সংস্থা’ হিসেবে উল্লেখ করা হবে। ভুক্তভোগীর পরিচয় এবং ASD-এর ACSC-এর হামলা মোকাবেলার কৌশল সুরক্ষিত রাখতে কিছু নির্দিষ্ট তথ্য সরিয়ে ফেলা হয়েছে।

মূল সারাংশ

এই প্রতিবেদনটি এপ্রিল ২০২২-এ সংস্থার নেটওয়ার্ক সফলভাবে হ্যাক হওয়ার ঘটনাটি নিয়ে ASD-এর ACSC-এর তদন্তে পাওয়া তথ্য তুলে ধরেছে। এই তদন্ত প্রতিবেদনটি সংস্থাকে সরবরাহ করা হয়েছে, যাতে পর্যবেক্ষিত ক্ষতিকর কার্যকলাপের সারাংশ তুলে ধরা যায় এবং প্রতিকারমূলক সুপারিশ প্রস্তাব করা যায়। তদন্তের ফলাফল ইঙ্গিত করে যে এই হ্যাকিং কার্যক্রমটি APT40 দ্বারা পরিচালিত হয়েছে।

২০২২ সালের মে মাসে ASD-এর ACSC একটি সংস্থাকে জানায় যে এপ্রিল ২০২২ থেকে তাদের নেটওয়ার্কে সন্দেহজনক ক্ষতিকর কার্যকলাপ চলছিল। পরবর্তীতে সংস্থাটি ASD-এর ACSC-কে জানায় যে তারা একটি ইন্টারনেট-সংযুক্ত সার্ভারে ক্ষতিকর সফটওয়্যার খুঁজে বের করা করেছে, যা তাদের কর্পোরেট রিমোট অ্যাক্সেস সল্যুশনের লগইন পোর্টাল হিসেবে ব্যবহৃত হচ্ছিল। এই সার্ভারটি একটি রিমোট অ্যাক্সেস লগইন এবং পরিচয় ব্যবস্থাপনা পণ্য ব্যবহার করত, এবং এই প্রতিবেদনে এটিকে ‘কমপ্রোমাইজড অ্যাপ্লায়েন্স’ হিসেবে উল্লেখ করা হবে। এই প্রতিবেদনটি ASD-এর ACSC কর্তৃক পরিচালিত তদন্তের ভিত্তিতে সংস্থার জন্য প্রস্তুতকৃত তদন্তের ফলাফল এবং প্রতিকারমূলক পরামর্শ তুলে ধরে।

প্রমাণ থেকে জানা যায় যে এপ্রিল ২০২২ থেকে সংস্থার রিমোট অ্যাক্সেস লগইন পোর্টালের মাধ্যমে তাদের নেটওয়ার্কের একটি অংশ ক্ষতিকর সাইবার আক্রমণকারীদের দ্বারা হ্যাক হয়েছে। এই সার্ভারটি একাধিক আক্রমণকারীর দ্বারা হ্যাক হয়েছে বলে ধারণা করা হচ্ছে, এবং সম্ভবত এটি এমন একটি রিমোট কোড এক্সিকিউশন (RCE) দুর্বলতার দ্বারা আক্রান্ত হয়েছে, যা হ্যাকিং এর সেই সময়ে ব্যাপকভাবে প্রচারিত হয়েছিল।

ASD-এর ACSC কর্তৃক পর্যবেক্ষণ করা মূল আক্রমণকারীর কার্যকলাপের মধ্যে অন্তর্ভুক্ত ছিল:

- হোস্ট এনুমারেশন, যা আক্রমণকারীকে নেটওয়ার্কের নিজস্ব মানচিত্র তৈরি করতে সক্ষম করে;
- ইন্টারনেট-সংযুক্ত অ্যাপ্লিকেশনগুলোর দুর্বলতা কাজে লাগানো এবং ওয়েব শেলের ব্যবহার যার মাধ্যমে আক্রমণকারী নেটওয়ার্কে প্রাথমিক প্রবেশাধিকার এবং কমান্ড চালানোর সক্ষমতা অর্জন করে।
- সফটওয়্যারের দুর্বলতা কাজে লাগিয়ে অধিকতর প্রবেশাধিকার অর্জন করা;
- নেটওয়ার্কের ভেতরে ধাপে ধাপে অনুপ্রবেশে সক্ষম হতে লগইন তথ্য সংগ্রহ

ASD-এর ACSC খুঁজে বের করা করেছে যে এপ্রিল ২০২২-এ একটি হ্যাক হওয়া অ্যাপ্লায়েন্স থেকে একটি ক্ষতিকর সাইবার আক্রমণকারী কয়েক শতাধিক ইউনিক ইউজারনেম ও পাসওয়ার্ড জোড়া, মাল্টি ফ্যাক্টর অথেনটিকেশন কোড এবং রিমোট অ্যাক্সেস সেশনের সঙ্গে সম্পর্কিত প্রযুক্তিগত উপাদান চুরি করেছে। সংস্থার পর্যালোচনায় দেখা গেছে যে চুরি হওয়া পাসওয়ার্ডগুলো বৈধ ছিল। ASD-এর ACSC মূল্যায়ন করেছে যে আক্রমণকারী এই প্রযুক্তিগত উপাদানগুলো সংগ্রহ করেছে, যাতে তারা বৈধ ব্যবহারকারীর পরিচয়ে রিমোট লগইন সেশন হাইজ্যাক বা তৈরি করতে পারে এবং সংস্থার অভ্যন্তরীণ কর্পোরেট নেটওয়ার্কে প্রবেশ করতে পারে।

তদন্তের ফলাফল

তদন্তের সারাংশ

ASD-এর ACSC নির্ধারণ করেছে যে আক্রমণকারী সংস্থার কর্মীদের রিমোট লগইন সেশন প্রদানকারী অ্যাপ্লায়েন্সগুলো হ্যাক করেছে এবং এই প্রবেশাধিকার ব্যবহার করে আরও কার্যকলাপ চালানোর চেষ্টা করেছে। এই অ্যাপ্লায়েন্সগুলো তিনটি লোড-ব্যালেন্সড হোস্ট নিয়ে গঠিত, যেখানে প্রথম হ্যাকিংয়ের প্রমাণ পাওয়া যায়। সংস্থা প্রাথমিক হ্যাকিংয়ের পর তিনটির মধ্যে দুটি হোস্ট বন্ধ করে দেয়। ফলে পরবর্তী সমস্ত কার্যকলাপ একটি মাত্র হোস্টে সংঘটিত হয়। হ্যাক হওয়া অ্যাপ্লায়েন্সের সঙ্গে যুক্ত অন্যান্য সার্ভারগুলোও একইভাবে লোড-ব্যালেন্সড ছিল। পাঠযোগ্যতার সুবিধার্থে, এই প্রতিবেদনের বেশিরভাগ অংশে সমস্ত হ্যাক হওয়া অ্যাপ্লায়েন্সকে 'একমাত্র অ্যাপ্লায়েন্স' হিসেবে উল্লেখ করা হয়েছে।

আক্রমণকারী এপ্রিল ২০২২ থেকে শুরু করে ব্যাপকভাবে পরিচিত দুর্বলতাগুলি ব্যবহার করে হ্যাক হওয়া অ্যাপ্লায়েন্সে ওয়েব শেল স্থাপন করেছে বলে ধারণা করা হয়। এই গ্রুপের সাইবার আক্রমণকারীরা অ্যাপ্লায়েন্সে অধিকতর প্রবেশাধিকার অর্জন করেছে বলে দেখা গেছে। ASD-এর ACSC লগিং-এর অভাবের কারণে সম্পূর্ণ কার্যকলাপ নির্ধারণ করতে পারেনি। তবে ডিভাইসে থাকা প্রমাণ অনুযায়ী, আক্রমণকারী নিম্নলিখিত কার্যকলাপ করেছে:

- কয়েক শতাধিক বৈধ ইউজারনেম ও পাসওয়ার্ড এর জোড়া সংগ্রহ করেছে; এবং
- এমন প্রযুক্তিগত উপাদান সংগ্রহ করেছে, যা ব্যবহার করে আক্রমণকারী বৈধ ব্যবহারকারীর পরিচয়ে ভার্চুয়াল ডেস্কটপ ইনফ্রাস্ট্রাকচার (VDI) সেশনে প্রবেশ করতে পারে বলে ধারণা করা হচ্ছে।

ASD-এর ACSC মূল্যায়ন করেছে যে, আক্রমণকারী, সংস্থার নেটওয়ার্কে আরও গভীরভাবে প্রবেশ করার চেষ্টা করেছে। আক্রমণকারীর দ্বারা চুরি করা এই উপাদানগুলো ব্যবহার করে তারা বৈধ ব্যবহারকারীর পরিচয়ে VDI সেশন হাইজ্যাক বা শুরু করতে পারে, এমনকি তাদের পছন্দের ব্যবহারকারী হিসেবে—যার মধ্যে অ্যাডমিনিস্ট্রেটরও থাকতে পারে। আক্রমণকারী এই প্রবেশপথ (access vector) ব্যবহার করে সংস্থার অন্যান্য পরিষেবা হ্যাক করার চেষ্টা করেছে, যাতে তারা স্থায়ীভাবে প্রবেশাধিকার এবং অন্যান্য উদ্দেশ্য অর্জন করতে পারে।

হোস্টিং প্রদানকারী দ্বারা পরিচালিত পরিবেশে সংস্থার অন্যান্য অ্যাপ্লায়েন্সে হ্যাকিংয়ের কোনো প্রমাণ পাওয়া যায়নি।

অ্যাক্সেস

হ্যাক হওয়া অ্যাপ্লায়েন্সের হোস্টটি, ব্যবহারকারীদের VDI সেশনে (T1021.001) সংযুক্ত হওয়ার জন্য একটিভ ডিরেক্টরি এবং একটি ওয়েবসার্ভারের মাধ্যমে অথেনটিকেশন প্রদান করত।

অবস্থান	হ্যাক হওয়া অ্যাপ্লায়েন্স হোস্টনেম (লোড ব্যালেন্সড)
ডেটা সেন্টার ১	হোস্ট১, হোস্ট২, হোস্ট৩

অ্যাপ্লায়েন্স অবকাঠামোর মধ্যে এমন অ্যাক্সেস গেটওয়ে হোস্ট অন্তর্ভুক্ত ছিল, যা অ্যাপ্লায়েন্স থেকে তৈরি ও ডাউনলোড করা একটি প্রমাণীকরণ টোকেন সংগ্রহের পর ব্যবহারকারীর জন্য VDI-তে একটি টানেল প্রদান করে।

এই হোস্টগুলোর কোনো হ্যাকিংয়ের প্রমাণ পাওয়া যায়নি। তবে, অ্যাক্সেস গেটওয়ে হোস্টের লগে পরিচিত ক্ষতিকর IP ঠিকানার সঙ্গে উল্লেখযোগ্য যোগাযোগের প্রমাণ পাওয়া গেছে। সম্ভবত এই কার্যকলাপ হোস্টে সংঘটিত হয়েছে, অথবা এটি এমন নেটওয়ার্ক সংযোগের প্রতিফলন, যা হুমকিস্বরূপ অবকাঠামোর সঙ্গে যুক্ত ছিল এবং এই হোস্টে পৌঁছেছে। উপলব্ধ প্রমাণ ব্যবহার করে এই কার্যকলাপের প্রকৃতি নির্ধারণ করা যায়নি, তবে এটি ইঙ্গিত করে যে গোষ্ঠীটি সংস্থার নেটওয়ার্কে (TA0008) ধাপে ধাপে করার চেষ্টা করেছে।

আভ্যন্তরীণ হোস্ট

ASD-এর ACSC সংস্থার অভ্যন্তরীণ নেটওয়ার্ক সেগমেন্ট থেকে সীমিত তথ্য বিশ্লেষণ করেছে। সংস্থার অভ্যন্তরীণ নেটওয়ার্ক সেগমেন্টকে ক্ষতিগ্রস্ত করেছে বলে পরিচিত পরীক্ষিত বা সফল ক্ষতিকর কার্যকলাপের মধ্যে অন্তর্ভুক্ত ছিল VDI-সম্পর্কিত উপাদানে আক্রমণকারীর প্রবেশাধিকার, একটি অভ্যন্তরীণ SQL সার্ভার (T1505.001) থেকে তথ্য সংগ্রহ, এবং পরিচিত ক্ষতিকর IP ঠিকানা থেকে অ্যাক্সেস গেটওয়ে অ্যাপ্লায়েন্সের (TA0011) মাধ্যমে অজানা ট্রাফিকের উপস্থিতি।

হ্যাক হওয়া অ্যাপ্লায়েন্সে প্রবেশাধিকার ব্যবহার করে গ্রুপটি বৈধ ইউজারনেম ও পাসওয়ার্ড (T1003), মাল্টি ফ্যাক্টর অথেনটিকেশন (MFA) টোকেন মান (T1111) সংগ্রহ করেছে। এছাড়াও গ্রুপটি ভার্চুয়াল ডেস্কটপ লগইন সেশন তৈরিতে ব্যবহৃত অথেনটিকেশন উপাদান JSON Web Token (JWT) (T1528) সংগ্রহ করেছে। এই উপাদানগুলো ব্যবহার করে আক্রমণকারী ভার্চুয়াল ডেস্কটপ সেশন (T1563.002) তৈরি বা হাইজ্যাক করতে পেরেছে বলে ধারণা করা হয়, এবং বৈধ ব্যবহারকারীর (T1078) পরিচয়ে সংস্থার অভ্যন্তরীণ নেটওয়ার্ক সেগমেন্টে প্রবেশ করেছে।

এছাড়াও আক্রমণকারী ক্ষতিগ্রস্ত যন্ত্রটির অ্যাক্সেস ব্যবহার করে সংস্থার অভ্যন্তরীণ নেটওয়ার্কে অবস্থিত একটি SQL সার্ভার (T1505.001) থেকে তথ্য সংগ্রহ করেছে। এই তথ্যের অ্যাক্সেস তাদের ছিল বলে ধারণা করা হচ্ছে।

যন্ত্রটির আক্সেস গেটওয়ে থেকে প্রাপ্ত প্রমাণ অনুযায়ী, যন্ত্রটির মাধ্যমে বা এর দিকে নেটওয়ার্ক ট্রাফিক হয়েছে কিছু পরিচিত ক্ষতিকর IP ঠিকানা থেকে। উপরে বর্ণিত তথ্য অনুযায়ী, এটি ইঙ্গিত করে যে সাইবার হামলাকারীরা এই যন্ত্রটিকে ব্যবহার বা প্রভাবিত করেছে—সম্ভবত অভ্যন্তরীণ নেটওয়ার্কে প্রবেশের জন্য।

তদন্তের সময়রেখা

নিম্নোক্ত তালিকাটি তদন্তের সময় আবিষ্কৃত গুরুত্বপূর্ণ কার্যক্রমসমূহের একটি ক্রম দেখায়।

সময়	ঘটনা
এপ্রিল ২০২২	পরিচিত ক্ষতিকর আইপি ঠিকানাগুলি আক্সেস গেটওয়ে হোস্ট HOST7-এর সঙ্গে যোগাযোগ করেছে। এই যোগাযোগের প্রকৃতি নির্ধারণ করা সম্ভব হয়নি।
এপ্রিল ২০২২	সকল হোস্ট—HOST1, HOST2 এবং HOST3—এক বা একাধিক ক্ষতিকর সাইবার হামলাকারীর দ্বারা আক্রান্ত হয়েছে, এবং এসব হোস্টে "ওয়েব শেল" স্থাপন করা হয়েছে। HOST2-তে একটি লগ ফাইল তৈরি বা পরিবর্তন করা হয়েছে। এই ফাইলটিতে এমন তথ্য রয়েছে যা সম্ভবত ক্ষতিকর সাইবার হামলাকারী দ্বারা সংগৃহীত লগইন তথ্য। HOST1 এবং HOST3-এ /etc/security/opasswd ও /etc/shadow ফাইল পরিবর্তন হয়েছে, যা নির্দেশ করে সেখানে পাসওয়ার্ড পরিবর্তন করা হয়েছে। HOST1-এ পাওয়া প্রমাণ অনুযায়ী, 'sshuser' নামের ব্যবহারকারীর পাসওয়ার্ড পরিবর্তিত হয়েছে বলে ধারণা করা হচ্ছে।
এপ্রিল ২০২২	সংস্থাটি HOST2-কে বন্ধ করে দিয়েছে। HOST1 এবং HOST3-এ অতিরিক্ত ওয়েব শেল (T1505.003) তৈরি করা হয়েছে। HOST1-এ HOST3 থেকে SSH ব্রুট ফোর্স বা জোরালো আক্রমণের চেষ্টা হয়েছে। HOST3-এ একটি লগ ফাইল (T1070) পরিবর্তন করা হয়েছে। এই ফাইলটিতে এমন তথ্য রয়েছে যা সম্ভবত ক্ষতিকর সাইবার হামলাকারী দ্বারা সংগৃহীত লগইন তথ্য। (T1078)। JWT সংগ্রহ করে (T1528) HOST3-এ একটি ফাইলে সংরক্ষণ করা হয়েছে। পরে সংস্থাটি HOST3-কে বন্ধ করে দিয়েছে। এরপরের সকল কার্যক্রম HOST1-এ হয়েছে।
এপ্রিল ২০২২	HOST1 (T1505.003) এ অতিরিক্ত ওয়েব শেল তৈরি করা হয়েছে। JWT সংগ্রহ করে HOST1-এ একটি ফাইলে সংরক্ষণ করা হয়েছে।
এপ্রিল ২০২২	HOST1 (T1505.003) এ অতিরিক্ত ওয়েব শেল তৈরি হয়েছে এবং পরিচিত একটি ক্ষতিকর আইপি ঠিকানা হোস্ট (TA0011) এর সঙ্গে যোগাযোগ করেছে। পরিচিত একটি ক্ষতিকর আইপি ঠিকানা আক্সেস গেটওয়ে HOST7 এর সঙ্গে যোগাযোগ করেছে।
মে ২০২২	পরিচিত একটি ক্ষতিকর আইপি ঠিকানা আক্সেস গেটওয়ে HOST7 (TA0011) এর সঙ্গে যোগাযোগ করেছে। HOST1-এর লগ-এ একটি ব্যবহারকারীর অথেনটিকেশন কার্যক্রমের সঙ্গে একটি পরিচিত ক্ষতিকর আইপি ঠিকানার সংযোগ পাওয়া গেছে। এই হোস্টে অতিরিক্ত একটি ওয়েব শেল (T1505.003) তৈরি করা হয়েছে।
মে ২০২২	একজন সাইবার হামলাকারী HOST1-এ একটি স্ক্রিপ্ট পরিবর্তন করেছে (T1543)। এই স্ক্রিপ্টে এমন কার্যকারিতা রয়েছে, যা সংস্থার অভ্যন্তরীণ SQL সার্ভার থেকে তথ্য সংগ্রহ করে নিত।
মে ২০২২	HOST1-এ একটি অতিরিক্ত লগ ফাইল শেষবার পরিবর্তন করা হয়েছে (T1070)। এই ফাইলে সংস্থার নেটওয়ার্কের জন্য প্রকৃত ব্যবহারকারীর নাম এবং পাসওয়ার্ডের জোড়া সংরক্ষিত রয়েছে বলে ধারণা করা হচ্ছে (T1078)।
মে ২০২২	একটি অতিরিক্ত লগ ফাইল শেষবার পরিবর্তিত হয়েছে (T1070)। এই ফাইলে HOST1 থেকে সংগ্রহ করা JWT সংরক্ষিত ছিল।
মে ২০২২	HOST1 (T1505.003) এ অতিরিক্ত ওয়েব শেল তৈরি হয়েছে। এই তারিখেই সংস্থা জানায় যে তারা এপ্রিল ২০২২-এ তৈরি হওয়া একটি ওয়েব শেলের উপস্থিতি খুঁজে বের করা করেছে এবং সেটি ASD-এর ACSC-কে রিপোর্ট করেছে।
মে ২০২২	HOST1-এ একাধিক স্ক্রিপ্ট তৈরি করা হয়েছে, যার মধ্যে একটি ছিল Log4jHotPatch.jar নামে।
মে ২০২২	আক্সেস গেটওয়ে হোস্টে iptables-save কমান্ড ব্যবহার করে দুটি ওপেন পোর্ট যুক্ত করা হয়েছে। এই পোর্ট দুটি ছিল ৯৯৯৮ এবং ৯৯৯৯ (T1572)।

