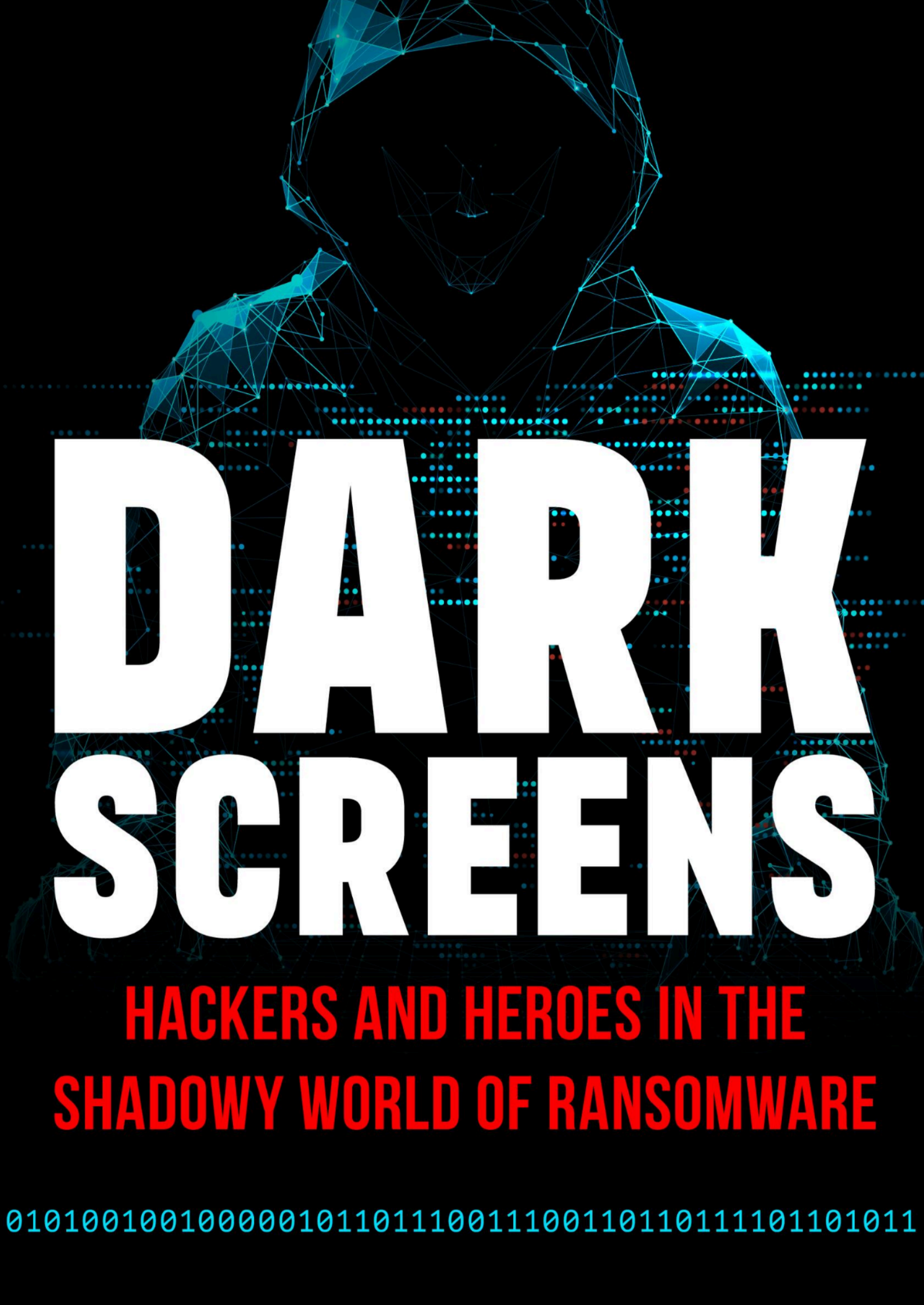

DARK SCREENS

HACKERS AND HEROES IN THE SHADOWY WORLD OF RANSOMWARE

01010010010000010110111001110011011011110110101 1

របាយការណ៍ស្រាវជ្រាវ៖ ក្រុមចោរព័ត៌មានវិទ្យា Cl0p (Cl0p Ransomware Group)

