សន្លឹកព័ត៌មាន៖

ការណែនាំអំពី សាធារណរដ្ឋ ប្រជាធិបតេយ្យ ប្រជាមានិត្យ កូរ៉េ បុគ្គលិក បច្ចេកវិទ្យា ពត៌មាន

ថ្ងៃទី 16 ខែឧសភា ឆ្នាំ 2022

រដ្ឋាភិបាលសហរដ្ឋអាមេរិក រដ្ឋាភិបាលកំពុងចេញ [សេចក្តីជូនដំណឹង](#)
នេះជាធនធានដ៏ទូលំទូលាយសម្រាប់សហគមន៍អន្តរជាតិ វិស័យឯកជន
និងសាធារណៈជនឱ្យល់កាន់តែច្បាស់ និងការពារប្រឆាំងនឹងការជ្រើសរើសដ៏ខ្ជីខ្ជា ការជួល
និងការសម្របសម្រួលរបស់បុគ្គលិកពត៌មានវិទ្យា (IT) សាធារណរដ្ឋប្រជាធិបតេយ្យប្រជាមានិតកូរ៉េ (DPRK, a.k.a. កូរ៉េខាងជើង) ។ សេចក្តីជូនដំណឹងនេះផ្តល់នូវព័ត៌មានលម្អិតអំពីរបៀបដែលបុគ្គលិក IT
របស់កូរ៉េខាងជើង (DPRK) ធ្វើប្រតិបត្តិការ និងកំណត់សូចនាករទង់ក្រហម
និងវិធានការប្រុងប្រយ័ត្នដ៏ត្រឹមត្រូវដើម្បីជួយបណ្តាក្រុមហ៊ុនឲ្យជៀសផុតពីការជួលអ្នកអភិវឌ្ឍន៍កម្មវិធីឯក
រាជ្យរបស់កូរ៉េខាងជើង និងដើម្បីជួយវេទិកាទូទាត់ឯករាជ្យ និងបែបឌីជីថលកំណត់អត្តសញ្ញាណបុគ្គលិក IT
កូរ៉េខាងជើងដែលបំពានសេវាកម្មរបស់ពួកគេ។ ការជួល ឬគាំទ្រសកម្មភាពនៃបុគ្គលិក IT
របស់កូរ៉េខាងជើង បង្កហានិភ័យជាច្រើន រាប់ចាប់ពីការលួចកម្មសិទ្ធិបញ្ញា ទិន្នន័យ និងមូលនិធិ
រហូតដល់ខូចខាតកេរ្តិ៍ឈ្មោះ និងផលវិបាកផ្នែកច្បាប់
រួមទាំងការដាក់ទណ្ឌកម្មនៅក្រោមអាជ្ញាធរសហរដ្ឋអាមេរិក និងអង្គការសហប្រជាជាតិ (UN)។

កូរ៉េខាងជើងបានបញ្ជូនបុគ្គលិកពត៌មានវិទ្យា ដែលមានជំនាញខ្ពស់រាប់ពាន់នាក់នៅជុំវិញពិភពលោក
ដោយទទួលបានប្រាក់ចំណូលសម្រាប់កូរ៉េខាងជើង ដែលរួមចំណែកដល់កម្មវិធីអាវុធរបស់ខ្លួន
ក្នុងការរំលោភបំពានលើទណ្ឌកម្មរបស់សហរដ្ឋអាមេរិក និងអង្គការសហប្រជាជាតិ។ បុគ្គលិកទាំងនេះ៖