হামলাকারীদের কৌশল ও পদ্ধতি

তদন্তের সময় যে কৌশল এবং পদ্ধতিগুলি চিহ্নিত হয়েছে, তা নিচে তুলে ধরা হয়েছে।

প্রাথমিক অ্যাক্সেস

T1190 সর্বসাধারণের জন্য উন্মুক্ত অ্যাপ্লিকেশনকে কাজে লাগানো

সম্ভবত, এই গোষ্ঠীটি রিমোট অ্যাক্সেস লগইন এবং আইডেন্টিটি ম্যানেজমেন্ট পণ্যের RCE, প্রিভিলেজ এসকেলেশন এবং অথেনটিকেশন বাইপাস দুর্বলতাগুলো কাজে লাগিয়ে নেটওয়ার্কে প্রাথমিক প্রবেশ করেছে।

এই প্রবেশ পদ্ধতিকে সবচেয়ে সম্ভাব্য ধরণ হিসেবে বিবেচনা করা হয়েছে নিম্নলিখিত কারণে:

- সার্ভার তখন এসব CVE-এর প্রতি দুর্বল ছিল;
- পরিচিত হ্যাকারদের অবকাঠামো থেকে এই দুর্বলতাগুলো কাজে লাগানোর চেষ্টা হয়েছিল; এবং
- দুর্বলতা কাজে লাগানোর চেষ্টা শুরু হওয়ার কিছুক্ষণ পরেই প্রথম সন্দেহজনক অভ্যন্তরীণ সাইবার আক্রমণের ঘটনাটি ঘটেছিল।

হামলা পরিচালনা

T1059.004 কমান্ড ও স্ক্রিপ্টিং ইন্টারপ্রেটার: ইউনিক্স শেল

উক্ত দুর্বলতাগুলো সফলভাবে কাজে লাগিয়ে, গোষ্ঠীটি সম্ভবত আক্রান্ত যন্ত্রে থাকা ইউনিক্স শেলে কমান্ড চালাতে সক্ষম হয়েছিল। তারা ঠিক কী কী কমান্ড চালিয়েছিল তা বলা সম্ভব নয় কারণ যন্ত্রে সেগুলোর লগ সংরক্ষিত ছিল না।

সিস্টেমে স্থায়ী অনুপ্রবেশ

T1505.003সার্ভার সফটওয়্যার কম্পোনেন্ট: ওয়েব শেল

আক্রমণকারীরা আক্রান্ত যন্ত্রে একাধিক ওয়েব শেল স্থাপন করেছে। সম্ভবত ভিন্ন ভিন্ন একাধিক গোষ্ঠী ওয়েব শেল স্থাপন করেছে, তবে এদের মধ্যে কম সংখ্যক গোষ্ঠী এসব ওয়েব শেল ব্যবহার করে কার্যক্রম চালিয়েছে। এই ওয়েব শেলগুলোর মাধ্যমে আক্রমণকারীরা আক্রান্ত যন্ত্রে ইচ্ছামতো কমান্ড চালাতে সক্ষম হয়েছে।

উচ্চ পর্যায়ের প্রবেশাধিকার

T1068 উচ্চ পর্যায়ের প্রবেশাধিকার অর্জনের জন্য সিস্টেম হ্যাক

প্রাপ্ত প্রমাণগুলো আক্রমণকারীরা ঠিক কোন স্তরের অধিকার অর্জন করেছে, তা স্পষ্ট করে না। তবে, তারা ওয়েব শেল ব্যবহার করে আক্রান্ত যন্ত্রে এমন একটি উচ্চ স্তরে পৌঁছাতো, যা ঐ যন্ত্রের ওয়েব সার্ভারের সমতুল্য ছিল। আক্রান্ত যন্ত্রে বিদ্যমান বলে ধারণা করা দুর্বলতাগুলো আক্রমণকারীদের সিস্টেমে প্রবেশ সুবিধা অর্জনের সুযোগ করে দিত।

ব্যবহারকারী নাম ও পাসওয়ার্ডের অননুমোদিত প্রবেশ

T1056.003 ইনপুট ক্যাপচার: ওয়েব পোর্টাল ক্যাপচার

আক্রান্ত যন্ত্রে প্রাপ্ত প্রমাণ থেকে জানা যায়, আক্রমণকারী শতাধিক প্রকৃত ব্যবহারকারীর ইউজারনেম ও পাসওয়ার্ড জোড়া, স্পষ্টাক্ষরে সংগ্রহ করেছিল, যেগুলিকে বৈধ বলে মনে করা হয়। সম্ভবত, তারা আসল অথেনটিকেশন প্রক্রিয়ার কিছু পরিবর্তন করে এই তথ্যগুলো একটি ফাইলে আউটপুট হিসেবে সংরক্ষণ করেছিল।

T1111 মাল্টি-ফ্যাক্টর অথেনটিকেশন ইন্টারসেপশন

আক্রমণকারী প্রকৃত লগইনের জন্য ব্যবহৃত MFA টোকেনের মান-ও সংগ্রহ করেছিল। এগুলো সম্ভবত অথেনটিকেশন প্রক্রিয়ার পরিবর্তনের মাধ্যমে একটি ফাইলে আউটপুট করানো হয়েছিল। তবে MFA টোকেনের নিরাপত্তা রক্ষায় ব্যবহৃত 'গোপন সার্ভার' আক্রান্ত হয়েছে বলে কোনো প্রমাণ নেই।

T1040 নেটওয়ার্কে চলা তথ্য চুরি করে দেখা

আক্রমণকারী আক্রান্ত যন্ত্রে HTTP ট্রাফিক ক্যাপচার করে JWTগুলি সংগ্রহ করেছে বলে ধারণা করা হচ্ছে। প্রমাণে দেখা যায় যে, আক্রান্ত যন্ত্রটিতে tcpdump নামক ইউটিলিটি চালানো হয়েছিল, যা আক্রমণকারীর জন্য এই JWTগুলি সংগ্রহের সম্ভাব্য মাধ্যম হতে পারে।

T1539ওয়েব সেশন কুকি চুরি

উপরোক্ত বর্ণনার ভিত্তিতে, আক্রমণকারী JWTগুলি সংগ্রহ করেছে, যা ওয়েব সেশন কুকি এর মতো কাজ করে। এই টোকেনগুলো পুনরায় ব্যবহার করে আক্রমণকারী আক্রান্ত যন্ত্রে আরও প্রবেশাধিকার অর্জন করতে পারতো।

তথ্য খোঁজা

T1046 নেটওয়ার্ক সার্ভিস ডিসকভারি

একই নেটওয়ার্ক সেগমেন্টে থাকা অন্যান্য যন্ত্র স্ক্যান করার জন্য আক্রান্ত যন্ত্রে nmap নামক নেটওয়ার্ক স্ক্যানিং টুল চালানোর প্রমাণ পাওয়া গেছে। অন্যান্য অ্যাক্সেসযোগ্য নেটওয়ার্ক সার্ভিস শনাক্ত করতে আক্রমণকারী সম্ভবত এই উপায়টি অবলম্বন করেছিল, যা ল্যাটারাল মুভমেন্ট বা নেটওয়ার্কের ভেতরে ধাপে ধাপে অনুপ্রবেশের সুযোগ তৈরি করতে পারে।

তথ্য সংগ্রহ

আক্রমণকারীরা কীভাবে তথ্য সংগ্রহ করেছে বা আক্রান্ত যন্ত্র অথবা অন্যান্য সিস্টেম থেকে ঠিক কী ধরনের তথ্য সংগ্রহ করা হয়েছে—সে সম্পর্কে স্পষ্ট প্রমাণ নেই। তবে সম্ভবত আক্রমণকারীরা আক্রান্ত যন্ত্রের সমস্ত ফাইলে প্রবেশাধিকার পেয়েছিল, যার মধ্যে চুরি করা লগইন তথ্য (T1003), MFA টোকেনের মান (T1111), এবং উপরোক্ত JWT অন্তর্ভুক্ত ছিল।

