ឯកសារសៀបរាប់សង្ខេបពី ក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋឈ្មោះ APT32

១. សេចក្តីផ្តើម

ការរីកចំរើននៃសេដ្ឋកិច្ចជាតិក្នុងរយៈពេល២០ឆ្នាំចុងក្រោយមុនជំងឺរាតត្បាតកូវីដ១៩បានចូលមកដល់ បានធ្វើប្រទេសកម្ពុជាក្លាយទៅកូននាគសេដ្ឋកិច្ចប្រចាំនៅតំបន់អាស៊ានដែលមានការរីកចំរើនសឹងតែគ្រប់វិស័យទាំងអស់ ។ ការរីករាលដាលនៃជំងឺកូវីដ-១៩បានផ្តល់ផលប៉ះពាល់យ៉ាងខ្លាំងដល់កំណើនសេដ្ឋកិច្ច ហើយថែមទាំងឆក់យកជីវិតប្រជាជនទៀតផង ។ ទន្ទឹមនឹងកត្តាអកុសលនៃជំងឺកូវីដ-១៩ ប្រទេសជាច្រើននៅក្នុងសកលលោកបានទទួលយកការប្រើប្រាស់បច្ចេកវិទ្យាយ៉ាងឆាប់រហ័សស្ទើរស្មានមិនដល់ រាជរដ្ឋាភិបាលកម្ពុជាក៏មិនខុសពីប្រទេសដ៏ទៃទៀតដែរ បានចាប់យកការប្រើប្រាស់បច្ចេកវិទ្យា និងបានសម្លឹងមើលឃើញកាលានុវត្តភាព និងវិសាលភាពនៃផលប្រយោជន៍សេដ្ឋកិច្ចក្នុងវិស័យឌីជីថលសម្រាប់ជម្រុញកំណើនសេដ្ឋកិច្ចបែបថ្មី និងជម្រុញ កំណើនផលិតភាពនៃវិស័យផ្សេងទៀត ។ រាជរដ្ឋាភិបាលកម្ពុជាបានដាក់ចេញនូវចក្ខុវិស័យវិស័យវែងឆ្ងាយក្នុងការកសាងសេដ្ឋកិច្ច និងសង្គមឌីជីថលផ្អែកតាមបរិការណ៍ "***ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា ២០២១-២០៣៥***" (១) ដើម្បីទទួលយក ផលប្រយោជន៍ជាអតិបរមាពីការរីកចម្រើននៃបច្ចេកវិទ្យាទូរគមនាគមន៍ និងព័ត៌មាន និងបច្ចេកវិទ្យា ឌីជីថល ប្រកបដោយបរិយាប័ន្ន ភាពជឿទុកចិត្ត និងសុវត្ថិភាពខ្ពស់ ព្រមទាំងរក្សានូវអត្តសញ្ញាណ និងវប្បធម៌ជាតិ ។ ដើម្បីធានាអោយបាននូវ "***បរិវត្តកម្មឌីជីថល***" រាជរដ្ឋាភិបាលត្រូវជម្រុញអោយខ្ពស់បំផុតនូវកិច្ចការសម្របសម្រួល និងពង្រឹងកិច្ចសហប្រតិបត្តិការអន្តរស្ថាប័ន រវាងក្រសួង-ស្ថាប័នជាធ្លុងមួយក្នុងស្មារតីបុរេសកម្ម និងអន្តរសកម្ម ។

ក្នុងរយៈពេលប៉ុន្មានឆ្នាំចុងក្រោយ ប្រទេសកម្ពុជាបានក្លាយជាទីតាំងប្រឈមនឹងភូមិសាស្ត្រនយោបាយរវាងមហាអំណាច ដោយសារភាពស្និតរមួត និងគាំទ្រគោលនយោបាយចិនតែមួយបានធ្វើអោយប្រទេសមួយចំនួននៅក្នុងតំបន់អាស៊ានដែលមាននិន្នាការប្រឆាំងនឹងចិនហាក់មិនសូវសប្បាយចិត្តនឹងប្រទេសកម្ពុជា ជាពិសេសប្រទេសវៀតណាមដែលប្រឈមជាមួយប្រទេសចិនរឿងនៅសមុទ្រចិនខាងត្បូង ។ ការលើកឡើងបែបនេះទាក់ទិននឹងប្រទេសវៀតណាម ដោយឃើញនូវការកើតឡើងនូវក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋនៅឆ្នាំ២០១៧ស្របពេលទៅនឹងកិច្ចប្រជុំកំពូលអាស៊ាននៅឆ្នាំ២០១៧ នៅប្រទេសហ្វីលីពីន ក្នុងគោលបំណងវាយប្រហារទៅលើវិបសាយស្ថាប័នរដ្ឋាភិបាលកម្ពុជា ប្រជាមានិតឡាវ និងប្រទេសហ្វីលីពីន [1] ។ ចំណុចនេះនឹងពិភាក្សាលម្អិតទៅលើចំណុចទី៣ នៃអត្ថបទនេះ ដោយក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋឈ្មោះ APT32 មានទំនាក់ទំនងជាមួយរដ្ឋាភិបាលវៀតណាម [2] និងត្រូវបានគេជឿជាក់ថាគោលដៅប្រតិបត្តិការរបស់ក្រុមនេះគឺស្របទៅនឹងទិសដៅរបស់រដ្ឋាភិបាលវៀតណាម [3] ។ នៅក្នុងឆ្នាំ២០១៧ដដែលនោះ គេក៏កត់សំគាល់ឃើញប្រទេសវៀតណាមបានបង្កើនសមត្ថភាពលើវិស័យសាយប័រផងដែរ [1] ។

ដូចនេះយើងត្រូវចោទសួរថា តើរដ្ឋាភិបាលកម្ពុជាគួរតែស្វែងយល់អំពីក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋ ជាពិសេសក្រុមAPT32 ដែរឬទេ? តើវាផ្តល់នូវអត្ថប្រយោជន៍ និងចំណុចសំខាន់អ្វីខ្លះ? ឯកសារនេះមិនព្យាយាមសិក្សាលម្អិតនូវបច្ចេកទេសនៃក្រុមAPT32 ដែលកើតចេញពីការវិភាគ និងស្វែងរកភស្តុតាងឌីជីថលដោយផ្ទាល់នោះទេ ។ ឯកសារនេះមានគោលបំណងផ្តល់នូវការវិភាគ និងសិក្សាទៅឯកសារដែលផ្តល់ការសិក្សាបច្ចេកទេស និងវិធីសាស្ត្រនៃក្រុមហោគឃ័រនេះបានអនុវត្តរួចមកហើយក្នុងន័យស្វែងយល់ដើម្បីទប់ស្កាត់នូវវាយប្រហាររបស់ក្រុមនេះនៅលើកក្រោយៗទៀត ។ ដូចនេះមុននឹងទៅដល់ចំណុចសិក្សាបច្ចេកទេសរបស់ក្រុមAPT32 យើងត្រូវយល់ជាមុនសិនថា "*អ្វីជាក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋ?*" ។

២. អ្វីទៅជាក្រុមហេគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋ?

ពាក្យថាក្រុមហេគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋគឺមានន័យថាជាក្រុមហេគឃ័រដែលមានជំនាញប៉ិនប្រសប់បំផុតនៅក្នុងការវាយប្រហារមកលើប្រព័ន្ធកុំព្យូទ័រ ក៏ដូចជាឧបករណ៍អេឡិចត្រូនិចផ្សេងៗ ហើយក្រុមហេគឃ័រនេះទទួលការផ្គត់ផ្គង់ និងគ្រប់គ្រងដោយរដ្ឋាភិបាលប្រទេសណាមួយ [4] ។ ក្រុមហេគឃ័រប្រភេទនេះជាតួអង្គគំរាមកំហែងមួយដ៏ពិបាកនឹងទប់ស្កាត់ដោយសារភាពប៉ិនប្រសប់ក្នុងការវាយប្រហាររបស់ពួកគេ ព្រមទាំងធនធានដ៏សម្បូរបែបរបស់ពួកគេដើម្បីសម្រេចគោលដៅ ។ ក្រុមហេគឃ័រប្រភេទនេះគឺមានគោលបំណងក្នុងការវាយប្រហារច្បាស់លាស់ដូចជា តាមដានស៊ើបយកការណ៍ ព័ត៌មានយោធា បំផ្លាញដំណើរការ លួចព័ត៌មានសំងាត់ និងនិន្នាការនយោបាយជាដើម ។

ក្រុមហេគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋគឺមានវដ្តក្នុងការអនុវត្តន៍ការងារច្បាស់លាស់ដែលបែងចែកជា ៦ ដំណាក់កាលដូចខាងក្រោម៖

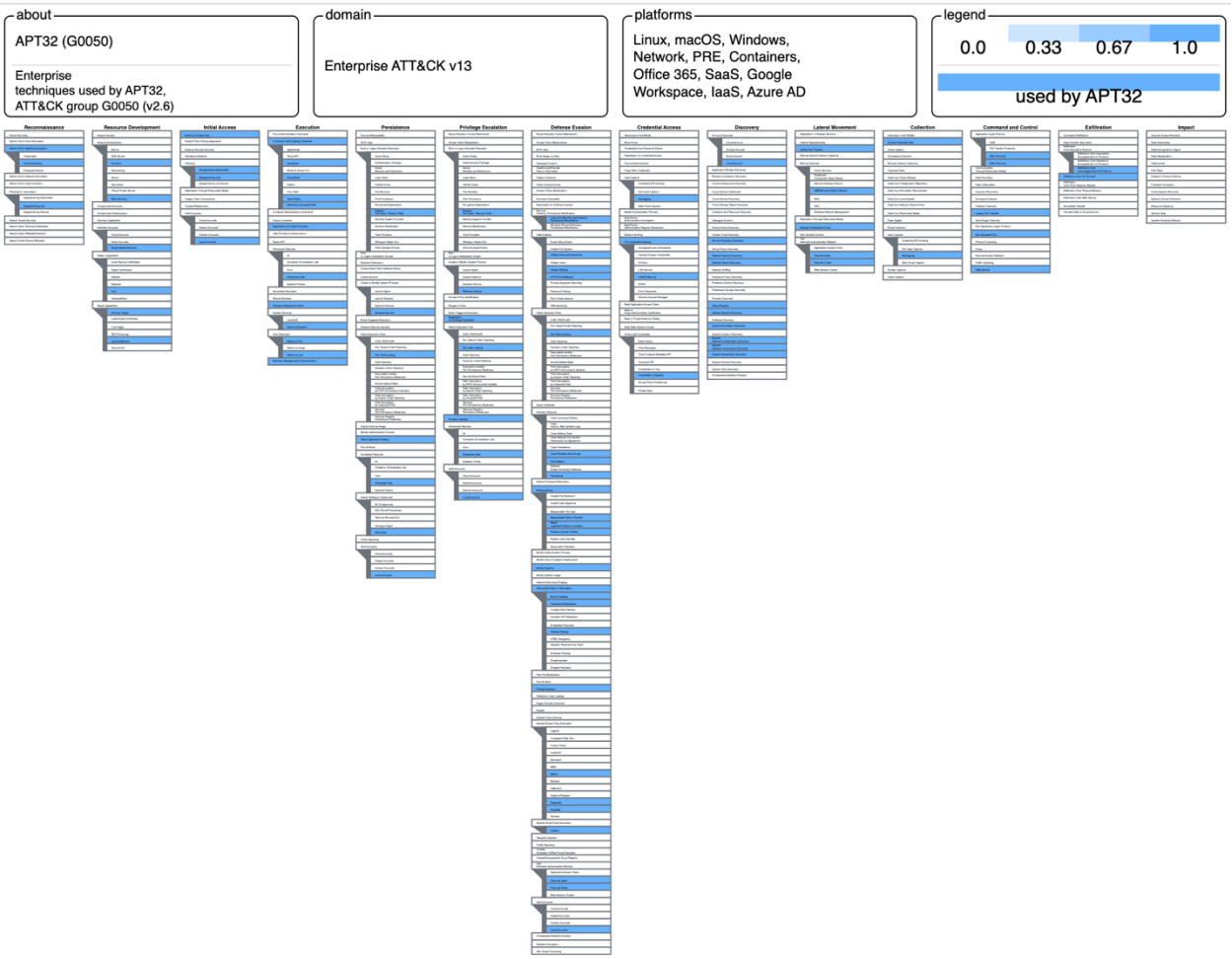
១. ការរៀបចំ និងត្រៀមខ្លួន (Preparation Phase)
២. ការវាយប្រហារចូលដំបូង (Initial Intrusion Phase)
៣. ពង្រីកវិសាលភាពគោលដៅវាយប្រហារ (Expansion Phase)
៤. ដំណាក់កាលសម្ងំ និងព្យាយាមភ្ជាប់នៅក្នុងប្រព័ន្ធ (Persistent Phase)
៥. បន្តស្វែងរក និងព្យាយាមទាញយកព័ត៌មាន (Exfiltration Phase)
៦. ដំណាក់កាលចុងក្រោយគឺបោសសំអាតដាន (Cleanup Phase)

រូបដ្យាក្រាមលម្អិតនៃវដ្តដំណើរការរបស់ក្រុមហេគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋ [5]

៣. ការសិក្សាបច្ចេកទេសរបស់ក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋ APT32

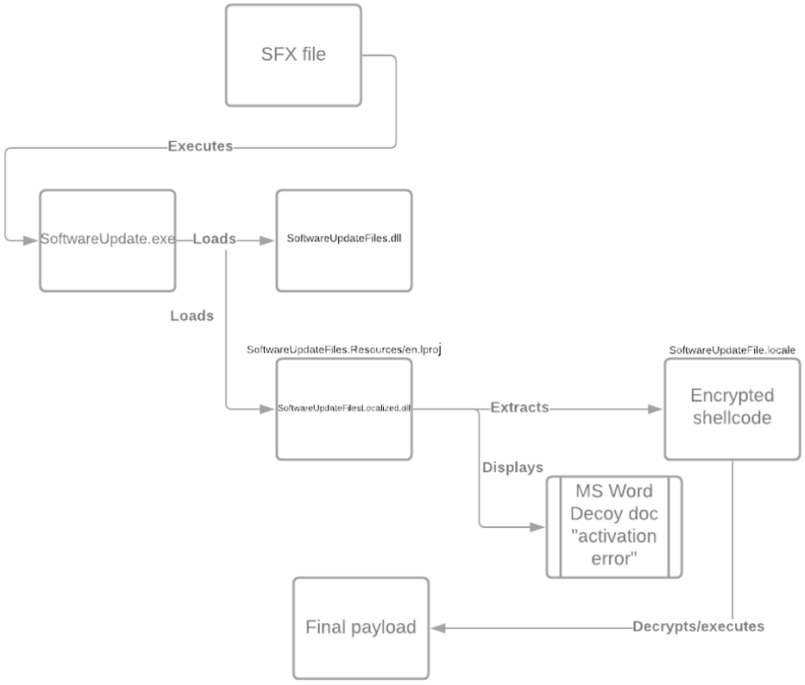
ក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋលេខ៣២នេះត្រូវបានគេឃើញថាមានសកម្មភាពចាប់តាំងពីឆ្នាំ២០១៤ ហើយដែលគេសង្ស័យថាមានទំនាក់ទំនង ឬក៏គ្រប់គ្រងដោយរដ្ឋាភិបាលវៀតណាម ។ ក្រុមហោគឃ័រនេះមានគោលដៅវាយប្រហារទៅលើអ្នកនយោបាយ ពាណិជ្ជករ មន្ត្រីរដ្ឋាភិបាលនៃប្រទេសហ្វីលីពីន ប្រជាមានិតឡាវ និងប្រទេសកម្ពុជា [6] ។ ក្រុមហោគឃ័រនេះបានប្រើប្រាស់វិធីសាស្ត្រដ៏ស្មុគស្មាញលើ បច្ចេកវិទ្យាវិបសាយដើម្បីវាយប្រហារចូលទៅក្នុងប្រព័ន្ធរបស់ប្រទេសគោលដៅ [7] ។ ក្រុមហោគឃ័រដែលគ្រប់គ្រងដោយរដ្ឋលេខ៣២ត្រូវបានគេដាក់ឈ្មោះអោយមួយចំនួនដូចជា៖ ក្រុម OCEAN LOTUS ក្រុម SEA LOTUS ក្រុម OCEAN BUFFALO ឬក៏ ក្រុម APT-C-00 ជាដើម [3] ។

តាមរយៈក្របខ័ណ្ឌ MITRE ATT&CK បានកត់ត្រានូវវិធីសាស្ត្រ បច្ចេកទេស និងតិចនិចក្នុងការវាយប្រហាររបស់ក្រុមហោគឃ័រលេខ៣២យ៉ាងលម្អិត [7] ។



បើយោងទៅឯកសាររបស់ក្រុមហ៊ុន Recorded Future វិញបានបង្ហាញអោយឃើញថាក្រុមហ៊ុនហោគឃ័រលេខ៣២នេះបានរៀបចំយុទ្ធនាការវាយប្រហារតាមរយៈការបញ្ជោតអោយជនគោលដៅចុចទៅលើឯកសារដែលបង្កប់នូវមេរោគពីខាងក្រោយ៖ **<u>ឯកសារទី១</u>**៖ (“បញ្ជីរាយនាមអនុព័ន្ធយោធាបរទេស និងការិយាល័យសហប្រតិបត្តិការយោធាប្រចាំកម្ពុជា.docx~[.]exe”) មេរោគនៅពីក្រោយនោះមានដល់ទៅបួនមេរោគបង្កប់ ៖ (១)SoftwareUpdate.exe (២)SoftwareUpdateFiles.dll (៣) SoftwareUpdateFilesLocalized.dll និង(៤)SoftwareUpdateFiles.locale ។ យោងទៅក្រុមអ្នកស្រាវជ្រាវ Insikt Group

នៃក្រុមហ៊ុន Recorded Future បញ្ជាក់ថាឯកសារមេរោគនេះបង្កប់ក្នុងប្រភេទឯកសារ SFX (Self-Extracting Archive) ហើយបានចែកចាយទៅប្រទេសគោលដៅ [1] ។



រូបភ្ជាក្រាម៖ ដំណើរការពេលបើកឯកសារមេរោគ

<u>ឯកសារទី២</u>៖ (“9_Programme_SOMCA_Japan_FINAL.docx~.exe”) ដែលបង្កប់នៅក្នុងប្រភេទឯកសារ SFX ទាក់ទិននឹងកិច្ចប្រជុំមន្ត្រីជាន់ខ្ពស់អាស៊ាននៃវប្បធម៌ និងសិល្បៈ ដែលមេរោគនេះវាយប្រហារទៅលើមន្ត្រីជាន់ខ្ពស់មកពីប្រទេសនៅអាស៊ាន ហើយត្រូវបានសង្កេតឃើញថាគោលដៅចំបងគឺមន្ត្រីជាន់ខ្ពស់រដ្ឋាភិបាលកម្ពុជា ។ ភស្តុតាងឌីជីថលបានបង្ហាញថាម៉ាស៊ីនមេបញ្ជាគឺនៅអាសយដ្ឋាន IP លេខ 43.254.132.212 ។ រូបខាងក្រោមគឺបញ្ជាក់អំពី ចំណុចដែលបែកធ្លាយ (Indicators of Compromised)

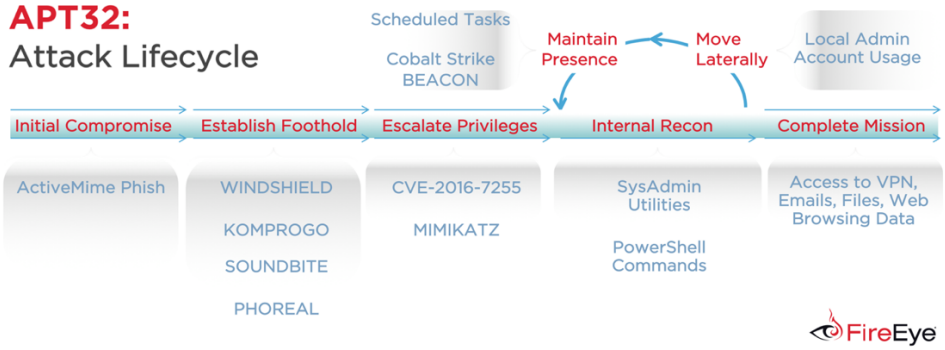
IP Address	Domain
43.254.132[.]117	bussinesappinstant[.]com, cloud.bussinesappinstant[.]com, query.bussinesappinstant[.]com
43.254.132[.]212	insappstaticanalyze[.]com, dns.insappstaticanalyze[.]com

Malware Hash	Malware Description
a030435018a67c07747751766132eb30a9a6bb6af161df225a27c0ec57156b61	Sample 1 parent SFX file
d873bdb08c45378650761bad71df7418c7b542adb13ccd4a87df2001801f4808	SoftwareUpdateFilesLocalized.dll
625f5253e306cce30da4dbff2a6ade608ca295b10d086b9eaaec4743e53b0c82	File named “SoftwareUpdateFiles.locale” containing encrypted shellcode
Dbde2b710bee38eb3ff1a72b673f756c27faa45d5c38cbe0f8a5dfccb16c18ba	APT32 sample referencing the 2020 ASEAN Summit
47ba92dc8c9302b2f70db70a0d46fef0ee2972edc3e1c4b637d5c76b4141c7a0	Sample 2 parent SFX file
75c61d9d8da4a87882ccdd37b664953c10a186b5545c5152fd1b6bf788a1a846	Historical Related APT32 Sample
cfbacb8a1ca087810d17d86fcf94d9c660cf3331ccb0b015709bb48a9adb1cc7	Historical Related APT32 Sample

ប្រភេទមេរោគត្រូវបានដែលក្រុមហេគឃ័រលេខ៣២បានប្រើប្រាស់ដើម្បីធ្វើសកម្មភាពចាប់តាំងពីឆ្នាំ២០១៤មក ក្រុមហ៊ុនសន្តិសុខដ៏ល្បីល្បាញ Madiant បានបង្ហាញនូវឈ្មោះមេរោគចំនួនបួន (១) KOMPROGO (២)WINDSHIELD (៣) SOUNDBITE និង(៤)មេរោគ BEACON [8] ។

Year	Country	Industry	Malware
2014	Vietnam	Network Security	WINDSHIELD
2014	Germany	Manufacturing	WINDSHIELD
2015	Vietnam	Media	WINDSHIELD
2016	Philippines	Consumer products	KOMPROGO WINDSHIELD SOUNDBITE BEACON
2016	Vietnam	Banking	WINDSHIELD
2016	Philippines	Technology Infrastructure	WINDSHIELD
2016	China	Hospitality	WINDSHIELD
2016	Vietnam	Media	WINDSHIELD
2016	United States	Consumer Products	WINDSHIELD PHOREAL BEACON SOUNDBITE

អ្វីដែលគួរអោយកត់សម្គាល់ចេញពីរបាយការណ៍របស់ក្រុមហ៊ុនសន្តិសុខ Madiant យើងឃើញថាក្រុមហេគឃ័រលេខ៣២នេះមិនត្រឹមតែដាក់គោលដៅទៅលើប្រទេសនៅក្នុងអាស៊ានទេ តែប្រទេសចិនក៏ស្ថិតនៅក្នុងគោលដៅរបស់ពួកគេដែលដោយសារបញ្ហាជម្លោះនៅសមុទ្រចិនខាងត្បូងរវាងវៀតណាម និងចិន ។ ហើយក្រុមហេគឃ័រ លេខ៣២ នេះក៏ព្យាយាមបង្កើនសមត្ថភាពមេរោគរបស់ពួកគេដែលអាចវាយប្រហារទៅប្រព័ន្ធប្រតិបត្តិការ MacOS របស់ក្រុមហ៊ុន Apple ផងដែរ ។



រូបដ្យាក្រាមវដ្តនៃការវាយប្រហាររបស់ក្រុមហេគឃ័រ លេខ៣២ ដែលរៀបចំដោយក្រុមហ៊ុន Madiant

៤. ខធីសាស្ត្រជម្លៀសការខាយប្រហារដោយក្រុមហោគយ័រដែលគ្រប់គ្រងដោយរដ្ឋ

ជាក់ស្តែងប្រសិនបើក្រុមហោគយ័រដែលគ្រប់គ្រងដោយរដ្ឋដាក់គោលដៅវាយប្រហារ ប្រទេសដែលងាយរងគ្រោះមានការលំបាកក្នុងការទប់ស្កាត់ និងជៀសផុតពីការជ្រៀតចូលទៅក្នុងប្រព័ន្ធ ។ ដូចនេះ ស្ថាប័ន ក៏ដូចជាមន្ត្រីត្រូវរៀបចំគោលនយោបាយសន្តិសុខសាយប័រ និងពង្រឹងនូវសមត្ថភាពមន្ត្រីគ្រប់រូបតាមរយៈកម្មវិធីបង្កើនការយល់ដឹងអំពីសន្តិសុខសាយប័រ [4] ។ មានការអនុវត្តល្អៗមួយចំនួនត្រូវបានលើកឡើងដើម្បីលើកកម្ពស់ការការពារសន្តិសុខសាយប័រដូចខាងក្រោម៖

- រៀបចំពង្រឹងសន្តិសុខទៅលើឧបករណ៍ និងជួសជុលនូវកម្មវិធី ក៏ដូចជាប្រព័ន្ធប្រតិបត្តិការជាប្រចាំ
- រៀបចំនូវគោលនយោបាយ និងវិធីសាស្ត្រការកំណត់សិទ្ធទៅតាមតួនាទីក្នុងប្រើប្រាស់ប្រព័ន្ធនីមួយៗ
- រៀបចំប្រើប្រាស់បច្ចេកវិទ្យាកូដនីយកម្មទៅលើទិន្នន័យទាំងពេលដែលទិន្នន័យនៅនឹងកន្លែង និងទិន្នន័យផ្ទេរទីតាំង ។

៥. សេចក្តីសន្និដ្ឋាន

ការសិក្សាទៅលើក្រុមហោគយ័រដែលគ្រប់គ្រងដោយរដ្ឋគឺជួយអោយយើងទាំងអស់គ្នាស្វែងយល់នូវវិធីសាស្ត្របច្ចេកទេស និងតិចនិចក្នុងការវាយប្រហារក្នុងគោលបំណងដើម្បីអាចពង្រឹងនូវវិធីសាស្ត្រការពារ ។ ជាក់ស្តែងដូចករណីក្រុមហោគយ័រលេខ៣២នេះបានប្រើប្រាស់វិធីសាស្ត្របោកបញ្ឆោតជនគោលដៅអោយចុចបើកឯកសារនៅលើកុំព្យូទ័រ ប្រសិនបើយើងដឹងនិងយល់ទាំងអស់គ្នានូវវិធីសាស្ត្រនេះ វានឹងជួយយើងទប់ស្កាត់នូវការវាយប្រហាររបៀបបែបនេះបាន ។ ការសិក្សាទៅលើបច្ចេកទេសរបស់ក្រុមហោគយ័រគឺការកសាងសមត្ថភាព និងពង្រឹងការយល់ដឹងទៅលើសន្តិសុខសាយប័រ ។

៦. ឯកសារយោង

[1] Pulse Report: New APT32 Malware Campaign Targets Cambodian Government, Recorded Future
[2] Ocean Lotus, Wikipedia. Link: https://en.wikipedia.org/wiki/OceanLotus
[3] Malpedia APT32. Link: https://malpedia.caad.fkie.fraunhofer.de/actor/apt32
[4] Advanced Persistence Threat Slides, Pluralsight
[5] Advanced Persistence Threat Wikipedia. Link: https://en.wikipedia.org/wiki/Advanced_persistent_threat
[6] OceanLotus APT Wikipedia. Link: https://en.wikipedia.org/wiki/OceanLotus
[7] APT32, MITRE ATT&CK. Link: https://attack.mitre.org/groups/G0050/
[8] Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations, Madiant.
Link: https://www.mandiant.com/resources/blog/cyber-espionage-apt32