- រំលោភបំពានប្រព័ន្ធអេកូឡូស៊ីទាំងស្រុងនៃវេទិកាការងារឯករាជ្យ
  ដើម្បីទទួលបានកិច្ចសន្យាអភិវឌ្ឍន៍ពត៌មានវិទ្យា
  ពីបណ្តាក្រុមហ៊ុនដែលជាអតិថិជនជុំវិញពិភពលោកដោយលួចលាក់
  រួមទាំងរំលោភបំពានលើវេទិកាប្រព័ន្ធផ្សព្វផ្សាយសង្គមជាច្រើនផងដែរ
  ដើម្បីទាក់ទងជាមួយអតិថិជន
  និងប្រព័ន្ធទូទាត់ប្រាក់ដើម្បីទទួលបានការទូទាត់សម្រាប់ការងាររបស់ពួកគេ។
- បង្កើតកម្មវិធី និងសូហ្វវែរដែលគ្របដណ្តប់លើវិស័យជាច្រើន រួមមាន
  ប៉ុន្តែមិនកំណត់ចំពោះអាជីវកម្ម រូបិយប័ណ្ណគ្រីបតូ សុខភាព និងកាយសម្បទា
  បណ្តាញទំនាក់ទំនងសង្គម កីឡា ការកម្សាន្ត និងរបៀបរស់នៅ។
- ក្នុងករណីជាច្រើនតែងបន្លំខ្លួនជាបុគ្គលិកទូរគមនាគមន៍បរទេស (មិនមែនកូរ៉េខាងជើង) ឬ
  បុគ្គលិកទូរគមនាគមន៍ដែលមានមូលដ្ឋាននៅសហរដ្ឋអាមេរិក រួមមានដោយការប្រើប្រាស់បណ្តាញ
  ឯកជននិម្មិត (VPNs) ម៉ាស៊ីនមេឯកជននិម្មិត (VPS) ដែលបានទិញអាសយដ្ឋាន IP ប្រទេសទីបី
  គណនីប្រូកស៊ី និងតែងបន្លំ ឬលួចឯកសារអត្តសញ្ញាណ; និង
- ប្រើប្រាសសិទ្ធចូលប្រើប្រាស់ពិសេសដែលទទួលបានជាអ្នកដេញថ្លៃក្នុងគោលបំណងខុសច្បាប់|
  រួមទាំងអនុញ្ញាតឲ្យមានការរំលោភបំពានតាមអ៊ីនធឺណិតដ៏គ្រោះថ្នាក់ដោយអ្នកចូលរួមកូរ៉េខាងជើ
  ងផ្សេងៗទៀត។

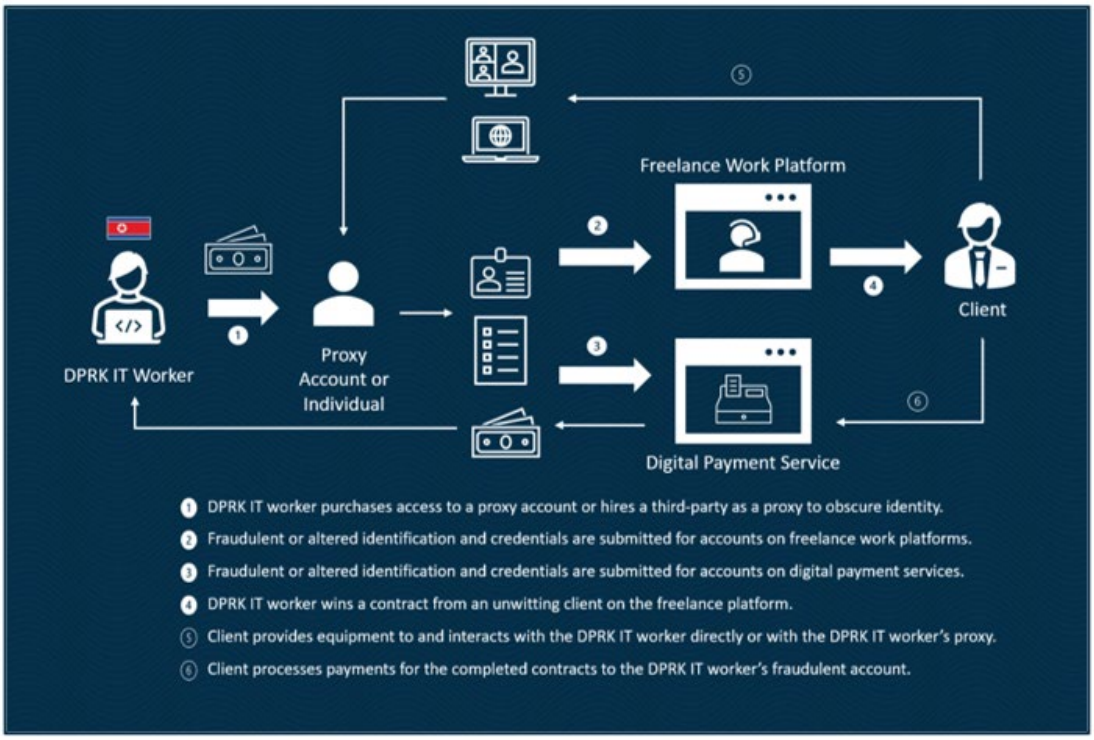
សញ្ញាបង្ហាញទង់ក្រហមនៃសកម្មភាពបុគ្គលិកពត៌មានវិទ្យារបស់កូរ៉ែខាងជើងដែលមានសក្តានុពលរួមមាន៖

- ការឡុកចូលច្រើនដងទៅក្នុងគណនីតែមួយពីអាសយដ្ឋាន IP ផ្សេងៗក្នុងរយៈពេលដ៏ខ្លី ជាពិសេសប្រសិនបើអាសយដ្ឋាន IP ត្រូវបានភ្ជាប់ជាមួយប្រទេសផ្សេងៗគ្នា។
- ការផ្ទេរប្រាក់ជាញឹកញាប់តាមរយៈប្រព័ន្ធទូទាត់ប្រាក់ ជាពិសេសទៅកាន់គណនីធនាគារដែលមានមូលដ្ឋាននៅសាធារណរដ្ឋប្រជាមានិតចិន (PRC) ឬសំណើសុំការទូទាត់ជារូបិយប័ណ្ណគ្រីបតូ។
- ភាពផ្ទុយគ្នានៃការប្រកបឈ្មោះ សញ្ជាតិ ទីកន្លែងការងារដែលត្រូវបានបង្ហាញ ព័ត៌មានទំនាក់ទំនង ប្រវត្តិអប់រំ ប្រវត្តិការងារ និងព័ត៌មានលម្អិតផ្សេងៗទៀតដុំវិញសំណុំព័ត៌មានកម្មវិធីឯករាជ្យរបស់អ្នកអភិវឌ្ឍន៍កម្មវិធី សំណុំព័ត៌មានផ្សព្វផ្សាយសង្គម គេហទំព័រផលប័ត្រខាងក្រៅ សំណុំពត៌មានកម្មវិធីទូទាត់ប្រាក់ និងទីតាំង និងម៉ោងដែលត្រូវបានចូលប្រើប្រាស់ និង
- អសមត្ថភាពក្នុងការធ្វើកិច្ចការក្នុងកំឡុងពេលម៉ោងធ្វើការ និងអសមត្ថភាពក្នុងការទាក់ទងបុគ្គលិកទាន់ពេលវេលា ជាពិសេសតាមរយៈវិធីសាស្ត្រទំនាក់ទំនង "ភ្លាមៗ"។

វិធានការប្រុងប្រយ័ត្នត្រឹមត្រូវដែលវិស័យឯកជនអាចពិចារណាដើម្បីបង្ការការជួលបុគ្គលិក IT របស់កូរ៉ែខាងជើងដោយខ្ជីខ្ជា ឬដោយមិនស្គាល់ច្បាស់ រួមមាន៖

- ផ្ទៀងផ្ទាត់ឯកសារដែលបានដាក់ស្នើជាផ្នែកនៃការពិនិត្យសំណើ ឬការដាក់ពាក្យសុំការងារដោយផ្ទាល់ជាមួយបណ្តាក្រុមហ៊ុននិងស្ថាប័នអប់រំដែលបានចុះបញ្ជី (មិនប្រើប្រាស់ព័ត៌មានទំនាក់ទំនងដែលត្រូវបានផ្តល់នៅលើឯកសារដែលបានដាក់ស្នើ);
- ពិនិត្យឲ្យបានដិតដល់នូវឯកសារបញ្ជាក់អត្តសញ្ញាណដែលបានដាក់ស្នើសម្រាប់ការត្រួតបន្ទុំ;
- ធ្វើការសម្ភាសន៍ជាវីដេអូ ដើម្បីផ្ទៀងផ្ទាត់អត្តសញ្ញាណរបស់បុគ្គលិកធ្វើការឯករាជ្យដែលមានសក្តានុពល។
- ធ្វើការត្រួតពិនិត្យប្រវត្តិការងារពីមុននិង/ឬការឡុកចូលដោយប្រើខ្ចៅដៃ/ទិន្នន័យឌីជីថល ដើម្បីផ្ទៀងផ្ទាត់អត្តសញ្ញាណ និងទីតាំងដែលត្រូវបានបង្ហាញ។
- ជៀសវាងការទូទាត់ជារូបិយប័ណ្ណគ្រីបតូ និងទាមទារឲ្យមានការផ្ទៀងផ្ទាត់ព័ត៌មានធនាគារដែលឆ្លើយតបទៅនឹងឯកសារកំណត់អត្តសញ្ញាណផ្សេងៗទៀត;
- ពិនិត្យមើលការប្រកបឈ្មោះ សញ្ជាតិ ទីតាំងដែលត្រូវបានបង្ហាញ ព័ត៌មានទំនាក់ទំនង ប្រវត្តិអប់រំ ប្រវត្តិការងារ និងព័ត៌មានលម្អិតផ្សេងទៀតនៃការជួលដែលអាចកើតមានគឺត្រូវគ្នាជុំវិញសំណុំពត៌មានកម្មវិធីឯករាជ្យរបស់អ្នកអភិវឌ្ឍន៍កម្មវិធី សំណុំពត៌មានប្រព័ន្ធផ្សព្វផ្សាយសង្គម គេហទំព័រផលប័ត្រខាងក្រៅ គណនីនៃប្រព័ន្ធទូទាត់ប្រាក់ និងទីតាំង និងម៉ោងដែលបានត្រូវបានចូលប្រើប្រាស់និង
- មានការសង្ស័យប្រសិនបើអ្នកអភិវឌ្ឍន៍កម្មវិធីមិនអាចទទួលបានព័ត៌មាននៅអាសយដ្ឋានស្តីពីឯកសារអត្តសញ្ញាណរបស់ពួកគេ។

ទិដ្ឋភាពទូទៅនៃការប្រតិបត្តិការបុគ្គលិក IT របស់កូរ៉េខាងជើង



*សម្រាប់ព័ត៌មានបន្ថែម សូមមើល **សេចក្តីជូនដំណឹងតាមអ៊ីនធឺណិតរបស់កូរ៉េខាងជើង**, សូមចូលទៅកាន់ **មជ្ឈមណ្ឌលធនធានរតនាគារ**, និង/ឬទាក់ទង **ការិយាល័យ FBI ក្នុងតំបន់** របស់អ្នក។*
ប្រសិនបើអ្នកមានព័ត៌មានអំពីសកម្មភាពកូរ៉េខាងជើងខុសច្បាប់ក្នុងបរិបទទំនាក់ទំនងតាមអ៊ីនធឺណិត រួមទាំងការធ្វើប្រតិបត្តិការកន្លងមក ឬដែលកំពុងដំណើរការ
អ្នកអាចមានសិទ្ធិទទួលបានរង្វាន់រហូតដល់ $5 លានដុល្លារ
*ដោយផ្តល់ព័ត៌មានបែបនេះតាមរយៈក្រសួងនៃកម្មវិធី **រង្វាន់សម្រាប់យុត្តិធម៌** របស់រដ្ឋ។*