কমান্ড এবং নিয়ন্ত্রণ

T1071.001 অ্যাপ্লিকেশন লেয়ার প্রোটোকল: ওয়েব প্রোটোকল

কমান্ড এবং নিয়ন্ত্রণের জন্য আক্রমণকারীরা ওয়েব শেল ব্যবহার করেছিল। ওয়েব শেল কমান্ডসমূহ আক্রান্ত যন্ত্রে বিদ্যমান ওয়েব সার্ভার ব্যবহার করে HTTPS প্রোটোকলের মাধ্যমে পাঠানো হয়ে থাকতে পারে (T1572)।

T1001.003 ডেটা অবফাসকেশন বা ডেটার অপ্রাসঙ্গিকিকরণ: প্রোটোকল নকল করা

আক্রমণকারীরা আক্রান্ত ডিভাইসগুলোকে হামলার সূচনা পয়েন্ট হিসেবে ব্যবহার করেছে, যাতে তাদের কার্যকলাপ বৈধ ট্র্যাফিকের মতো মনে হয়।

সনাক্তকরণ ও প্রতিরোধ সুপারিশ

ASD-এর ACSC সাইবার নিরাপত্তা দুর্ঘটনা এড়াতে ASD জরুরি আট নিয়ন্ত্রণ এবং সংশ্লিষ্ট কৌশলসমূহ বাস্তবায়নের জন্য দৃঢ়ভাবে সুপারিশ করছে। APT40 দ্বারা অনুপ্রবেশ সনাক্ত ও প্রতিরোধে নিচে কিছু নেটওয়ার্ক নিরাপত্তা পদক্ষেপ গ্রহণ করার সুপারিশ করা হয়েছে, এরপর টেবিল ১-এ চারটি গুরুত্বপূর্ণ TTP-এর নির্দিষ্ট প্রতিরোধ ব্যবস্থা সংক্ষিপ্তভাবে ব্যাখ্যা করা হয়েছে।

শনাক্তকরণ

উল্লেখযোগ্য কিছু ফাইল C:\Users\Public* এবং C:\Windows\Temp* এর মতো অবস্থানে ড্রপ করা হয়েছে। এই লোকেশনগুলো ডেটা লেখার জন্য সুবিধাজনক জায়গা হিসেবে বিবেচিত হয়, কারণ সাধারণত এগুলো ওয়ার্ল্ড রাইটেবল, অর্থাৎ Windows-এ নিবন্ধিত সকল ইউজার অ্যাকাউন্টেরই এই ডিরেক্টরি ও সাবডিরেক্টরিতে অ্যাক্সেস থাকে। প্রায়ই যেকোনো ইউজার পরবর্তীতে এই ফাইলগুলিতে প্রবেশ করতে পারে, যা নেটওয়ার্কের ভেতরে ধাপে ধাপে অনুপ্রবেশ, ডিফেন্স এভেশন, লো-প্রিভিলেজ এক্সিকিউশন, এবং তথ্য পাচারের জন্য স্টেজিং–এর সুযোগ তৈরি করে।

এই ধরনের সন্দেহজনক লোকেশন থেকে ফাইল এক্সিকিউশনের ঘটনাগুলো শনাক্ত করার জন্য সিগমা পদ্ধতি ব্যবহৃত হয়, যেগুলো অস্বাভাবিক কার্যকলাপের ইঙ্গিত দিতে পারে। তবে, সকল ক্ষেত্রেই আক্রমণের প্রকৃতি ও উৎস নিশ্চিত করতে পরবর্তী তদন্ত অপরিহার্য।

শিরোনামঃ ওয়ার্ল্ড রাইটেবল এক্সিকিউশন - টেম্প

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

বিবরণ: C:\Windows\Temp ডিরেক্টরি থেকে প্রসেস এক্সিকিউশন শনাক্ত করা

পটভূমি:

এই নিয়মটি বিশেষভাবে C:\Windows\Temp* লোকেশন থেকে প্রসেস এক্সিকিউশন শনাক্ত করার উপর কেন্দ্রিত। Temp ডিরেক্টরি অনেক বেশি ব্যবহৃত হয় বৈধ অ্যাপ্লিকেশনগুলোর দ্বারা, ফলে C:\Windows এ অন্য ওয়ার্ল্ড রাইটেবল সাবডিরেক্টরিগুলোর তুলনায় এটি থেকে এক্সিকিউশনের ঘটনা তুলনামূলক কম সন্দেহজন হিসেবে মনে করা হয়।

SYSTEM বা NETWORK SERVICE ব্যবহারকারীর মাধ্যমে চালিত অ্যাপ্লিকেশনগুলো বাদ দিলে এই নিয়মে নির্বাচিত বৈধ কার্যকলাপের পরিমাণ উল্লেখযোগ্যভাবে কমে যায়। এর মানে হলো, এই নিয়মটি হয়তো উঁচু প্রিভিলেজ স্তরে হওয়া ক্ষতিকর এক্সিকিউশনগুলো ধরতে পারে না, তবে ব্যবহারকারী SYSTEM প্রিভিলেজে যেতে চাচ্ছে কি না, তা নির্ধারণের জন্য অন্য নিয়মগুলো ব্যবহার করার পরামর্শ দেওয়া হয়।

তদন্ত:

1. এই ফাইল এক্সিকিউশনের সাথে সরাসরি যুক্ত তথ্য বিশ্লেষণ করুন, যেমন— ব্যবহারকারীর প্রেক্ষাপট, এক্সিকিউশন ইন্টিগ্রিটি লেভেল, তৎক্ষণাৎ পরবর্তী কার্যক্রম, এবং ফাইলটি দ্বারা লোড হওয়া ইমেজগুলো।
2. সন্দেহজনক কার্যকলাপ কি না তা মূল্যায়নের জন্য হোস্টে থাকা সংশ্লিষ্ট প্রসেস, নেটওয়ার্ক, ফাইল ও অন্যান্য সহায়ক তথ্যসমূহ পর্যালোচনা করুন।
3. প্রয়োজনে রিভার্স ইঞ্জিনিয়ারিংয়ের জন্য ফাইলের একটি কপি সংগ্রহের চেষ্টা করুন, যাতে এর বৈধতা নির্ধারণ করা যায়।

রেফারেন্স:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

প্রস্তুতকারী: ASD's ACSC

তারিখ: 2024/06/19

স্ট্যাটাস: পরীক্ষামূলক

ট্যাগ:

- tlp.green
- classification.au.official
- attack.execution

লগ সোর্স:

ক্যাটাগরি: প্রক্রিয়া_তৈরি
পণ্য: windows

শনাক্তকরণ:

টেম্প:
চিত্র| শুরু হয়েছে: 'C:\\Windows\\Temp\\'
কমন_ টেম্প_পাথ:
চিত্র|re|ignorecase: 'C:\\Windows\\Temp\\\{[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]{12}\}\\'
সিস্টেম_ব্যবহারকারী:
ব্যবহারকারী:
- 'সিস্টেম'
- 'নেটওয়ার্ক সার্ভিস'

dismhost:

চিত্র|শেষ হয়েছে: 'dismhost.exe'

পরিচিত_মূল প্রক্রিয়া:

পরিচিত চিত্র |শেষ হয়েছে:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

শর্ত: টেম্প এবং না common_temp_path বা system_user বা dismhost বা known_parent)

ভুল সতর্কবার্তা:

- কিছু অ্যালাওলিস্ট অডিটিং অ্যাপ্লিকেশনকে Temp ফোল্ডার থেকে এক্সিকিউটেবল চালাতে দেখা গেছে।
- Temp ফোল্ডারটি বৈধভাবে বিভিন্ন ধরনের সেটআপ অ্যাপ্লিকেশন ও লঞ্চার ধারণ করে, তাই নিয়মটি প্রয়োগের আগে মনিটর করা নেটওয়ার্কে এই আচরণের প্রচলন কেমন (এবং এটি অ্যালাউলিস্ট করা সম্ভব কি না) তা বিবেচনা করা উচিত।

লেভেল: নিম্ন

শিরোনাম: ওয়ার্ল্ড রাইটেবল একজিকিউশন - নন - টেম্প সিস্টেম সাবডিরেক্টরি

আইডি: 5b187157-e892-4fc9-84fc-aa48aff9f997

বিবরণ: Windows OS ইনস্টলেশন লোকেশনের কোনো সাবডিরেক্টরিতে ওয়ার্ল্ড রাইটেবল লোকেশন থেকে প্রসেস এক্সিকিউশন শনাক্ত করুন।

পটভূমি:

এই নিয়মটি C:\ এর মধ্যে world writable ডিরেক্টরি থেকে এবং বিশেষভাবে C:\Windows* সাবডিরেক্টরি থেকে প্রসেস এক্সিকিউশন শনাক্ত করার জন্য প্রণীত, তবে C:\Windows\Temp ব্যতিক্রম হিসেবে বিবেচিত (যা সাধারণ অ্যাপ্লিকেশন দ্বারা ব্যাপকভাবে ব্যবহৃত হয় এবং তাই কম সন্দেহজনক সূচক হিসেবে গণ্য হয়।

AppData ফোল্ডারগুলো বাদ দেওয়া হয় যদি কোনো ফাইল SYSTEM হিসেবে চালিত হয় —এটি বহু সাময়িক অ্যাপ্লিকেশনের বৈধ এক্সিকিউশন পদ্ধতি।

নেটওয়ার্কে প্রাথমিক বেইসলাইন সম্পন্ন করে এবং এই লোকেশনগুলো থেকে পরিচিত বৈধ এক্সিকিউশন শনাক্ত করার পর, এই নিয়মটি খুব কমই সক্রিয় হওয়া উচিত।

তদন্ত:

1. এই ফাইল এক্সিকিউশন সম্পর্কিত সরাসরি তথ্য বিশ্লেষণ করুন, যেমনঃ ব্যবহারকারীর প্রেক্ষাপট, এক্সিকিউশন ইন্টিগ্রিটি লেভেল, তাৎক্ষণিক পরবর্তী কার্যক্রম, এবং ফাইল দ্বারা লোডকৃত ইমেজসমূহ।
2. হোস্টে থাকা সংশ্লিষ্ট প্রসেস, নেটওয়ার্ক, ফাইল ও অন্যান্য সহায়ক তথ্য বিশ্লেষণ করুন, যাতে নিধারণ করা যায় এই কার্যকলাপটি ক্ষতিকর কিনা।
3. প্রয়োজনে রিভার্স ইঞ্জিনিয়ারিংয়ের জন্য ফাইলের একটি কপি সংগ্রহের চেষ্টা করুন, যাতে এর বৈধতা নিধারণ করা যায়।

রেফারেন্স:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

প্রস্তুতকারী: ASD's ACSC

তারিখ: ২০২৪/০৬/১৯
স্ট্যাটাস: পরীক্ষামূলক

ট্যাগ:

- tlp.green
- classification.au.official
- attack.execution

লগ সোর্স:

ক্যাটাগরি: প্রক্রিয়া_তৈরি
পণ্য: windows

শনাক্তকরণ:

রাইটেবল_পাথ:

চিত্র| এটিতে রয়েছে:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'

- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

অ্যাপডেটা:

ছবি|এটিতে রয়েছে: '\\অ্যাপডেটা\\'
ব্যবহারকারী: 'সিস্টেম'

শর্ত: রাইটেবল_পাথ এবং অ্যাপডেটা নয়

ভুল সতর্কবার্তা:

অ্যালাউলিস্ট অডিটিং অ্যাপ্লিকেশনসমূহকে এই ডিরেক্টরিগুলোর মধ্য থেকে এক্সিকিউটেবল চালাতে দেখা গেছে।

সম্ভাবনা রয়েছে যে মনিটর করা পরিবেশে ব্যবহৃত স্ক্রিপ্ট এবং প্রশাসনিক টুলগুলি এই ডিরেক্টরিগুলোর কোনো একটিতে অবস্থান করতে পারে এবং এগুলোকে আলাদা আলাদা প্রেক্ষাপটে বিশ্লেষণ করা উচিত।

লেভেল: উচ্চ

শিরোনাম: ওয়ার্ল্ড রাইটেবল এক্সিকিউশন - ব্যবহারকারী

ID: 6dda3843-182a-4214-9263-925a80b4c634

বিবরণ: C:\Users\Public* এবং ব্যবহারকারীদের অন্যান্য ওয়ার্ল্ড রাইটেবল ফোল্ডার থেকে প্রসেস এক্সিকিউশন শনাক্ত করুন।

পটভূমি

AppData ফোল্ডারগুলো বাদ দেওয়া হয় যদি কোনো ফাইল SYSTEM হিসেবে চালিত হয় —এটি বহু সাময়িক অ্যাপ্লিকেশনের বৈধ এক্সিকিউশন পদ্ধতি।

তদন্ত:

1. এই ফাইল এক্সিকিউশনের সাথে সরাসরি যুক্ত তথ্য বিশ্লেষণ করুন, যেমন— ব্যবহারকারীর প্রেক্ষাপট, একিসকিউশন ইন্টিগ্রিটি লেভেল, তৎক্ষণাৎ পরবর্তী কার্যক্রম, এবং ফাইলটি দ্বারা লোড হওয়া ইমেজগুলো।
2. সন্দেহজনক কার্যকলাপ কি না তা মূল্যায়নের জন্য হোস্টে থাকা সংশ্লিষ্ট প্রসেস, নেটওয়ার্ক, ফাইল ও অন্যান্য সহায়ক তথ্যসমূহ পর্যালোচনা করুন।
3. প্রয়োজনে রিভার্স ইঞ্জিনিয়ারিংয়ের জন্য ফাইলের একটি কপি সংগ্রহের চেষ্টা করুন, যাতে এর বৈধতা নির্ধারণ করা যায়।

রেফারেন্স:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

প্রস্তুতকারী: ASD's ACSC

তারিখ: ২০২৪/০৬/১৯

স্ট্যাটাস: পরীক্ষামূলক

ট্যাগ:

- tlp.green
- classification.au.official
- attack.execution

লগ সোর্স:

ক্যাটাগরি: প্রক্রিয়া_তৈরি
পণ্য: windows

শনাক্তকরণ:

ব্যবহারকারী:

চিত্র| এটিতে রয়েছে:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

চিত্র| এটিতে রয়েছে: '\\ অ্যাপডেটা \\'
ব্যবহারকারী: ' সিস্টেম '

অবস্থা: ব্যবহারকারী, অ্যাপডেটা নয়

ভুল সতর্কবার্তা:

- সম্ভাবনা রয়েছে যে মনিটর করা পরিবেশে ব্যবহৃত স্ক্রিপ্ট এবং প্রশাসনিক টুলগুলি এই ডিরেকটরিগুলোর কোনো একটি তে অবস্থান করতে পারে এবং এগুলোকে আলাদা আলাদা প্রেক্ষাপটে বিশ্লেষণ করা উচিত।

লেভেল: মধ্যম

প্রতিকার ব্যবস্থা

লগিং

ASD-এর ACSC তদন্ত চলাকালে একটি সাধারণ সমস্যা ছিল—যেটি তদন্তের কার্যকারিতা ও গতি কমিয়ে দেয়—তা হলো ওয়েব সার্ভার রিকোয়েস্ট লগ, উইন্ডোজ ইভেন্ট লগ এবং ইন্টারনেট প্রক্সি লগ-এর ক্ষেত্রে সম্পূর্ণ ও ঐতিহাসিক লগিং তথ্যের অভাব।

ASD-এর ACSC উইন্ডোজ ইভেন্ট লগিং এবং ফরওয়ার্ডিং সংক্রান্ত তাদের নির্দেশনা পর্যালোচনা ও বাস্তবায়ন করার সুপারিশ করেছে, যার মধ্যে রয়েছে উইন্ডোজ ইভেন্ট লগিং রিপজিটরিতে থাকা কনফিগারেশন ফাইল ও স্ক্রিপ্ট ব্যবহার, এবং সিস্টেম মনিটরিং এর জন্য ইনফরমেশন সিকিউরিটি ম্যানুয়েল এর নির্দেশাবলী অনুসরণ করতে, যাতে লগগুলো কেন্দ্রীভূতভাবে সংরক্ষণ করা যায় এবং উপযুক্ত সময়কাল ধরে রাখা যায়।

প্যাচ ব্যবস্থাপনা:

ইন্টারনেটে উন্মুক্ত সকল ডিভাইস ও সার্ভিস—যেমন ওয়েব সার্ভার, ওয়েব অ্যাপ্লিকেশন, রিমোট অ্যাক্সেস গেটওয়ে—তৎক্ষণাৎ প্যাচ করুন। কেন্দ্রীভূত প্যাচ ব্যবস্থাপনা সিস্টেম বাস্তবায়নের কথা বিবেচনা করুন, যাতে প্রক্রিয়াটি স্বয়ংক্রিয় ও দ্রুততর হয়। ASD-এর ACSC সিস্টেম মনিটরিং এর জন্য ISM এর নির্দেশাবলী অনুসরণ করতে সুপারিশ করেছে, বিশেষ করে System Patching নিয়ন্ত্রণসমূহ যেখানে প্রযোজ্য।

আক্রমণকারীরা যেসব এক্সপ্লয়েট ব্যবহার করেছে, সেগুলোর বেশিরভাগই পাবলিকলি পরিচিত ছিল এবং প্যাচ বা প্রতিকার ব্যবস্থা পাওয়া যেত। প্রতিষ্ঠানগুলো নিশ্চিত করবে যে ইন্টারনেট-সংযুক্ত অবকাঠামোয় নিরাপত্তামূলক প্যাচ বা প্রতিকার ব্যবস্থা ৪৮ ঘণ্টার মধ্যে প্রয়োগ করা হয়েছে। সম্ভব হলে সর্বশেষ সংস্করণের সফটওয়্যার এবং অপারেটিং সিস্টেম ব্যবহার করার পরামর্শ দেওয়া হয়।

নেটওয়ার্ক বিভাজন

নেটওয়ার্ক বিভাজন এমন একটি কৌশল যা দুষ্কৃতিকারীদের জন্য সংস্থার সংবেদনশীল তথ্য খুঁজে বের করা এবং তাতে প্রবেশ করা অনেক কঠিন করে তোলে। নেটওয়ার্ক বিভাজন করুন, যাতে এক কম্পিউটার থেকে অন্য কম্পিউটারে অপ্রয়োজনীয় ট্রাফিক বন্ধ করে আক্রমণকারীদের পাশের সিস্টেমে ছড়িয়ে পড়া কঠিন হয়ে পড়ে। Active Directory এবং অন্যান্য প্রমাণীকরণ সার্ভারগুলো শুধুমাত্র নির্দিষ্ট কিছু মধ্যবর্তী সার্ভার (যাকে বলা হয় 'জাম্প সার্ভার') থেকে পরিচালনা করা উচিত। এই জাম্প সার্ভারগুলো নিয়মিত পর্যবেক্ষণ করা উচিত, উচ্চ নিরাপত্তা ব্যবস্থা থাকা উচিত, এবং কোন ব্যবহারকারী ও কোন ডিভাইস সংযোগ করতে পারবে, তা সীমিত করা উচিত।

যদিও কিছু ক্ষেত্রে ল্যাটারাল মুভমেন্ট (একবার প্রবেশ করার পর পাশের সিস্টেমে ছড়িয়ে পড়া) প্রতিরোধ করা গেছে, আরও নেটওয়ার্ক বিভাজন বিভাজন থাকলে আক্রমণকারীরা আরও কম তথ্য অ্যাক্সেস ও বের করে নিতে পারত।

অতিরিক্ত প্রতিকার ব্যবস্থা

নির্দেশিকা প্রস্তুতকারী সংস্থাগুলো APT40 এবং অন্যান্য TTP ব্যবহারের বিরুদ্ধে নিচের প্রতিরোধমূলক ব্যবস্থা গ্রহণের পরামর্শ দেয়।

- অপ্রয়োজনীয় নেটওয়ার্ক সার্ভিস, পোর্ট এবং প্রোটোকল বন্ধ করুন
- সঠিকভাবে কনফিগার করা ওয়েব অ্যাপ্লিকেশন ফায়ারওয়াল (WAF) ব্যবহার করুন, যাতে ওয়েব সার্ভার ও অ্যাপ্লিকেশন সুরক্ষিত থাকে।
- ব্যবহারকারীদের সার্ভার, ফাইল শেয়ার, এবং অন্যান্য রিসোর্সে সীমিত অ্যাক্সেস দিন।
- মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) এবং ম্যানেজড সার্ভিস অ্যাকাউন্ট ব্যবহার করুন, যাতে লগইন তথ্য হ্যাক বা পুনঃব্যবহার করা কঠিন হয়ে পড়ে। নিচের ইন্টারনেট-সংযুক্ত রিমোট অ্যাক্সেস সার্ভিসগুলোতে MFA প্রয়োগ করুন:
  - ওয়েব ও ক্লাউড-ভিত্তিক ইমেইল
  - সহযোগিতা প্ল্যাটফর্ম
  - ভার্চুয়াল প্রাইভেট নেটওয়ার্ক সংযোগ
  - রিমোট ডেস্কটপ সার্ভিস
- পুরাতন ও মেয়াদোত্তীর্ণ যন্ত্রপাতি প্রতিস্থাপন করুন

টেবিল ১ প্রতিকার কৌশল/পদ্ধতি

TTP	জরুরি আট প্রতিকার কৌশল	ISM কন্ট্রোল
প্রাথমিক অ্যাক্সেস T1190 ইন্টারনেট থেকে সরাসরি ব্যবহারযোগ্য অ্যাপ্লিকেশন হ্যাক	অ্যাপ্লিকেশনগুলো প্যাচ করুন অপারেটিং সিস্টেম প্যাচ করুন মাল্টি-ফ্যাক্টর অথেনটিকেশন অ্যাপ্লিকেশন নিয়ন্ত্রণ	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
হামলা পরিচালনা T1059 কম্যান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার	অ্যাপ্লিকেশন নিয়ন্ত্রণ মাইক্রোসফট অফিস ম্যাক্রো সীমিত করুন অ্যাডমিনিস্ট্রেটিভ সুবিধা সীমিত করুন	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
সিস্টেমে স্থায়ী অনুপ্রবেশ T1505.003 সার্ভার সফটওয়্যার কম্পোনেন্ট: ওয়েব শেল	অ্যাপ্লিকেশন নিয়ন্ত্রণ অ্যাডমিনিস্ট্রেটিভ সুবিধা সীমিত করুন	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
সিস্টেমে প্রাথমিক প্রবেশ/উচ্চ পর্যায়ের নিয়ন্ত্রণ নেয়া/ স্থায়ী অনুপ্রবেশ T1078 বৈধ অ্যাকাউন্ট	অপারেটিং সিস্টেম প্যাচ করুন মাল্টি-ফ্যাক্টর অথেনটিকেশন অপারেটিং সিস্টেম প্যাচ করুন অ্যাপ্লিকেশন নিয়ন্ত্রণ ব্যবহারকারীদের অ্যাপ্লিকেশনগুলোকে নিরাপদভাবে কনফিগার করা	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

সাধারণ ঝুঁকি শনাক্ত ও প্রতিরোধ সংক্রান্ত আরও পরামর্শ জানতে চাইলে, অনুগ্রহ করে এই সতর্কতামূলক পরামর্শের শেষে থাকা MITRE ATT&CK সারাংশে যেসব পদ্ধতি তালিকাভুক্ত রয়েছে—সেগুলোর প্রত্যেকটির জন্য MITRE ATT&CK ওয়েব পেজের ঝুঁকি প্রতিকার এবং শনাক্তকরণ অংশগুলো দেখে নিন।

দাবিত্যাগ

এই প্রতিবেদনে দেওয়া তথ্য শুধুমাত্র তথ্যগত উদ্দেশ্যে 'যেমন আছে' তেমনভাবেই প্রদান করা হয়েছে। নির্দেশিকা প্রস্তুতকারী সংস্থাগুলো কোনও বাণিজ্যিক প্রতিষ্ঠান, পণ্য, কোম্পানি বা পরিষেবা অনুমোদন করে না, যার মধ্যে এই নথিতে লিঙ্ক করা কোনও প্রতিষ্ঠান, পণ্য বা পরিষেবাও অন্তর্ভুক্ত। সার্ভিস মার্ক, ট্রেডমার্ক, প্রস্তুতকারক বা অন্য যেকোনোভাবে এই প্রতিবেদনে উল্লিখিত কোনো নির্দিষ্ট বাণিজ্যিক প্রতিষ্ঠান, পণ্য, প্রক্রিয়া বা সেবার উল্লেখ নির্দেশিকা প্রস্তুতকারী সংস্থাগুলোর অনুমোদন, সুপারিশ বা পক্ষপাতিত্ব বোঝায় না।

এই নথিটি TLP:CLEAR হিসেবে চিহ্নিত। এর তথ্য প্রকাশে কোনো সীমাবদ্ধতা নেই তথ্য ব্যবহারে অপব্যবহারের সম্ভাবনা খুব কম বা নেই—এমন ক্ষেত্রে, প্রযোজ্য নিয়ম ও প্রকাশের পদ্ধতি অনুসারে TLP:CLEAR ব্যবহার করা যেতে পারে। প্রচলিত কপিরাইট নিয়মের আওতায়, TLP:CLEAR তথ্য সীমাবদ্ধতা ছাড়াই বিতরণ করা যেতে পারে। Traffic Light Protocol (TLP) সংক্রান্ত আরও তথ্যের জন্য cisa.gov/tlp ওয়েবসাইট দেখুন।

MITRE ATT&CK – APT40 অতীতে কী কী কৌশলে সাইবার আক্রমণ চালিয়েছে

RECONNAISSANCE (TA0043)	
আক্রান্তের মালিকানাধীন ওয়েবসাইট অনুসন্ধান (T1594)	ভিকটিম পরিচয় তথ্য সংগ্রহ করুন: লগইন তথ্য (T1589.001)
সক্রিয় পরীক্ষা: দুর্বলতা পরীক্ষা (T1595.002)	ভিকটিম হোস্টের তথ্য সংগ্রহ করুন (T1592)
ওপেন ওয়েবসাইট/ডোমেন অনুসন্ধান করুন: সার্চ ইঞ্জিন (T1593.002)	ভিকটিম নেটওয়ার্কের তথ্য সংগ্রহ করুন: ডোমেন প্রোপার্টি (T1590.001)
ভিকটিম পরিচয় তথ্য সংগ্রহ করুন: ইমেল ঠিকানা (T1589.002)	

সম্পদ উন্নয়ন (TA0042)	
অবকাঠামো প্রস্তুত করুন: ডোমেইন (T1583.001)	অবকাঠামো প্রস্তুত করুন (T1583)
অবকাঠামো প্রস্তুত করুন: DNS সার্ভার (T1583.002)	অ্যাকাউন্টস হ্যাক করা (T1586)
সক্ষমতা তৈরি: কোড সাইনিং সার্টিফিকেট (T1587.002)	অবকাঠামো হ্যাক করা (T1584)
সক্ষমতা বিকাশ: ডিজিটাল সার্টিফিকেট (T1587.003)	সক্ষমতা বিকাশ: ম্যালওয়্যার (T1587.001)
সক্ষমতা অর্জন: কোড সাইনিং সার্টিফিকেট (T1588.003)	অ্যাকাউন্ট খোলা: ক্লাউড অ্যাকাউন্টস (T1585.003)
অবকাঠামো হ্যাক করা: নেটওয়ার্ক ডিভাইস (T1584.008)	সক্ষমতা অর্জন: ডিজিটাল সার্টিফিকেট (T1588.004)

প্রাথমিক প্রবেশাধিকার (TA0001)	
বৈধ অ্যাকাউন্ট (T1078)	ফিশিং (T1566)
বৈধ অ্যাকাউন্ট: পূর্বনির্ধারিত অ্যাকাউন্ট (T1078.001)	ফিশিং: স্পিয়ারফিশিং সংযুক্তি (T1566.001)
বৈধ অ্যাকাউন্ট: ডোমেইন অ্যাকাউন্ট (T1078.002)	ফিশিং: স্পিয়ারফিশিং লিঙ্ক (T1566.002)
এক্সটার্নাল রিমোট সার্ভিসেস (T1133)	ইন্টারনেটে যুক্ত অ্যাপ্লিকেশনকে কাজে লাগানো (T1190)
অজান্তে সংক্রমিত হওয়া (T1189)	

বাস্তবায়ন (TA0002)	
উইন্ডোজ ম্যানেজমেন্ট ইন্সট্রুমেন্টেশন (T1047)	কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার: পাইথন (T1059.006)
নির্ধারিত করণীয়/কাজ: (T1053.002) এ	কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার: জাভাস্ক্রিপ্ট (T1059.007)
নির্ধারিত কাজ/কাজ: নির্ধারিত কাজ (T1053.005)	নেটিভ API (T1106)
কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার (T1059)	আন্তঃপ্রক্রিয়া যোগাযোগ (T1559)
কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার: উইন্ডোজ কমান্ড শেল (T1059.003)	সিস্টেম পরিষেবা: সার্ভিসে হামলা পরিচালনা (T1569.002)
কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার: পাওয়ারশেল (T1059.001)	ক্লায়েন্ট-সাইডে কোড চালানোর জন্য দুর্বলতা ব্যবহার (T1203)
কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার: ভিজ্যুয়াল বেসিক (T1059.005)	ব্যবহারকারীর সম্পাদন: ক্ষতিকারক ফাইল (T1204.002)
কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার: ইউনিক্স শেল (T1059.004)	কমান্ড এবং স্ক্রিপ্টিং ইন্টারপ্রেটার: অ্যাপল স্ক্রিপ্ট (T1059.002)
নির্ধারিত কাজ/কাজ: ক্রোন (T1053.003)	সফটওয়্যার ডিপ্লয়মেন্ট টুলস (T1072)

সিস্টেমে স্থায়ী অনুপ্রবেশ	
বৈধ অ্যাকাউন্ট (T1078)	সার্ভার সফটওয়্যার কম্পোনেন্ট: ওয়েব শেল (T1505.003)
অফিস অ্যাপ্লিকেশন স্টার্টআপ: অফিস টেমপ্লেট ম্যাক্রো (T1137.001)	সিস্টেম প্রক্রিয়া তৈরি বা পরিবর্তন করুন: উইন্ডোজ সার্ভিস (T1543.003)
নির্ধারিত কাজ/কাজ: (T1053.002) এ	বুট অথবা লগঅন অটোস্টার্ট এক্সিকিউশন: রেজিস্ট্রি রান কী / স্টার্টআপ ফোল্ডার (T1547.001)
নির্ধারিত কাজ/কাজ: নির্ধারিত কাজ (T1053.005)	বুট অথবা লগঅন অটোস্টার্ট এক্সিকিউশন: শর্টকাট পরিবর্তন (T1547.009)
এক্সটার্নাল রিমোট সার্ভিসেস (T1133)	হাইজ্যাক কার্যকর করার প্রক্রিয়া: DLL অনুসন্ধান অর্ডার হাইজ্যাকিং (T1574.001)
নির্ধারিত কাজ/কাজ: ক্রোন (T1053.003)	হাইজ্যাক কার্যকর করার প্রক্রিয়া: DLL সাইড-লোডিং (T1574.002)
অ্যাকাউন্ট পরিবর্তন করে ফেলা (T1098)	বৈধ অ্যাকাউন্ট: ক্লাউড অ্যাকাউন্টস (T1078.004)
বৈধ অ্যাকাউন্ট: ডোমেইন অ্যাকাউন্ট (T1078.002)	

উচ্চ পর্যায়ের নিয়ন্ত্রণ (TA0004)	
নির্ধারিত কাজ/কাজ: (T1053.002) এ	সিস্টেম প্রক্রিয়া তৈরি বা পরিবর্তন করুন: উইন্ডোজ সার্ভিস (T1543.003)
নির্ধারিত করণীয়/কাজ: নির্ধারিত করণীয় (T1053.005)	বুট অথবা লগঅন অটোস্টার্ট এক্সিকিউশন: রেজিস্ট্রি রান কী / স্টার্টআপ ফোল্ডার (T1547.001)
বৈধ প্রক্রিয়ায় ম্যালওয়্যার ঢুকানো: থ্রেড এক্সিকিউশন হাইজ্যাকিং (T1055.003)	বুট অথবা লগঅন অটোস্টার্ট এক্সিকিউশন: শর্টকাট পরিবর্তন (T1547.009)
বৈধ প্রক্রিয়ায় ম্যালওয়্যার ঢুকানো: বৈধ প্রসেসকে ফাঁকা করে ক্ষতিকর কার্যক্রম চালানো (T1055.012)	হাইজ্যাক কার্যকর করার প্রক্রিয়া: DLL অনুসন্ধান অর্ডার হাইজ্যাকিং (T1574.001)

উচ্চ পর্যায়ের নিয়ন্ত্রণ নেয়া (TA0004)	
বৈধ অ্যাকাউন্ট: ডোমেইন অ্যাকাউন্ট (T1078.002)	উচ্চ পর্যায়ের নিয়ন্ত্রণ প্রতিষ্ঠার জন্য হামলা (T1068)
অ্যাক্সেস টোকেন ম্যানিপুলেশন: টোকেন ছদ্মবেশ ধারণ/চুরি (T1134.001)	নির্দিষ্ট ঘটনার মাধ্যমে কার্যক্রম শুরু: ইউনিক্স শেল কনফিগারেশন পরিবর্তন (T1546.004)
বৈধ প্রক্রিয়ায় ম্যালওয়্যার ঢুকানো: ডাইনামিক-লিঙ্ক লাইব্রেরি ঢুকিয়ে কোড চালানো (T1055.001)	বৈধ অ্যাকাউন্ট: ডোমেইন অ্যাকাউন্ট (T1078.002)
বৈধ অ্যাকাউন্ট: স্থানীয় অ্যাকাউন্ট (T1078.003)	

প্রতিরক্ষা ফাঁকি (TA0005)	
রুটকিট (T1014)	পরোক্ষ কমান্ড এক্সিকিউশন (T1202)
অস্পষ্ট ফাইল বা তথ্য (T1027)	সিস্টেম বাইনারি প্রক্সি এক্সিকিউশন: মশতা (T1218.005)
অস্পষ্ট ফাইল বা তথ্য: সফটওয়্যার প্যাকিং (T1027.002)	সিস্টেম বাইনারি প্রক্সি এক্সিকিউশন: Regsvr32 (T1218.010)
অস্পষ্ট ফাইল বা তথ্য: স্টেগানোগ্রাফি (T1027.003)	নিরাপত্তার যাচাইকরণকে ধোঁকা দেওয়া: কোড সাইনিং (T1553.002)
অস্পষ্ট ফাইল বা তথ্য: ডেলিভারির পরে কম্পাইল করুন (T1027.004)	ফাইল এবং ডিরেক্টরি অনুমতি পরিবর্তন: লিনাক্স এবং ম্যাক ফাইল এবং ডিরেক্টরি অনুমতি পরিবর্তন (T1222.002)
ভুয়া পরিচয় নিয়ে বৈধ সিস্টেমে ঢুকে পড়া: বৈধ নাম বা অবস্থান মিলান (T1036.005)	ভার্চুয়ালাইজেশন/স্যান্ডবক্স ফাঁকি: সিস্টেম চেক (T1497.001)
বৈধ প্রক্রিয়ায় ম্যালওয়্যার ঢুকানো: বৈধ প্রসেসের থ্রেড হাইজ্যাক করে ম্যালওয়্যার চালানো (T1055.003)	ভুয়া পরিচয় নিয়ে বৈধ সিস্টেমে ঢুকে পড়া (T1036)
প্রতিফলিত কোড লোডিং (T1620)	দুর্বল প্রতিরক্ষা: সিস্টেম ফায়ারওয়াল (T1562.004) অক্ষম বা সংশোধন করুন
বৈধ প্রক্রিয়ায় ম্যালওয়্যার ঢুকানো: প্রক্রিয়া ফাঁকা (T1055.012)	শিল্পকর্ম লুকান: লুকানো ফাইল এবং ডিরেক্টরি (T1564.001)
সূচক অপসারণ: ফাইল মুছে ফেলা (T1070.004)	শিল্পকর্ম লুকান: লুকানো জানালা (T1564.003)
সূচক অপসারণ: টাইমস্টম্প (T1070.006)	হাইজ্যাক কার্যকর করার প্রক্রিয়া: DLL অনুসন্ধান অর্ডার হাইজ্যাকিং (T1574.001)
সূচক অপসারণ: উইন্ডোজ ইভেন্ট লগ সাফ করুন (T1070.001)	হাইজ্যাক কার্যকর করার প্রক্রিয়া: ডিএলএল সাইড-লোডিং (T1574.002)
রেজিস্ট্রি পরিবর্তন করুন (T1112)	ওয়েব সার্ভিস (T1102)
ফাইল বা তথ্য ডিঅবফাস্কেট/ডিকোড করুন (T1140)	ভুয়া পরিচয় নিয়ে বৈধ সিস্টেমে ঢুকে পড়া: ভুয়া টাস্ক বা সার্ভিসকে বৈধ নাম দিয়ে চালানো (T1036.004)
সিস্টেমের প্রতিরক্ষা ভেঙে ফেলা (T1562)	

ব্যবহারকারী নাম ও পাসওয়ার্ডের অননুমোদিত প্রবেশ (TA0006)	
ওএস ক্রেডেনশিয়াল ডাম্পিং: LSASS মেমোরি (T1003.001)	অনিরাপদ লগইন তথ্য: ফাইলগুলিতে লগইন তথ্য (T1552.001)
ওএস ক্রেডেনশিয়াল ডাম্পিং: এনটিডিএস (T1003.003)	বারবার চেষ্টা করে নিরাপত্তা ভেঙে ফেলা: পাসওয়ার্ড অনুমান (T1110.001)
নেটওয়ার্কে চলা তথ্য চুরি করে দেখা (T1040)	জোরপূর্বক প্রমাণীকরণ (T1187)

ব্যবহারকারী নাম ও পাসওয়ার্ডের অননুমোদিত প্রবেশ (TA0006)	
পাসওয়ার্ড স্টোর থেকে প্রাপ্ত লগইন তথ্য: কীচেইন (T1555.001)	কার্বেরোসের টিকিট চুরি বা জাল করা: কার্বেরোস্টিং (T1558.003)
ইনপুট ক্যাপচার: কীলগিং (T1056.001)	মাল্টি-ফ্যাক্টর অথেনটিকেশন ইন্টারসেপশন (T1111)
ওয়েব সেশন কুকি চুরি (T1539)	অ্যাপ্লিকেশন অ্যাক্সেস টোকেন চুরি (T1528)
লগইন তথ্যে প্রবেশের জন্য হামলা (T1212)	বারবার চেষ্টা করে নিরাপত্তা ভেঙে ফেলা: পাসওয়ার্ড ক্র্যাকিং (T1110.002)
ইনপুট ক্যাপচার: ওয়েব পোর্টাল ক্যাপচার (T1056.003)	ওএস ক্রেডেনশিয়াল ডাম্পিং: ডিসিসিঙ্ক (T1003.006)
পাসওয়ার্ড স্টোর (T1555) থেকে প্রাপ্ত লগইন তথ্য	পাসওয়ার্ড স্টোর থেকে প্রাপ্ত লগইন তথ্য: ওয়েব ব্রাউজার থেকে প্রাপ্ত প্রমাণপত্রাদি (T1555.003)

খুঁজে বের করা (TA0007)	
সিস্টেম সার্ভিস খুঁজে বের করা (T1007)	সিস্টেম ইনফরমেশন খুঁজে বের করা (T1082)
অ্যাপ্লিকেশন উইন্ডো খুঁজে বের করা (T1010)	অ্যাকাউন্ট খুঁজে বের করা: স্থানীয় অ্যাকাউন্ট (T1087.001)
কোয়েরি রেজিস্ট্রি (T1012)	সিস্টেম ইনফরমেশন ডিসকভারি, টেকনিক T1082 - এন্টারপ্রাইজ | MITER ATT&CK®
ফাইল এবং ডিরেক্টরি খুঁজে বের করা (T1083)	সিস্টেম টাইম খুঁজে বের করা (T1124)
নেটওয়ার্ক সার্ভিস খুঁজে বের করা (T1046)	সিস্টেম মালিক/ব্যবহারকারী খুঁজে বের করা (T1033)
রিমোট সিস্টেম খুঁজে বের করা (T1018)	ডোমেন ট্রাস্ট খুঁজে বের করা (T1482)
অ্যাকাউন্ট খুঁজে বের করা: ইমেল অ্যাকাউন্ট (T1087.003)	অ্যাকাউন্ট খুঁজে বের করা: ডোমেইন অ্যাকাউন্ট (T1087.002)
সিস্টেম নেটওয়ার্ক সংযোগ খুঁজে বের করা (T1049)	ভার্চুয়ালাইজেশন/স্যান্ডবক্স ফাঁকি: সিস্টেম চেক (T1497.001)
প্রক্রিয়া খুঁজে বের করা (T1057)	সফটওয়্যার খুঁজে বের করা (T1518)
অনুমতি গোষ্ঠী খুঁজে বের করা: ডোমেন গ্রুপ (T1069.002)	নেটওয়ার্ক শেয়ার ডিসকভারি, টেকনিক T1135 - এন্টারপ্রাইজ | MITRE ATT&CK®
সিস্টেম নেটওয়ার্ক কনফিগারেশন খুঁজে বের করা: ইন্টারনেট সংযোগ খুঁজে বের করা (T1016.001)	

নেটওয়ার্কের ভেতরে ধাপে ধাপে অনুপ্রবেশে সক্ষম (TA0008)	
দূরবর্তী পরিষেবা: রিমোট ডেস্কটপ প্রোটোকল (T1021.001)	দূরবর্তী সার্ভিসেস (T1021)
দূরবর্তী পরিষেবা: SMB/Windows অ্যাডমিন শেয়ার (T1021.002)	বিকল্প প্রমাণীকরণ উপাদান ব্যবহার করুন: টিকিট পাস করা (T1550.003)
দূরবর্তী পরিষেবা: উইন্ডোজ রিমোট ম্যানেজমেন্ট (T1021.006)	ল্যাটেরাল টুল ট্রান্সফার (T1570)

সংগ্রহ (TA0009)	
স্থানীয় সিস্টেম (T1005) থেকে তথ্য	সংগৃহীত তথ্য সংরক্ষণাগারভুক্ত করুন: লাইব্রেরির মাধ্যমে সংরক্ষণাগার (T1560.002)
নেটওয়ার্ক শেয়ার্ড ড্রাইভ (T1039) থেকে ডেটা	ইমেল সংগ্রহ: রিমোট ইমেল সংগ্রহ (T1114.002)

সংগ্রহ (TA0009)	
ইনপুট ক্যাপচার: কীলগিং (T1056.001)	ক্লিপবোর্ড ডেটা (T1115)
স্বয়ংক্রিয় সংগ্রহ (T1119)	তথ্য সংগ্রহস্থল (T1213) থেকে প্রাপ্ত তথ্য
ইনপুট ক্যাপচার: ওয়েব পোর্টাল ক্যাপচার (T1056.003)	ডেটা পর্যায়ভুক্ত: রিমোট ডেটা স্টেজিং (T1074.002)
ডেটা পর্যায়ভুক্ত: স্থানীয় ডেটা স্টেজিং (T1074.001)	সংগৃহীত তথ্য সংরক্ষণাগারভুক্ত করুন (T1560)
ইমেল সংগ্রহ (T1114)	

তথ্য পাচার (TA0010)	
C2 চ্যানেলের উপর এক্সফিল্ট্রেশন (T1041)	বিকল্প প্রোটোকলের মাধ্যমে তথ্য পাচার: অসমমিতিক এনক্রিপ্টেড নন-C2 প্রোটোকলের মাধ্যমে তথ্য পাচার (T1048.002)
বিকল্প প্রোটোকলের মাধ্যমে তথ্য পাচার (T1048)	ওয়েব সার্ভিসের মাধ্যমে তথ্য পাচার: ক্লাউড স্টোরেজে তথ্য পাচার (T1567.002)

কমান্ড এবং নিয়ন্ত্রণ (TA0011)	
তথ্য অস্পষ্টতা: প্রোটোকল ছদ্মবেশ (T1001.003)	ওয়েব পরিষেবা: ডেড ড্রপ রেজলভার (T1102.001)
সাধারণত ব্যবহৃত পোর্ট (T1043)	ওয়েব পরিষেবা: একমুখী যোগাযোগ (T1102.003)
অ্যাপ্লিকেশন লেয়ার প্রোটোকল: ওয়েব প্রোটোকল (T1071.001)	ইনগ্রেস টুল ট্রান্সফার (T1105)
অ্যাপ্লিকেশন লেয়ার প্রোটোকল: ফাইল ট্রান্সফার প্রোটোকল (T1071.002)	প্রক্সি: অভ্যন্তরীণ প্রক্সি (T1090.001)
প্রক্সি: বহিরাগত প্রক্সি (T1090.002)	নন-স্ট্যান্ডার্ড পোর্ট (T1571)
প্রক্সি: মাল্টি-হপ প্রক্সি (T1090.003)	একটা প্রোটোকলের ভেতরে আরেকটা লুকিয়ে তথ্য পাঠানো (T1572)
ওয়েব পরিষেবা: দ্বিমুখী যোগাযোগ (T1102.002)	এনক্রিপ্ট করা চ্যানেল (T1573)
এনক্রিপ্ট করা চ্যানেল: অসমমিতিক ক্রিপ্টোগ্রাফি (T1573.002)	ইনগ্রেস টুল ট্রান্সফার (T1105)
প্রক্সি, টেকনিক T1090 - এন্টারপ্রাইজ | MITER ATT&CK®	

ইমপ্যাক্ট (TA0040)	
সার্ভিস স্টপ (T1489)	ডিস্ক ওয়াইপ (T1561)
সিস্টেম শাটডাউন/রিবুট (T1529)	রিসোর্স হাইজ্যাকিং (T1496)

মন্তব্য

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 ভেতরে ব্যবহারের জন্য উপলভ্য।

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre