ការប្រុងប្រៀប និងឆ្លើយតបទៅនឹង ការវាយប្រហារដោយបិទសេវាកម្ម

បោះពុម្ពលើកទីមួយ៖ ខែកញ្ញា ឆ្នាំ2011
បានធ្វើបច្ចុប្បន្នភាពចុងក្រោយ៖ ខែមីនា ឆ្នាំ2025

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

សេចក្តីផ្តើម

ការបោះពុម្ពផ្សាយនេះបានបង្កើតឡើងដោយអគ្គនាយកដ្ឋានស៊ើបសញ្ញាសារអេឡិចត្រូនិកអូស្ត្រាលី (ASD) ដោយសហការជាមួយ មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិប្រទេសនូវែលសេឡង់ (NCSC-NZ), ក្រុមហ៊ុន Akamai Technologies Ltd និងក្រុមហ៊ុន Cloudflare Pty Ltd ដើម្បីឆ្លើយតបទៅនឹងនិន្នាការកើនឡើងនៃការវាយប្រហារដោយបិទសេវាកម្ម (DoS) នៅក្នុងតំបន់របស់យើង។ វាផ្តល់ការណែនាំដល់ស្ថាប័ននានាស្តីពីឧត្តមានុវត្តន៍ស្តីពីការបន្ធូរបន្ថយដោយផ្អែកលើឧបាយកលពាណិជ្ជកម្មកាត់បន្ថយការគំរាមកំហែងដែលកើតឡើងនៅពេលបច្ចុប្បន្ន ដើម្បីប្រុងប្រៀប និងឆ្លើយតបទៅនឹងការវាយប្រហារ DoS។

យើងសូមណែនាំឱ្យអានការណែនាំនេះ ដោយភ្ជាប់ជាមួយនឹងឯកសារបោះពុម្ពផ្សាយស្តីពី *ឧបករណ៍នានាដែលភ្ជាប់តាមប្រព័ន្ធអ៊ីនធឺណិត (Internet of Things devices)* របស់ ASD និង *ការធានាសុវត្ថិភាព វ៉ាយហ្វាយ និងរ៉ៅទ័រ* របស់អ្នក។ ឯកសារបោះពុម្ពផ្សាយទាំងនេះ ជួយបុគ្គលម្នាក់ៗឱ្យជៀសវាងការរួមចំណែកដោយអចេតនាចំពោះការវាយប្រហារ DoS ដែលអាចប៉ះពាល់ដល់អ្នកដទៃ។

ការវាយប្រហារ DoS គឺជាការវាយប្រហារតាមអ៊ីនធឺណិត ដែលបានរចនាឡើងដើម្បីរំខាន ឬធ្វើឱ្យខូចសេវាកម្មអនឡាញនានាដូចជាគេហទំព័រ អ៊ីមែល និងសេវាកម្មប្រព័ន្ធឈ្មោះដែន (DNS) ដើម្បីបដិសេធការចូលប្រើដល់អ្នកប្រើប្រាស់ដែលត្រឹមត្រូវតាមច្បាប់នានា។ ជាធម្មតា នេះត្រូវបានសម្រេចដោយបំពោកសេវាកម្មអនឡាញជាមួយនឹងទិន្នន័យ ការតភ្ជាប់ ឬសំណើនានាដើម្បីសន្ធប់សេវាកម្ម និងធ្វើឱ្យខូចមុខងាររបស់វា។

ការវាយប្រហារ DoS ជាធម្មតាទាមទារឱ្យមានចំនួនចរាចរបណ្តាញច្រើន ដើម្បីទទួលបានជោគជ័យ។ វាកំពុងក្លាយជារឿងទូទៅកាន់តែច្រើនឡើង ដែលមួយផ្នែកដោយសារតែការកើនឡើងនៃចំនួនឧបករណ៍នានាដែលភ្ជាប់តាមប្រព័ន្ធអ៊ីនធឺណិត (IoT) ដែលត្រូវបានសម្របសម្រួលយ៉ាងងាយស្រួល។ ដោយសារក្រុមហ៊ុនផលិត IoT តែងតែផ្តល់អាទិភាពដល់បទពិសោធន៍អ្នកប្រើប្រាស់ច្រើនជាងសន្តិសុខអ៊ីនធឺណិត ឧបករណ៍ដែលងាយរងគ្រោះនានាអាចរួមបញ្ចូលរបស់របរប្រើប្រាស់ក្នុងផ្ទះធម្មតាដែលភ្ជាប់ទៅអ៊ីនធឺណិត ដូចជាទូរទស្សន៍ឆ្លាតវៃ កំសៀវ ម៉ាស៊ីនបូមធូលី និងប្រព័ន្ធសន្តិសុខ។ ឧបករណ៍ទាំងនេះ ជារឿយៗអាចត្រូវបានសម្របសម្រួលពីចម្ងាយដោយតួអង្គព្យាបាទនានាដើម្បីបង្កើត ‘បណ្តាញឧបករណ៍ដែលងាយរងការវាយប្រហារ’ ដើម្បីបង្កើតចរាចរបណ្តាញនេះ ដែលអាចបណ្តាលឱ្យគ្រួសារ និងស្ថាប័ននានារួមចំណែកដោយអចេតនាចំពោះហេដ្ឋារចនាសម្ព័ន្ធដែលអនុញ្ញាតឱ្យការវាយប្រហារ DoS កើតឡើង។

