



# Cl0p Ransomware Group Analysis

ការពិនិត្យដឹងទូលំទូលាយនៃប្រតិបត្តិការ ransomware ដើម្បីរួចរាល់ពិភពលោក

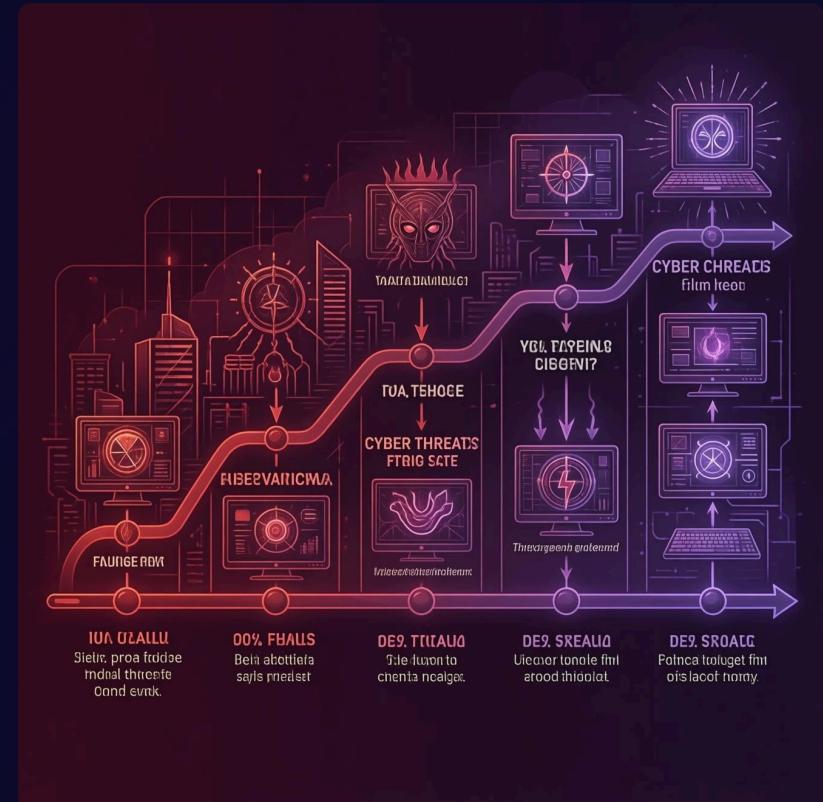
# សេចក្តីផ្តើម និង សារតាម

## Origins and Evolution

Cl0p ជាលេចឡូជាលើកដំបូងនៅថ្ងៃមេធ្នូ 2019 ជាការវិគ្គនឹងដីទំនើបនៃក្រុមត្រួរសារ ransomware CryptoMix។ ក្រុមនេះបានសម្រាប់ខ្លួនយ៉ាងឆាប់រហូតតាមរយៈបច្ចុកទេសអុន គ្រឿបក្រើមត្រួតពិនិត្យសំណង់និងការកំណត់គោលដៅជាមួយនា។

ឈ្មោះរបស់ពួកគេជានមកពីផ្ទៀកបន្ថែមដឹកសារ .clop ដែលត្រូវបានដាក់ជានមកសារដែលបានអុនិនគ្រឿប។  
ក្រុមនេះដំណើរការជាថម្យដឹកសារអីរុបខាងកើត ហើយមានទំនាក់ទំនងជាមួយសម្បន្តខ្លួនគ្នា។  
អ្នកដឹកសារ TA505។

នៅឆ្នាំ 2020 Cl0p បានកើតឡើងដូចជាប្រព័ន្ធសាស្ត្ររបស់ពួកគេដើម្បីផ្តល់តម្លៃលើគោលដៅដែលមានតម្លៃខ្ពស់ ដែលជាការផ្តល់បញ្ជីទៅការរាយប្រហារទ្រង់ត្រាយដំ។



# ការលើកទីកច្ចាន់ ន្រក់ចំណោញ ផ្ទកហិរញ្ញវត្ថុជាមរយ: 'Big Game Hunting'

## High-Value Targets

Cl0p ស្អដែកតែអង្គភាពដែលមាន  
ធនធានហិរញ្ញវត្ថុប្រើប្រាស់ និងប្រព័ន្ធឌីជីថប់  
ទិន្នន័យសំខាន់ៗ។

## Ransom Demands

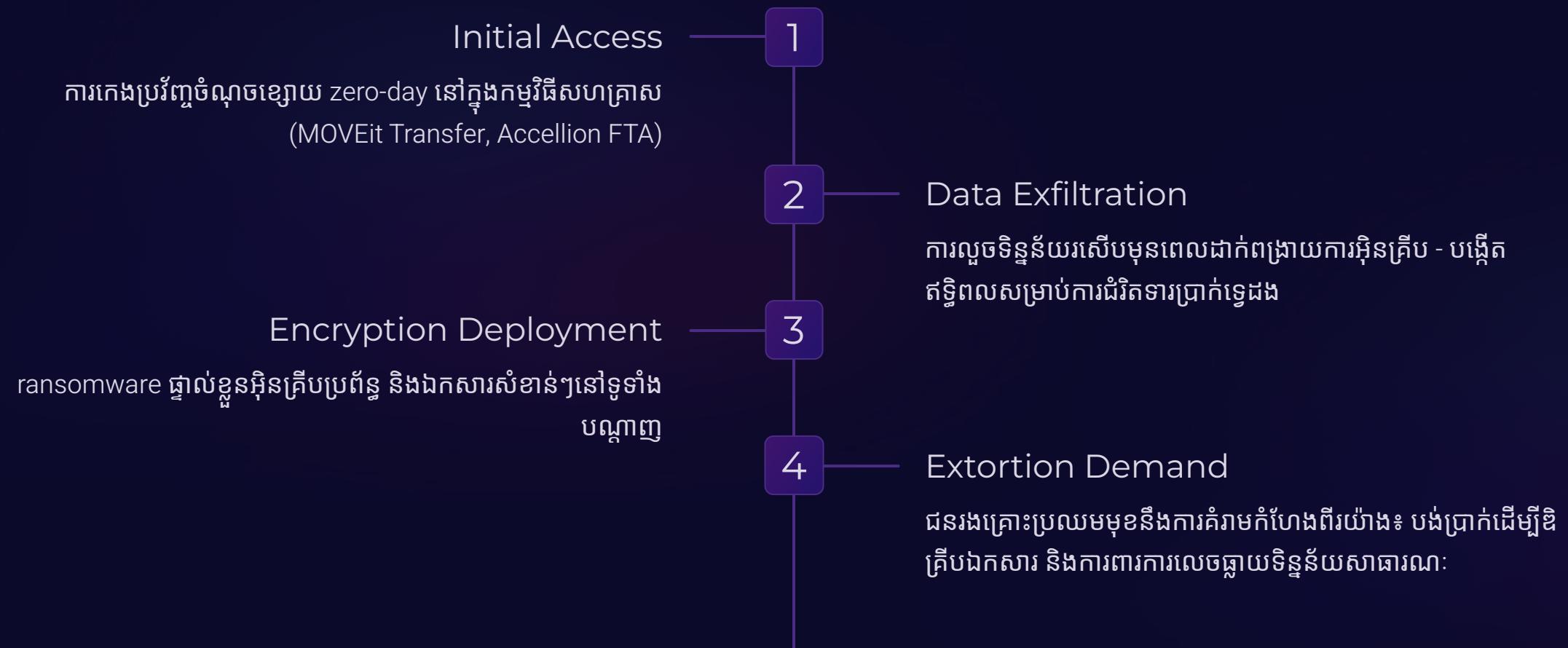
ការទាមទារប្រាក់លោកដាមូលដ្ឋានចាប់ពី  
៥ លានដុល្លារ ដល់ ២៥ លានដុល្លារ  
ដោយខ្លះលើសពី ៥០ លានដុល្លារ

## Data Leverage

ទិន្នន័យរសិបដែលត្រូវបានគេលួចផ្តល់ទូទាត់ដឹងទាំងអស់



# Attack Methods: Zero-Day Exploits & Double Extortion



- ▢ ចំណុចខ្សោយ MOVEit (CVE-2023-34362) តែមួយមុខដានធ្វើឱ្យបែប៖ពាល់ដល់អង្គភាពជាង 2,000 នៅទូទាំងពិភពលោក

# គោលដៅធ្វើធម្មតាទំនើមអ្នកណាមួយដែលមានហានីភ័យ?



## Large Corporations

ក្រុមហ៊ុន Fortune 500 ដែលមានផនធានបរព្យាព្យាប់យ៉ាងទូលំទូលាយ  
និងកម្មសិទ្ធិបញ្ជាផីមានតម្លៃ



## Government Agencies

អង្គភាពក្រុង និងរដ្ឋដែលមានទិន្នន័យពលរដ្ឋរសីប និងចរើកាសនិស្សុខ  
តាមអ្នកជើរិកាសកំណត់



## Healthcare Systems

មន្ទីរពេទ្យ និងបណ្តាញផ្តល់សាស្ត្រដែលមានទិន្នន័យអ្នកជើសរើស សំខាន់ៗ  
និងការអគ្គន៍របស់ពេទ្យពេលវេលាអារិយាជាតា



ការថែទាំសុខភាពនៅក្នុងការរួមច្បាប់ជាប្រព័ន្ធដែលមាន  
ទំនាក់ទំនងនៅក្នុងការប្រព័ន្ធឌើម្បី បច្ចេកវិទ្យាថាសំខាន់នៃប្រតិបត្តិការ  
ដែលធ្វើឱ្យពួកគេទំនងជាបង់ប្រាក់លោកយ៉ាងឆាប់រហូត។

# ផលបែះពាល់សកល

\$75... 2000+ 77M

## Average Campaign Losses

ការខួចខាលហិរញ្ញវត្ថុដែលបាន  
បានប្រមាណភាពក្នុងមួយយុទ្ធសាស្ត្រ  
ការ Cl0p ដើម្បីសំខាន់រូមទាំង  
ការណោះពេលរលាយនៅថ្ងៃនេះ

ការសង្កោះ

## Organizations Compromised

ដនវងគ្រោះដែលរងជលបែះ  
ពាល់ដោយការកែងប្រើពេញភាព  
ងាយរងគ្រោះ MOVEit នៅ  
២០២៣ តែម្នាក់នេង

## Records Exposed

ឯកសារធ្វាល់ខ្ពស់ត្រូវបានគេ  
លួច និងលើចធ្វាយតាមរយៈ  
គេហទំនើសរបស់ខ្លួន នៃ  
របស់ Cl0p

ក្រោពីការខាលបង់ផ្ទុកហិរញ្ញវត្ថុដោយធ្វាល់ ការរាយប្រហារ Cl0p បានបណ្តាលឱ្យមានការអំខានជំ  
ប្រតិបត្តិការរយៈពេលជាប្រើប្រាស់ ការពិនិត្យផ្ទុកបទបង្ហាញ និងការខួចខាលកេរីស្មានរយៈពេល  
រៀងជល់អង្គការដនវងគ្រោះ។

# យុទ្ធសាស្ត្រវកយើញ និងផ្លូវតាម



# Endpoint Detection & Response (EDR)

## Threat Intelligence

មតិពីរឿងមានស្តីបការនៅសម្បាត់តាមពេលវេលាដាក់  
ស្ថិតិថ្មីនូវស្ថិតិនាករនៃការសម្របសម្រួល  
(IOCs) និងយុទ្ធសាស្ត្ររបស់ភ្នាក់ងារគណៈកម្មកំហែង  
សម្រាប់ការការពារប្រកបដោយភាពសកម្ម។

## Rapid Incident Response

ការបង់ចេកបណ្តាលព្យាមា និងការព្យួរត្រួតពិនិត្យ  
កាត់បន្ទូយការវិភាគជាលើនៃមេរាជចាប់ដីវិទិកឯង  
អំឡុងពេលវាយប្រហារសកម្ម

## Key Detection Indicators:

- Unusual outbound data transfers
  - Mass file modification events
  - Disabled security tools
  - Unauthorized credential access





# ការធ្វើសំបុរសនឹងសុខសកល

1

# Supply Chain Security Focus

តន្លេរែនេះ អង្គការនានាដើរាមាយតម្លៃម្ចាស់  
ម៉ោចចំណាំពីអ្នកលក់ភាគីទិន្នន័យ បន្ទាប់ពីការកែងប្រវត្តិ  
សម្រាកកម្មវិធីផែលគ្រឹះទុកចិត្តរបស់ CIOp ។ ខ្លួន  
សង្គាក់ផ្តល់ជូនកម្មវិធីបានភ្លាយជាអូចកម្មរាយ  
ប្រហារដើម្បីសំខាន់ម្ចាស់ផែលតម្លៃម្ចាស់មានការត្រួត  
ពិនិត្យជាបន្ទាប់។

2

# Zero-Day Vulnerability Management

រដ្ឋូនការជាក់ពង្រាយបំណះដែលបង្កើនលើវា  
និងកម្មវិធីបង្ហាញភាពងាយរងគ្រោះបានភាយជា  
ស្ថិជារខស្សាបកម្ម។ ឥឡូវនេះ ក្នុងហុងនាន  
រក្សានឹតិវិធីបំណះបន្ទាន់សម្រាប់ភាពងាយរង  
គ្រោះផ្លូវ។

3

## Regulatory Evolution

# ក្រុមសីលផែន និងភាពស្របច្បាំរៀង និងភាពពីរយ៉ាងនៃការលើចច្បូល ប្រព័ន្ធអីនធិណិត

- Unauthorized access to systems
  - Data theft and extortion
  - Financial fraud and ransomware
  - Violation of computer fraud laws
  - Potential prison sentences and fines



# Ethical Hacking

- Authorized penetration testing
  - Vulnerability research and disclosure
  - Security improvements and defense
  - Compliance with legal frameworks
  - Professional certifications (CEH, OSCP)



# មេរីនសំខាន់ៗសម្រាប់អ្នកជំនាញ សន្តិសុខតាមអ្នកជើងិជិត

01

## Stay Current on Threat Landscape

តាមដានជាបន្ទូបន្ទាប់នូវការគំរាយកំហែង យុទ្ធសាស្ត្រ  
និងភាពងាយរងគ្រារដែលកំពុងលេចចេញតាមរយៈ  
ប្រតិបត្តិការណ៍សម្ងាត់គំរាយកំហែង

02

## Implement Defense-in-Depth

ការគ្រប់គ្រងសុវត្ថិភាពជាប្រសព្វបំផុតទាំងបណ្តាលៗ  
ចំណុចបញ្ចប់ កម្មវិធី និងកម្រិតនិន្នន័យ

03

## Prioritize Supply Chain Security

ត្រួតពិនិត្យអ្នកលក់តារីបី និងរក្សាទាមមីនីយ៍  
ទៅលើភាពអាស្រែយនៃកម្មវិធី

04

## Develop Incident Response Plans

រៀបចំ និងសាកល្បងនឹតិវិធីឆ្លើយតប ransomware ជាប្រចាំមុនពេលមានខប្បន្តិ  
ហេតុកើតឡើង

05

## Champion Ethical Practice

ប្រើប្រាស់ជំនាញបច្ចេកទេសដោយមានការទទួលខុសត្រូវក្នុងក្របខ័ណ្ឌច្បាប់ និង  
សិលជម់ ដើម្បីការពារអង្គភាពនានា

"ការការពារដីមានប្រសិទ្ធភាពបំផុតប្រព័ន្ធនឹងអ្នកគំរាយកំហែងដើម្បីទិន្នន័យជាប្រធាន់ CIO មិនមែនជាបច្ចេកវិទ្យាអំឡុងយោន់ទេ ប៉ុន្តែជាការអនុមបញ្ហាល័ត្នរវាងអ្នកជំនាញដែល  
មានជំនាញ ដែរការវិនិច្ឆ័យ និងការសម្របខ្លួនជាបន្ទូបន្ទាប់។"