១. ប្រវត្តិនៃក្រុម Hacker

- **ពេលវេលា៖** ក្រុម **Cl0p** បានចាប់ផ្តើមលេចឡើងដំបូងនៅក្នុងខែកុម្ភៈ ឆ្នាំ២០១៩។ វាគឺជាប្រភេទមេរោគដែលអភិវឌ្ឍបន្តពីមេរោគ "CryptoMix"។
- **ភាពល្បីល្បាញ៖** ក្រុមនេះល្បីល្បាញខ្លាំងក្នុងការប្រើប្រាស់យុទ្ធសាស្ត្រ "Big Game Hunting" ដែលសំដៅលើការវាយប្រហារទៅលើក្រុមហ៊ុនខ្នាតយក្ស និងការប្រើប្រាស់ចន្លោះប្រហោង Software ដែលមិនទាន់ត្រូវបានគេរកឃើញ (Zero-day vulnerabilities) ដើម្បីវាយលុកក្នុងទ្រង់ទ្រាយធំ។
- **ការជំរុញទឹកចិត្ត៖** ក្រុមនេះធ្វើសកម្មភាពដើម្បី **ផលចំណេញហិរញ្ញវត្ថុ** ជាចម្បង។ ទោះបីជាពួកគេត្រូវបានគេជឿថាមានមូលដ្ឋាននៅក្នុងប្រទេសដែលនិយាយភាសារុស្ស៊ី ប៉ុន្តែគោលដៅចម្បងគឺការជំរិតទារប្រាក់ពីក្រុមហ៊ុនធំៗ។

២. របៀបដែលក្រុមនេះប្រតិបត្តិការ (កម្រិតទូទៅ)

- **ប្រភេទនៃការវាយប្រហារទូទៅ៖**
  - **ការទាញយកផលប្រយោជន៍ពីចន្លោះប្រហោង (Zero-Day Exploits):** ពួកគេស្វែងរកចន្លោះប្រហោងក្នុងកម្មវិធីផ្ទេរទិន្នន័យ (File Transfer Services) ដើម្បីចូលទៅក្នុងប្រព័ន្ធរបស់ក្រុមហ៊ុនរាប់ពាន់ក្នុងពេលតែមួយ។
  - **ការជំរិតទារប្រាក់ពីរជាន់ (Double Extortion):** ពួកគេមិនត្រឹមតែចាក់សោរទិន្នន័យ (Encrypt) ប៉ុណ្ណោះទេ ប៉ុន្តែពួកគេថែមទាំងលួចចម្លងទិន្នន័យនោះចេញទៀតផង។ ប្រសិនបើជនរងគ្រោះមិនព្រមបង់ប្រាក់ ពួកគេនឹងគំរាមបញ្ចេញទិន្នន័យទាំងនោះជាសាធារណៈ។
  - **ការវាយប្រហារលើខ្សែសង្វាក់ផ្គត់ផ្គង់ (Supply Chain Attacks):** វាយប្រហារលើក្រុមហ៊ុនផ្តល់សេវាកម្មតែមួយ ដើម្បីទទួលបានច្រកចូលទៅកាន់ក្រុមហ៊ុនរាប់រយផ្សេងទៀតដែលប្រើប្រាស់សេវាកម្មនោះ។
- **គោលដៅទូទៅ៖** ស្ថាប័នរដ្ឋាភិបាល, ក្រុមហ៊ុនពហុជាតិ, ធនាគារ, សាកលវិទ្យាល័យធំៗ និងវិស័យសុខាភិបាល។

៣. មូលហេតុ និងគោលដៅ

- **ហេតុអ្វីបានជាក្រុមនេះវាយប្រហារ?** ដើម្បីទទួលបានទឹកប្រាក់យ៉ាងច្រើនសន្ធឹកសន្ធាប់ពីការជំរិត។
- **គោលបំណងចម្បង៖**
    - **លុយកាក់៖** ការទារប្រាក់រាប់លានដុល្លារពីជនរងគ្រោះ។
    - **ប្រសិទ្ធភាព៖**
      ការប្រើប្រាស់បច្ចេកវិទ្យាស្វ័យប្រវត្តិដើម្បីវាយប្រហារក្រុមហ៊ុនជាច្រើនក្នុងពេលតែមួយ ដើម្បីបង្កើនឱកាសទទួលបានប្រាក់។

៤. ផលប៉ះពាល់នៃការវាយប្រហារ

- **ការបាត់បង់ហិរញ្ញវត្ថុ៖** ក្រុមហ៊ុនត្រូវចំណាយប្រាក់លើការបង់ថ្លៃជំរិត, ថ្លៃមេធាវី និងការចំណាយលើការជួសជុលប្រព័ន្ធឡើងវិញ។
- **ការលេចធ្លាយទិន្នន័យ៖** ព័ត៌មានផ្ទាល់ខ្លួនរបស់មនុស្សរាប់លាននាក់ដូចជា លេខសន្តិសុខសង្គម, ប្រវត្តិវេជ្ជសាស្ត្រ និងទិន្នន័យធនាគារត្រូវបានលួច។
- **ការរអាក់រអួលនៃសេវាកម្ម៖** ប្រព័ន្ធបើកប្រាក់បៀវត្សរ៍ ឬប្រព័ន្ធគ្រប់គ្រងសិស្ស-និស្សិតត្រូវបានផ្អាកដំណើរការរាប់សប្តាហ៍។
- **ការខូចខាតកេរ្តិ៍ឈ្មោះ៖** បាត់បង់ទំនុកចិត្តពីអតិថិជន និងដៃគូអាជីវកម្មនៅពេលដែលទិន្នន័យសម្ងាត់ត្រូវបានលេចធ្លាយ។

៥. ការឆ្លើយតបរបស់ក្រុមសន្តិសុខបច្ចេកវិទ្យា

- **ការរកឃើញ៖** ក្រុមសន្តិសុខប្រើប្រាស់ឧបករណ៍ EDR ដើម្បីតាមដានសកម្មភាពខុសប្រក្រតី ដូចជាការបញ្ជូនទិន្នន័យក្នុងបរិមាណដ៏ច្រើនទៅកាន់អាសយដ្ឋាន IP ដែលមិនស្គាល់។
- **ការប្រើប្រាស់ព័ត៌មានសម្ងាត់ (Threat Intelligence):**
  ការចែករំលែកព័ត៌មានអំពីវិធីសាស្ត្ររបស់ក្រុម Cl0p ក្នុងចំណោមអ្នកជំនាញសន្តិសុខ ដើម្បីត្រៀមខ្លួនការពារជាមុន។
- **យុទ្ធសាស្ត្រការពារ៖**
    - **ការធ្វើបច្ចុប្បន្នភាព (Patch Management):**
      ដំឡើងកំណែថ្មីៗនៃសូហ្វវែរភ្លាមៗដើម្បីបិទចន្លោះប្រហោង។
    - **ស្ថាបត្យកម្ម Zero Trust:** កម្រិតសិទ្ធិប្រើប្រាស់ក្នុងប្រព័ន្ធ ដើម្បីកុំឱ្យ Hacker អាចធ្វើដំណើរទៅកាន់ផ្នែកផ្សេងៗបានដោយងាយ។

៦. ផលប៉ះពាល់ដល់សន្តិសុខសាយប័រជាសកល

- **ការយល់ដឹងអំពីខ្សែសង្វាក់ផ្គត់ផ្គង់៖** ការវាយប្រហាររបស់ Cl0p បានធ្វើឱ្យពិភពលោកយល់ថា ក្រុមហ៊ុននីមួយៗមានសុវត្ថិភាពត្រឹមតែកម្រិតដែលសូហ្វវែរដែលពួកគេទិញមកប្រើប្រាស់មានសុវត្ថិភាពប៉ុណ្ណោះ។
- **ច្បាប់ថ្មីៗ៖**
  បង្កើនការរឹតបន្តឹងលើច្បាប់រាយការណ៍អំពីការលេចធ្លាយទិន្នន័យឱ្យបានឆាប់រហ័សដល់សាធារណជន។

៧. បញ្ហាសីលធម៌ និងច្បាប់

- **ភាពខុសច្បាប់៖** ការប្រើប្រាស់ Ransomware គឺជាបទល្មើសព្រហ្មទណ្ឌធ្ងន់ធ្ងរ រួមមានការលួចចូលប្រព័ន្ធដោយគ្មានការអនុញ្ញាត, ការជំរិតទារប្រាក់ និងការលាងលុយកខ្វក់។
- **ទោសទណ្ឌ៖** សមាជិកក្រុម Hacker អាចប្រឈមនឹងការចាប់ខ្លួនជាអន្តរជាតិ ការរឹបអូសទ្រព្យសម្បត្តិ និងការជាប់ពន្ធនាគារជាច្រើនទសវត្សរ៍។
- **ការលួចចូលប្រព័ន្ធប្រកបដោយសីលធម៌ (Ethical Hacking) vs ការលួចចូលជាបទល្មើស៖**
  - **Hacker បទល្មើស (Cl0p):** វាយលុកដើម្បីលួច និងបង្កការខូចខាតដើម្បីប្រយោជន៍ខ្លួនឯង។
  - **Ethical Hacker:**
    ប្រើប្រាស់ជំនាញដូចគ្នាដើម្បីស្វែងរកចន្លោះប្រហោងក្នុងបំណងជួយជួសជុល និងការពារប្រព័ន្ធ។

៨. សេចក្តីសន្និដ្ឋាន

- **មេរៀនដែលទទួលបាន៖** ក្រុម Cl0p បង្ហាញថា
  សូម្បីតែកម្មវិធីដែលយើងទុកចិត្តបំផុតក៏អាចក្លាយជាច្រកផ្លូវសម្រាប់សត្រូវដែរ។
  ការការពារដ៏ល្អបំផុតគឺការធ្វើបច្ចុប្បន្នភាពជាប្រចាំ។
- **សារៈសំខាន់នៃការយល់ដឹង៖** ការយល់ដឹងអំពីវិធីសាស្ត្ររបស់ក្រុម Hacker ជួយឱ្យអ្នកការពារអាចប្តូរពីការ "ដេញតាមដោះស្រាយបញ្ហា" មកជាការ "ការពារជាមុន" ដើម្បីកាត់បន្ថយគ្រោះថ្នាក់។