សកម្មភាពថ្មីៗបង្ហាញថា នៅពេលដែលតួអង្គព្យាបាទបានសម្របសម្រួលឧបករណ៍ IoT មួយចំនួនធំ ពួកគេអាចជួល ឬលក់ហេដ្ឋារចនាសម្ព័ន្ធនេះទៅឱ្យឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត និងសកម្មជនចោរបច្ចេកវិទ្យា ដែលចាប់អារម្មណ៍កាន់តែខ្លាំងក្នុងការអនុវត្តការវាយប្រហារ DoS ប្រឆាំងនឹងគោលដៅនានាដែលពួកគេជ្រើសរើស។ ក្នុងករណីភាគច្រើន ការវាយប្រហារ DoS ត្រូវបានអនុវត្តដើម្បីបង្កឱ្យមានការបាត់បង់ផលិតភាព និងហិរញ្ញវត្ថុរបស់ស្ថាប័ន ឬដើម្បីទទួលបានការយកចិត្តទុកដាក់ជាសាធារណៈសម្រាប់ហេតុផលមួយ។ ឧទាហរណ៍នៃសកម្មភាពនេះត្រូវបានពិពណ៌នានៅក្នុង *តួអង្គសម្របសម្រួលរ៉ៅទ័រ ដែលភ្ជាប់ដោយសាធារណរដ្ឋប្រជាមានិតចិនរបស់ ASD និងក្រុមប្រឹក្សាត្រួតពិនិត្យ* ឧបករណ៍ IoT សម្រាប់ប្រតិបត្តិការបណ្តាញឧបករណ៍ដែលងាយរងការវាយប្រហារ។

នៅពេលដែលសេដ្ឋកិច្ចរបស់យើងចម្រើនទៅកាន់ពិភពឌីជីថល ហើយចំនួនឧបករណ៍ IoT ដែលមិនមានសុវត្ថិភាពភ្ជាប់ទៅអ៊ីនធឺណិតកើនឡើង ការវាយប្រហារ DoS ទំនងជានឹងបន្តកើនឡើង។

ដើម្បីរំខាន ឬធ្វើឱ្យខូចសេវាកម្មអនឡាញរបស់ស្ថាប័នមួយ តួអង្គព្យាបាទប្រើវិធីសាស្ត្រមួយចំនួន រួមទាំង៖

- បង្វែរបរិមាណចរាចរនៃបណ្តាញដែលមិនចង់បានដ៏ធំមួយទៅកាន់សេវាកម្មអនឡាញនានា ក្នុងការប៉ុនប៉ងបំផ្លាញចំនួនអតិបរមានៃទិន្នន័យផ្ទេរឆ្លងកាត់បណ្តាញដែលមានទាំងអស់
- បង្វែរចរាចរបណ្តាញដែលបានកែសម្រួលទៅកាន់សេវាកម្មអនឡាញនានា ក្នុងការប៉ុនប៉ងបំផ្លាញធនធានដំណើរការកុំព្យូទ័ររបស់ពួកគេ
- ប្រើប្រាស់កុំព្យូទ័រច្រើន ឧបករណ៍ IoT ឬឧបករណ៍ដែលភ្ជាប់អ៊ីនធឺណិតផ្សេងទៀត ដើម្បីបង្វែរចរាចរបណ្តាញទៅកាន់សេវាកម្មអនឡាញនានាពីទិសដៅជាច្រើន និងក្នុងទ្រង់ទ្រាយកាន់តែធំ ប្រភេទការវាយប្រហារ DoS ទូទៅដែលគេហៅថាការវាយប្រហារ DoS (DDoS) បែងចែកជាច្រើនមុខសញ្ញា
- ប្លន់យកមកគ្រប់គ្រងការចុះឈ្មោះដែនអាសយដ្ឋានបណ្តាញ ឬម៉ាស៊ីនមេ DNS របស់ស្ថាប័ន ក្នុងការប៉ុនប៉ងបង្វែរអ្នកប្រើប្រាស់ត្រឹមត្រូវតាមច្បាប់ ចេញពីសេវាកម្មអនឡាញរបស់ស្ថាប័ន។

ស្ថាប័នមិនអាចជៀសផុតពីគោលដៅនៃការវាយប្រហារ DoS បានទេ ប៉ុន្តែមានវិធានការមួយចំនួនដែលស្ថាប័នអាចអនុវត្តដើម្បីប្រុងប្រៀប និងកាត់បន្ថយផលប៉ះពាល់របស់ពួកគេ។ ប្រុងប្រៀបសម្រាប់ការវាយប្រហារ DoS មុនពេលវាកើតឡើង គឺជាយុទ្ធសាស្ត្រដ៏ល្អបំផុត ពីព្រោះបើគ្មានការប្រុងប្រៀបទេនោះ វាពិបាក និងមិនសូវមានប្រសិទ្ធភាពក្នុងការឆ្លើយតបក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS។

ទោះបីជាស្ថាប័នផ្តោតជាចម្បងលើការការពារខ្លួនពីការវាយប្រហារ DoS ក៏ដោយ ក៏ពួកគេគួរតែចាត់វិធានការដើម្បីការពារសេវាកម្មអនឡាញ និងឧបករណ៍ដែលភ្ជាប់អ៊ីនធឺណិតរបស់ពួកគេ ពីការបំពានដោយតួអង្គព្យាបាទដើម្បីយកអ្នកដទៃជាគោលដៅ។

ការប្រុងប្រៀបសម្រាប់ការវាយប្រហារ DoS

នៅក្នុងបរិបទនៃការកើនឡើងនៃការវាយប្រហារ DoS នៅទូទាំងតំបន់របស់យើង មុនពេលអនុវត្តវិធានការណាមួយដើម្បីប្រុងប្រៀបសម្រាប់ការវាយប្រហារ DoS ស្ថាប័នរបស់អ្នក គួរវាយតម្លៃតម្រូវការអាជីវកម្មរបស់ខ្លួនជាមុនសិន ដើម្បីកំណត់ថាតើសេវាកម្មអនឡាញនីមួយៗរបស់អ្នក ត្រូវតែបន្តដំណើរការក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS ឬប្រសិនបើការរំខានសេវាកម្មបណ្តោះអាសន្នអាចទទួលយកបាន។

ប្រសិនបើស្ថាប័នរបស់អ្នកចង់បង្កើនសមត្ថភាពរបស់ខ្លួន ក្នុងការទប់ទល់នឹងការវាយប្រហារ DoS អ្នកគួរតែអនុវត្តវិធានការខាងក្រោមយ៉ាងសកម្មជាមុន នៅពេលណាដែលសមស្រប និងជាក់ស្តែង មុនពេលការវាយប្រហារ DoS កើតឡើង។

- ប្រសិនបើស្ថាប័នរបស់អ្នកកំពុងប្រើប្រាស់បណ្តាញផ្តល់មាតិកា (CDN) អ្នកគួរតែអនុវត្តវិធានការបន្ថែមខាងក្រោមនៅពេលណាដែលសមស្រប និងជាក់ស្តែង។
  - ពិចារណាប្រើ CDN ដែលរួមបញ្ចូលមុខងារដើម្បីការពារម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នក ពីកម្មវិធីផ្សេងៗគ្នា និងការវាយប្រហារស្រទាប់បណ្តាញ – CDNs មួយចំនួនអាចដាក់បញ្ចូលលក្ខណៈពិសេសទាំងនេះ ជាផ្នែកនៃជញ្ជាំងភ្លើង (firewall) ការពារកម្មវិធីគេហទំព័រចុងក្រោយបំផុត។
  - ជៀសវាងការលាតត្រដាងជាសាធារណៈដែលមិនចាំបាច់នៃអាសយដ្ឋានអាយភី (IP) របស់ម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នក ហើយត្រូវប្រាកដថា ការលាតត្រដាងជាសាធារណៈណាមួយត្រូវបានការពារពីការវាយប្រហារ DoS។

  - ជៀសវាងការប្រើអាសយដ្ឋានអាយភី សម្រាប់ម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នក ដែលតួអង្គព្យាបាទអាចទស្សន៍ទាយបាន ជាឧទាហរណ៍ អាសយដ្ឋានអាយភី នៅក្នុងបណ្តាញរងនៃបណ្តាញដូចគ្នានៃអាសយដ្ឋានអាយភីដែលបានបង្ហាញអាសយដ្ឋានអាយភី ជាសាធារណៈនៃសេវាកម្មអនឡាញរបស់អ្នក។
  - ប្រើការគ្រប់គ្រងការចូលប្រើបណ្តាញ (ដូចជា ជញ្ជាំងភ្លើង) ដើម្បីធានាថាមានតែ CDN និងបណ្តាញគ្រប់គ្រងដែលមានការអនុញ្ញាតពីស្ថាប័នរបស់អ្នកប៉ុណ្ណោះ ដែលអាចចូលប្រើម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នកបាន។
  - ពិចារណាប្រើការតភ្ជាប់បណ្តាញចម្រុះដែលធន់ ដែលអាចរួមបញ្ចូលការតភ្ជាប់បណ្តាញឯកជន រវាងម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នក និងអ្នកផ្តល់ CDN របស់អ្នក ប្រសិនបើអ្នកត្រូវការកម្រិតនៃការការពារខ្ពស់ជាងសម្រាប់ម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នក។
  - កំណត់រចនាសម្ព័ន្ធ CDN ម៉ាស៊ីនមេគេហទំព័រដើម និងចំណងជើង HTTP របស់អតិថិជន ដើម្បីកែលម្អចំនួននៃទិន្នន័យដែលបានរក្សាទុកជាបណ្តោះអាសន្ន។
  - ពិចារណាលើការបែងចែកម៉ាស៊ីនមេគេហទំព័រដើម ដើម្បីឱ្យសំណើពីអាសយដ្ឋានអាយភី ដែលមានហានិភ័យទាបត្រូវបានចាត់ចែងដោយឡែកពីគ្នា ដើម្បីស្នើពីអាសយដ្ឋានអាយភី ដែលមានហានិភ័យខ្ពស់ ប្រសិនបើអ្នកត្រូវការភាពអាចប្រើប្រាស់បានដែលមានកម្រិតខ្ពស់ជាង។
- កំណត់មុខងារ និងគុណភាពនៃសេវាកម្មណាដែលអាចទទួលយកបានសម្រាប់អ្នកប្រើប្រាស់ដែលត្រឹមត្រូវតាមច្បាប់នៃសេវាកម្មអនឡាញរបស់អ្នក របៀបរក្សាមុខងារនោះ និងមុខងារអ្វីដែលមិនត្រូវការក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS។
- ទិញ និងប្រើប្រាស់សេវាកម្មកាត់បន្ថយការវាយប្រហារ DoS ក្នុង cloud (ក្លៅ)។
- ពិចារណាកាត់បន្ថយចំណុចដែលជាគោលដៅវាយប្រហាររបស់ស្ថាប័នអ្នកដោយ៖
  - ការផ្តល់សេវាកម្មអនឡាញជាមូលដ្ឋាន (ដូចជា DNS) ទៅកាន់អ្នកផ្តល់សេវាកម្មល្បីឈ្មោះពីក្រៅនានា ដែលអាចទប់ទល់នឹងការវាយប្រហារ DoS
  - ការបែងចែកសេវាកម្មអនឡាញសំខាន់ៗ (ដូចជាអ៊ីមែល) ពីសេវាកម្មអនឡាញផ្សេងទៀតដែលទំនងជាគោលដៅនៃការវាយប្រហារ (ដូចជាគេហទំព័រនានា)
  - ធានាថាសេវាកម្មកាត់បន្ថយការវាយប្រហារ DoS អនុញ្ញាតតែចរាចរបណ្តាញណាដែលភ្ជាប់ជាមួយច្រកបណ្តាញរបស់សេវាកម្មអនឡាញប៉ុណ្ណោះ។
- ពិភាក្សាជាមួយអ្នកផ្តល់សេវាកម្មរបស់អ្នក អំពីព័ត៌មានលម្អិតនៃយុទ្ធសាស្ត្រការពារ និងកាត់បន្ថយការវាយប្រហារ DoS របស់ពួកគេ ជាពិសេស៖
  - សមត្ថភាពពិតប្រាកដដើម្បីទប់ទល់នឹងការវាយប្រហារ DoS ពីជុំវិញពិភពលោក
  - ប្រវត្តិដែលបានបង្ហាញអំពីការគ្រប់គ្រងទាំងការវាយប្រហារ DoS និងការធ្វើតេស្តលើការវាយប្រហារ DoS ដែលបានអនុញ្ញាតយ៉ាងទូលំទូលាយ
  - សមត្ថភាពក្នុងការកាត់បន្ថយប្រភេទនៃការវាយប្រហារ DoS ភាគច្រើនដោយស្វ័យប្រវត្តិ ដោយមិនមានការពាក់ព័ន្ធរបស់មនុស្ស ដូចជាការវិភាគដោយដៃនៃចរាចរបណ្តាញ
  - វិធីសាស្ត្រក្នុងការកំណត់តម្លៃសេវាកម្មរបស់ពួកគេ ដូចជាថាតើវាជាតម្លៃថេរ ឬប្រែប្រួលអាស្រ័យលើបរិមាណនៃចរាចរបណ្តាញ និងធនធានដំណើរការកុំព្យូទ័រដែលបានប្រើ និងថាតើអ្នកអាចកំណត់ដែននៃការចំណាយបានដែរឬអត់
  - កម្រិតនៃការជូនដំណឹងដល់អ្នក ឬការបិទសេវាកម្មអនឡាញរបស់ពួកគេ ក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS
  - សកម្មភាពដែលបានអនុម័តជាមុន ដែលអាចអនុវត្តក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS
  - ការរៀបចំការទប់ស្កាត់ការវាយប្រហារ DoS ជាមួយអ្នកផ្តល់សេវាកម្មដើមនានា។
- អនុវត្តវិធានការដើម្បីស្វែងរកការវាយប្រហារ DoS ដូចជាការត្រួតពិនិត្យជាបន្តតាមពេលវេលាជាក់ស្តែង និងការជូនដំណឹងអំពីភាពអាចប្រើប្រាស់បាននៃប្រព័ន្ធ ចរាចរបណ្តាញ ធនធានដំណើរការកុំព្យូទ័រ និងការចំណាយពាក់ព័ន្ធនានា។
- រៀបចំកំណែឋិតិវន្តនៃគេហទំព័ររបស់អ្នក ដែលតម្រូវឱ្យមានដំណើរការតិចតួចបំផុត និងកម្រិតបញ្ជូនទិន្នន័យដើម្បីជួយសម្រួលដល់ការបន្តនៃសេវាកម្មក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS។
- ទិញ និងប្រើប្រាស់សេវាកម្មអនឡាញនានាដែលមានភាពធន់ខ្ពស់ ជាមួយនឹងកម្រិតបញ្ជូនទិន្នន័យធំ ធនធានដំណើរការកុំព្យូទ័រគ្រប់គ្រាន់ ទីតាំងបង្ហោះដែលរាយតាមភូមិសាស្ត្រ និងការសម្អាតចរាចរក្នុង cloud ដើម្បីបញ្ឈប់ចរាចរបណ្តាញដែលមិនចង់បាន - ជាទូទៅ វារួមបញ្ចូលការប្រើប្រាស់ CDN ល្បីឈ្មោះ ដើម្បីរក្សាទុកមាតិកានៅលើគេហទំព័រឋិតិវន្ត និងការពារម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នក ពីចរាចរបណ្តាញដែលមិនចង់បាន។

- ការពារឈ្មោះដែនអាសយដ្ឋានបណ្តាញរបស់ស្ថាប័នអ្នក ដោយប្រើការចាក់សោរបស់អ្នកគ្រប់គ្រងបញ្ជី ការបញ្ជាក់ព័ត៌មានទំនាក់ទំនងលម្អិតនៃការចុះឈ្មោះដែនអាសយដ្ឋានបណ្តាញ និងព័ត៌មានលម្អិតផ្សេងទៀតថាត្រឹមត្រូវ ហើយធ្វើតាមការណែនាំបន្ថែមដូចបានរៀបរាប់នៅក្នុងឯកសារបោះពុម្ពផ្សាយ*[សន្តិសុខប្រព័ន្ធឈ្មោះដែនអាសយដ្ឋានបណ្តាញសម្រាប់ម្ចាស់ដែនអាសយដ្ឋានបណ្តាញ](#)* របស់ ASD។
- រក្សាព័ត៌មានទំនាក់ទំនងថ្មីៗសម្រាប់អ្នកផ្តល់សេវាកម្មរបស់អ្នក និងចែករំលែកព័ត៌មានទំនាក់ទំនងលម្អិតរបស់ស្ថាប័នអ្នកជាមួយពួកគេ ដោយធានាថា ទំនាក់ទំនងទាំងអស់អាចរកបានដោយផ្អែកលើតម្រូវការរបស់ស្ថាប័នអ្នក ជាឧទាហរណ៍ 24 ម៉ោងក្នុងមួយថ្ងៃ 7 ថ្ងៃក្នុងមួយសប្តាហ៍។
- ផ្តល់ព័ត៌មានទំនាក់ទំនងក្រៅបណ្តាញរបស់ស្ថាប័នអ្នក សម្រាប់បណ្តាញទំនាក់ទំនងដែលគួរឱ្យទុកចិត្ត ដល់អ្នកផ្តល់សេវាកម្មនានារបស់អ្នក សម្រាប់ពេលដែលបណ្តាញទំនាក់ទំនងធម្មតាមិនដំណើរការ។
- បង្កើត អនុវត្ត និងរក្សាផែនការឆ្លើយតបឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត ដែលគ្របដណ្តប់ប្រភេទផ្សេងៗនៃការវាយប្រហារ DoS ប្រឆាំងនឹងសេវាកម្មអនឡាញនីមួយៗរបស់អ្នក ដែលត្រូវការដើម្បីទប់ទល់នឹងការវាយប្រហារ DoS និងអនុវត្តផែនការនេះយ៉ាងហោចណាស់ជារៀងរាល់ឆ្នាំ។
- រចនាកម្មវិធីនានាដើម្បីការពារមុខងារដែលត្រូវបានរំលោភបំពានជាទូទៅ ដែលប្រើប្រាស់ធនធានដំណើរការកុំព្យូទ័រកើនឡើង ឬដែលទទួលរងការចំណាយហិរញ្ញវត្ថុបន្ថែម (ដូចជាការផ្ញើសារ SMS)។
  - ការការពាររួមមានការកំណត់កម្រិត និងការផ្ទៀងផ្ទាត់ថាសំណើនានាគឺមកពីមនុស្ស។
  - អនុវត្តការធ្វើតេស្តលើការវាយប្រហារ DoS រួមទាំងការកំណត់គោលដៅលំហូរឡូស៊ីកមិនត្រឹមត្រូវនៅក្នុងមុខងារកម្មវិធី។
  - អនុវត្តការធ្វើតេស្តបន្ទុកកាន់តែទូលំទូលាយដើម្បីកំណត់អត្តសញ្ញាណ និងជួសជុលវ៉ិចទ័រ (vector) DoS។

ឆ្លើយតបទៅនឹងការវាយប្រហារ DoS

ប្រសិនបើស្ថាប័នរបស់អ្នកមិនបានប្រុងប្រៀបសម្រាប់ការវាយប្រហារ DoS ទេ អ្នកអាចព្យាយាមអនុវត្តវិធានការខាងលើមួយចំនួនក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS ថ្វីបើវាអាចមិនសូវមានប្រសិទ្ធភាព ហើយចំណាយពេលក្នុងការអនុវត្តដោយកាត់បន្ថយសមត្ថភាពឆ្លើយតបរបស់ស្ថាប័នរបស់អ្នកក៏ដោយ។

ស្ថាប័នរបស់អ្នកគួរតែអនុវត្តវិធានការនានាខាងក្រោមក្នុងអំឡុងពេលនៃការវាយប្រហារ DoS នៅពេលសមស្រប និងជាក់ស្តែង។

- អនុវត្តផែនការឆ្លើយតបឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិតរបស់អ្នក។
- សួរអ្នកផ្តល់សេវាកម្មរបស់អ្នក ថាតើពួកគេអាចអនុវត្តសកម្មភាពឆ្លើយតបភ្លាមៗបានឬអត់ - ប្រសិនបើអ្នកមិនបានពិភាក្សាពីសមត្ថភាពរបស់ពួកគេក្នុងការឆ្លើយតបពីមុនទេ អ្នកអាចរកឃើញថាពួកគេមិនអាច ឬមិនចង់ឆ្លើយតប ឬគិតថ្លៃបន្ថែម។
- បិទមុខងារមិនសំខាន់ ឬលុបមាតិកាមិនសំខាន់ចេញពីសេវាកម្មអនឡាញរបស់អ្នក ដែលធ្វើឱ្យការវាយប្រហារ DoS បច្ចុប្បន្នមានប្រសិទ្ធភាព ជាឧទាហរណ៍ ដាក់ពង្រាយកំណែគេហទំព័ររបស់អ្នកដោយគ្មានមុខងារស្វែងរក មាតិកាថាមវន្ត ឬឯកសារធំៗ។
- រក្សាការប្រាស្រ័យទាក់ទងជាមួយអតិថិជនរបស់អ្នក និងអ្នកផ្តល់សេវាកម្មនានារបស់អ្នក រួមទាំងអ្នកផ្តល់សេវាកម្មកាត់បន្ថយការវាយប្រហារ DoS របស់អ្នក និងបន្តតាមដានភាពអាចប្រើប្រាស់បាននៃសេវាកម្មអនឡាញរបស់អ្នក។
- ពិចារណាផ្លាស់ប្តូរអាសយដ្ឋានអាយភី នៃម៉ាស៊ីនមេគេហទំព័រដើមរបស់អ្នក ប្រសិនបើវាក្លាយជាគោលដៅវាយប្រហារដោយផ្ទាល់ និងជៀសវាងការបង្ហាញជាសាធារណៈនៃអាសយដ្ឋានអាយភីថ្មី ដោយមិនមានការការពារដាក់ឱ្យដំណើរការ។
- រាយការណ៍ពីការវាយប្រហារ DoS ទៅភាគីពាក់ព័ន្ធនានា រួមទាំង ASD និង NCSC-NZ តាមផ្នែក 'ព័ត៌មានទំនាក់ទំនង' នៃឯកសារបោះពុម្ពផ្សាយនេះ។

ជៀសវាងការរួមចំណែកដល់ការវាយប្រហារ DoS

ស្ថាប័នរបស់អ្នកគួរអនុវត្តវិធានការនានាខាងក្រោម ដើម្បីជៀសវាងការរួមចំណែកដោយអចេតនាចំពោះការវាយប្រហារ DoS ដែលអាចប៉ះពាល់ដល់អ្នកដទៃ។

- ជៀសវាងការលាតត្រដាងសេវាកម្មនានា ឧបករណ៍ IoT និងឧបករណ៍ដែលភ្ជាប់អ៊ីនធឺណិតផ្សេងទៀតទៅកាន់អ៊ីនធឺណិតដែលមិនត្រូវការ កំណត់រចនាសម្ព័ន្ធមិនមានសុវត្ថិភាព ឬការថែទាំមិនគ្រប់គ្រាន់។
- កំណត់រចនាសម្ព័ន្ធ ថែទាំ និងត្រួតពិនិត្យដោយសុវត្ថិភាពនូវសេវាកម្ម ឧបករណ៍ IoT និងឧបករណ៍ភ្ជាប់អ៊ីនធឺណិតផ្សេងទៀត ដែលលាតត្រដាងបង្ហាញឱ្យឃើញតាមអ៊ីនធឺណិត។
  - ការណែនាំបន្ថែមសម្រាប់អាជីវកម្មខ្នាតតូចមាននៅក្នុងឯកសារបោះពុម្ពផ្សាយរបស់ ASD ស្តីពី *ឧបករណ៍នានាដែលភ្ជាប់តាមប្រព័ន្ធអ៊ីនធឺណិត* និង *រក្សាសុវត្ថិភាព Wi-Fi និងរ៉ោទ័ររបស់អ្នក* ។

ប្រសិនបើស្ថាប័នរបស់អ្នកកំពុងដំណើរការសេវាកម្មអនឡាញ អ្នកគួរតែអនុវត្តវិធានការបន្ថែមខាងក្រោម។

- ផ្តល់អាទិភាពដល់ការពិនិត្យឡើងវិញនូវពិធីការដែលមានចែងនៅក្នុងទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិត និងសន្តិសុខនៃហេដ្ឋារចនាសម្ព័ន្ធ (CISA) របស់សហរដ្ឋអាមេរិក *ដំបូន្មានអំពី* ការពង្រឹកការវាយប្រហារទៅលើពិធីការផ្ទុកក្រុមទិន្នន័យរបស់អ្នកប្រើប្រាស់ (UDP)។
- ត្រួតពិនិត្យមើលវិចន័រពង្រឹកថ្មី ដោយសារវាត្រូវបានកំណត់អត្តសញ្ញាណ និងការពារសន្តិសុខសេវាកម្មអនឡាញរបស់អ្នកប្រឆាំងនឹងការវាយប្រហារទាំងនេះ។
- កំណត់រចនាសម្ព័ន្ធការគ្រប់គ្រងការចូលប្រើបណ្តាញទាំងពីខាងក្នុង និងពីខាងក្រៅ ដើម្បីកំណត់ការចូលប្រើសេវាកម្ម និងស្ថាប័នអនឡាញដែលមានការអនុញ្ញាត។
- ទប់ស្កាត់ការចូលប្រើជាសាធារណៈអនាមិក សម្រាប់សេវាកម្មអនឡាញដែលងាយនឹងពង្រឹក ប្រសិនបើមិនចាំបាច់។
- ពិចារណាអនុវត្តយន្តការកំណត់កម្រិត ដើម្បីកាត់បន្ថយផលវិបាកនានានៃការប្រើប្រាស់ខុស ប្រសិនបើការទប់ស្កាត់ ឬអនុវត្តការគ្រប់គ្រងការចូលប្រើមិនអាចធ្វើទៅបាន ឬសមស្រប។

ព័ត៌មានបន្ថែម

សៀវភៅណែនាំសន្តិសុខព័ត៌មាន របស់ ASD គឺជាក្របខ័ណ្ឌសន្តិសុខអ៊ីនធឺណិត ដែលស្ថាប័នអាចអនុវត្តដើម្បីការពារប្រព័ន្ធ និងទិន្នន័យរបស់ពួកគេពីការគំរាមកំហែងតាមអ៊ីនធឺណិត។ ដំបូន្មាននៅក្នុង *យុទ្ធសាស្ត្រកាត់បន្ថយឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត* រួមជាមួយនឹងយុទ្ធសាស្ត្រការពារសន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិតសំខាន់ទាំងប្រាំបី (Essential Eight) បំពេញបន្ថែមលើក្របខ័ណ្ឌនេះ។

សៀវភៅណែនាំសន្តិសុខព័ត៌មានរបស់ប្រទេសនូវែលសេឡង់ គឺជាសៀវភៅណែនាំរបស់រដ្ឋាភិបាលនូវែលសេឡង់ ស្តីពីការធានាព័ត៌មាន និងសន្តិសុខប្រព័ន្ធព័ត៌មាន។ វាគឺជាសៀវភៅណែនាំរបស់អ្នកអនុវត្តដែលបានរចនាឡើង ដើម្បីបំពេញតម្រូវការរបស់អ្នកគ្រប់គ្រងសន្តិសុខព័ត៌មានរបស់ភ្នាក់ងារ ក៏ដូចជាអ្នកលក់ អ្នកម៉ៅការ និងអ្នកប្រឹក្សាដែលផ្តល់សេវាកម្មដល់ទីភ្នាក់ងារនានា។

ព័ត៌មានបន្ថែមអំពីប្រភេទផ្សេងៗនៃការវាយប្រហារ DoS មាននៅក្នុងឯកសារបោះពុម្ពផ្សាយ *ការណែនាំសង្ខេបខ្លីៗ (Quick Guide) ស្តីពី DDoS* របស់ CISA និង *ការយល់ដឹង និងការឆ្លើយតបចំពោះការវាយប្រហារ DoS បែងចែកជាច្រើនមុខសញ្ញា*។

ព័ត៌មានទំនាក់ទំនង

នៅប្រទេសអូស្ត្រាលី ប្រសិនបើអ្នកមានសំណួរណាមួយអំពីការណែនាំនេះ *សូមសរសេរទៅ ASD* ឬទូរសព្ទទៅលេខ 1300 CYBER1 (1300 292 371)។

នៅប្រទេសនូវែលសេឡង់ ដើម្បីរាយការណ៍អំពីឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត សូមអ៊ីម៉ែលទៅ incidents@ncsc.govt.nz ឬចូលទៅកាន់គេហទំព័ររបស់ NCSC-NZស្តីពី *រាយការណ៍អំពីឧប្បត្តិហេតុ*។

ការបដិសេធទំនួលខុសត្រូវ

សម្ភារនៅក្នុងសៀវភៅណែនាំនេះគឺមានលក្ខណៈជាទូទៅ ហើយមិនគួរចាត់ទុកថាជាដំបូន្មានផ្នែកច្បាប់ ឬការពឹងផ្អែកសម្រាប់ជាជំនួយក្នុងកាលៈទេសៈជាក់លាក់ណាមួយ ឬក្នុងស្ថានភាពសង្គ្រោះបន្ទាន់ឡើយ។ ក្នុងបញ្ហាសំខាន់ណាមួយ អ្នកគួរតែស្វែងរកដំបូន្មានដែលមានជំនាញវិជ្ជាជីវៈឯករាជ្យសមស្រប ទាក់ទងនឹងកាលៈទេសៈផ្ទាល់ខ្លួនរបស់អ្នក។

Commonwealth (ខុម្មុនវែល) មិនទទួលយកការទទួលខុសត្រូវ ឬបំណុលចំពោះការខូចខាត ការបាត់បង់ ឬការចំណាយណាមួយបណ្តាលមកពីការពឹងផ្អែកលើព័ត៌មានដែលមាននៅក្នុងសៀវភៅណែនាំនេះឡើយ។

រក្សាសិទ្ធិ

ការប្រើប្រាស់សញ្ញាជាតិ

លក្ខខណ្ឌនានាដែលសញ្ញាជាតិអាចត្រូវបានប្រើ គឺរៀបរាប់ជាលម្អិតនៅលើគេហទំព័ររបស់ក្រសួងនាយករដ្ឋមន្ត្រី និងគណៈរដ្ឋមន្ត្រីស្តីពី ព័ត៌មាន និងគោលការណ៍ណែនាំរបស់ Commonwealth Coat of Arms | pmc.gov.au។

សម្រាប់ព័ត៌មានបន្ថែម ឬដើម្បីរាយការណ៍អំពីឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត សូមទាក់ទងមកយើង៖

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

លេខនេះអាចប្រើបានតែក្នុងប្រទេសអូស្ត្រាលីប៉ុណ្ណោះ។

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre