# Threat Analysis Report

## รายงานวิเคราะห์การโจมตี Ransomware ของกลุ่ม Dire Wolf


22/08/2025

TLP:CLEAR

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ ชั้น ๗ อาคารซี ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

# สารบัญ

สารบัญ ..... 2
บทสรุปสำหรับผู้บริหาร ..... 3
Threat Actor Profile ..... 4
กลยุทธ์ เทคนิค และขั้นตอน (TTPs) ..... 5
เครื่องมือและมัลแวร์ (Tools and Malware) ..... 7
Indicator of Compromise (IOCs) ..... 10
แนวทางการเฝ้าระวัง ป้องกัน และรับมือ ..... 11
อ้างอิง (References) ..... 13

# บทสรุปสำหรับผู้บริหาร

Dire Wolf เป็นกลุ่มแรนซัมแวร์ที่ปรากฏตัวขึ้นในเดือนพฤษภาคม 2025 และใช้วิธีการขู่กรรโชกซ้ำซ้อน (double-extortion model) หลังจากเข้าถึงระบบของเหยื่อได้แล้ว ผู้โจมตีจะขโมยข้อมูลที่ละเอียดอ่อนออกไปก่อนที่จะเข้ารหัสไฟล์ด้วยนามสกุลเฉพาะคือ “.direwolf” เหยื่อจะพบจดหมายเรียกค่าไถ่ ซึ่งโดยทั่วไปจะใช้ชื่อว่า “HowToRecoveryFiles.txt” โดยในจดหมายจะมีลิงก์สำหรับติดต่อผ่านเครือข่าย Tor และตัวนับเวลาถอยหลัง ซึ่งมักจะให้เวลาเหยื่อเพียง 3 วัน ในการเจรจาก่อนที่ข้อมูลจะถูกปล่อยสู่โลกออนไลน์ หากยังไม่มีการจ่ายค่าไถ่ ผู้โจมตีจะยกระดับการคุกคามโดยการปล่อยข้อมูลบางส่วนหรือทั้งหมดออกมาในช่วงหลายสัปดาห์ถัดไป

แรนซัมแวร์ Dire Wolf ถูกพัฒนาขึ้นด้วยภาษา Go (Golang) และถูกบีบอัดด้วย UPX ทำให้ยากต่อการตรวจจับและสามารถทำงานข้ามแพลตฟอร์มได้ เมื่อถูกสั่งให้ทำงาน มันจะตรวจสอบเครื่องหมาย (marker) และมิวเท็กซ์ (mutex) ที่เฉพาะเจาะจงเพื่อหลีกเลี่ยงการติดเชื้อซ้ำซ้อน หากตรวจพบตัวบ่งชี้ดังกล่าว มัลแวร์จะทำลายตัวเอง การทำงานอย่างมีประสิทธิภาพนี้แสดงให้เห็นถึงความซับซ้อนที่มุ่งเป้าไปที่การลดโอกาสถูกตรวจจับและสร้างความเสียหายให้ได้มากที่สุด เพื่อปิดการทำงานของระบบป้องกัน Dire Wolf จะมุ่งเป้าไปที่ล็อกของระบบ (system logs) และซอฟต์แวร์แอนติไวรัส มันใช้ PowerShell และ WMI เพื่อปิดการบันทึกเหตุการณ์ของ Windows (Windows event logging) ซึ่งทำให้ทีมความปลอดภัยไม่สามารถตรวจสอบอะไรได้ นอกจากนี้ มัลแวร์ยังบังคับปิดโปรเซสและเซอร์วิสหลายสิบรายการ รวมถึงเครื่องมือสำรองข้อมูลและเครื่องมือป้องกันต่างๆ จากนั้นจะออกคำสั่งเพื่อลบ Shadow Copies และทรัพยากรสำรองข้อมูลอื่นๆ เพื่อให้แน่ใจว่าเหยื่อจะไม่สามารถกู้คืนข้อมูลได้หากไม่มีคีย์ถอดรหัส ไฟล์ที่ถูกเข้ารหัสจะถูกล็อกโดยใช้อัลกอริทึมการเข้ารหัสแบบผสมผสานระหว่าง Curve25519 และ ChaCha20 ซึ่งเป็นที่รู้จักในด้านความปลอดภัยและความเร็ว ในจดหมายเรียกค่าไถ่แต่ละฉบับ กลุ่มผู้โจมตีจะระบุข้อมูลสำหรับล็อกอินเข้าสู่พอร์ทัลเจรจาต่อรองที่ไม่ซ้ำกัน เพื่อให้เหยื่อสามารถติดต่อกับผู้โจมตีได้ ซึ่งมักจะอยู่ภายใต้การข่มขู่ว่าจะเปิดเผยข้อมูลในทันที มีคดีที่มีชื่อเสียงหลายคดีที่เชื่อมโยงกับ Dire Wolf รวมถึงการโจมตีที่เกี่ยวข้องกับการขโมยข้อมูลที่ละเอียดอ่อนขนาดหลายร้อยกิกะไบต์ ยอดเงินค่าไถ่ที่เรียกนั้นมีมูลค่าสูงถึงหลายแสนดอลลาร์ ในบางกรณี กลุ่มผู้โจมตีได้ปล่อยตัวอย่างข้อมูลที่ขโมยมา (proof-of-leak) เพื่อกดดันให้เหยื่อยอมทำตาม ที่น่าสนใจคือ มีกรณีหนึ่งที่กลุ่มนี้ประกาศรายชื่อเหยื่อหลังจากที่เหยื่อรายเดียวกันเพิ่งถูกประกาศโดยกลุ่มใหม่อีกกลุ่มหนึ่งชื่อ Devman

# Threat Actor Profile

| | |
|---|---|
| **ชื่อกลุ่ม** | Dire Wolf Ransomware |
| **ประวัติ** | Dire Wolf เป็นกลุ่มแรนซัมแวร์ที่ปรากฏตัวขึ้นในเดือนพฤษภาคม 2025 และใช้วิธีการขู่กรรโชกซ้ำซ้อน (double-extortion model) หลังจากเข้าถึงระบบของเหยื่อได้แล้ว ผู้โจมตีจะขโมยข้อมูลที่ละเอียดอ่อนออกไปก่อนที่จะเข้ารหัสไฟล์ด้วยนามสกุลเฉพาะคือ “.direwolf” เหยื่อจะพบจดหมายเรียกค่าไถ่ ซึ่งโดยทั่วไปจะใช้ชื่อว่า “HowToRecoveryFiles.txt” โดยในจดหมายจะมีลิงก์สำหรับติดต่อผ่านเครือข่าย Tor และตัวนับเวลาถอยหลัง ซึ่งมักจะให้เวลาเหยื่อเพียง 3 วันในการเจรจาก่อนที่ข้อมูลจะถูกปล่อยสู่โลกออนไลน์ หากยังไม่มีการจ่ายค่าไถ่ ผู้โจมตีจะยกระดับการคุกคามโดยการปล่อยข้อมูลบางส่วนหรือทั้งหมดออกมาในช่วงหลายสัปดาห์ถัดไป |
| **ประเภทของ Threat Actor** | Ransomware Group |
| **เป้าหมายการโจมตี** | • สหรัฐอเมริกา<br>• ไทย<br>• ไต้หวัน<br>• สิงคโปร์<br>• อิตาลี<br>• อินเดีย<br>• ญี่ปุ่น<br>• ออสเตรเลีย<br>• เยอรมนี<br>• แคนาดา<br>• เกาหลีใต้ |
| **อุตสาหกรรมเป้าหมาย** | • เทคโนโลยี<br>• การผลิต<br>• การบริการทางการเงิน<br>• การดูแลสุขภาพ<br>• บริการก่อสร้าง<br>• รัฐบาล |
| **ความเชื่อมโยงกับกลุ่มแรนซัมแวร์อื่น** | • Devman |

# กลยุทธ์ เทคนิค และขั้นตอน (TTPs)

สรุปภาพรวมของช่องทางการโจมตี แหล่งที่มา ความรุนแรง และผลกระทบ เพื่อให้เห็นภาพความสัมพันธ์ของความเสี่ยงต่างๆ และช่วยในการวางแผนป้องกันได้อย่างมีประสิทธิภาพ

**ตาราง MITRE ATT&CK**

| Tactic (กลยุทธ์) | Technique ID | Technique | Description |
|---|---|---|---|
| Execution | T1059.001 | Command and Scripting Interpreter: PowerShell | ใช้ PowerShell เพื่อรันคำสั่งในการปิดการทำงานของ Windows Event Log |
| | T1047 | Windows Management Instrumentation (WMI) | ใช้ WMI ร่วมกับ PowerShell เพื่อปิดการทำงานของระบบบันทึกเหตุการณ์ (Logging) |
| Defense Evasion | T1027 | Obfuscated Files or Information | มัลแวร์ถูกบีบอัด (packed) ด้วย UPX เพื่อทำให้การวิเคราะห์ทำได้ยากและหลบเลี่ยงการตรวจจับจาก Antivirus |
| | T1562.001 | Impair Defenses: Disable or Modify Tools | บังคับปิดการทำงาน (Terminate) ของโปรเซสและเซอร์วิสต่างๆ ที่เกี่ยวข้องกับซอฟต์แวร์ Antivirus และเครื่องมือป้องกันอื่นๆ |
| | T1070.001 | Indicator Removal: Clear Windows Event Logs | ปิดการทำงานของเซอร์วิส Event Log ของ Windows เพื่อลบร่องรอยและทำให้ทีมความปลอดภัยไม่สามารถตรวจสอบกิจกรรมที่เกิดขึ้นได้ |

| | | | |
|---|---|---|---|
| | T1490 | Inhibit System Recovery | ออกคำสั่งเพื่อลบ Volume Shadow Copies และทรัพยากรสำรองข้อมูลอื่นๆ เพื่อขัดขวางการกู้คืนระบบโดยไม่ใช้คีย์ถอดรหัส |
| Exfiltration | T1567 | Exfiltration Over Web Service | ขโมยและส่งข้อมูลที่ละเอียดอ่อนของเหยื่อออกไปยังเซิร์ฟเวอร์ของผู้โจมตีก่อนทำการเข้ารหัส (เป็นส่วนหนึ่งของ Double-Extortion) |
| Impact | T1486 | Data Encrypted for Impact | เข้ารหัสไฟล์ของเหยื่อด้วยอัลกอริทึม Curve25519 และ ChaCha20 แล้วเปลี่ยนนามสกุลเป็น .direwolf เพื่อเรียกค่าไถ่ |

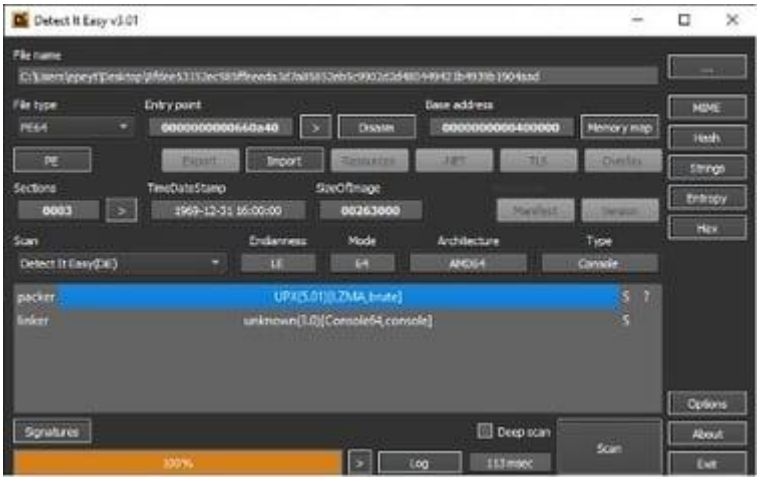
# เครื่องมือและมัลแวร์ (Tools and Malware)

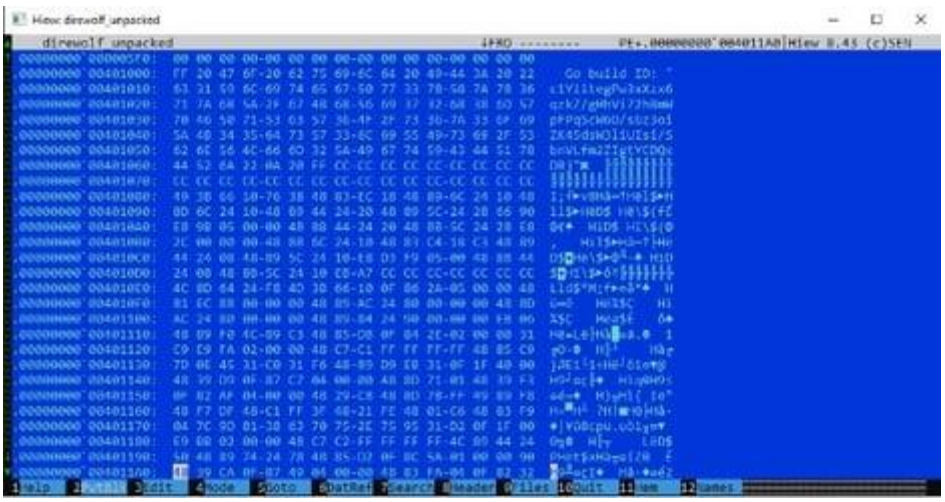
## Malware

หลังจากเจาะเข้าระบบได้สำเร็จ ผู้โจมตีจะทำการติดตั้งมัลแวร์หรือเพย์โหลดประเภทต่างๆ เพื่อบรรลุเป้าหมายที่ต้องการ

**Ransomware:**

ตัวอย่าง Ransomware ของ Dire Wolf ที่ได้มาจากบริการ Virustotal Hunting ของ Trustwave และพบว่าในเบื้องต้นถูกบีบอัด (packed) ด้วย UPX ซึ่งเป็นวิธีที่ผู้โจมตีนิยมใช้เพื่ออำพรางมัลแวร์และเป็นอุปสรรคต่อการวิเคราะห์เชิงสถิต (static analysis) เมื่อทำการคลายการบีบอัดแล้ว การวิเคราะห์ไฟล์ไบนารีก็พบว่ามันถูกเขียนขึ้นด้วยภาษา Go (Golang) ภาษา Go เป็นภาษาโปรแกรมแบบข้ามแพลตฟอร์ม (cross-platform) ที่ได้รับความนิยมเพิ่มขึ้นอย่างมากในหมู่อาชญากรไซเบอร์ เนื่องจากความสะดวกในการนำไปใช้งาน (portability) และความสามารถในการทำงานบนระบบปฏิบัติการต่างๆ ได้โดยมีการแก้ไขเพียงเล็กน้อย ผู้ผลิตโปรแกรม Anti-virus บางรายยังคงประสบปัญหาในการตรวจจับมัลแวร์ที่เขียนด้วยภาษา Go ซึ่งนี่ก็เป็นอีกเหตุผลหนึ่งที่ทำให้มันได้รับความนิยมในหมู่ผู้โจมตีเพิ่มขึ้น





[ภาพ unpacked ตัวอย่าง ransomware Dire Wolf]

**ตารางพารามิเตอร์ของ ransomware Dire Wolf**

| Parameter | Description |
|---|---|
| -h, -help | Display usage |
| -d <path> | Encrypts specific path |

**กระบวนการเข้ารหัส (Encryption)**

Ransomware สายพันธุ์นี้ใช้การผสมผสานระหว่างอัลกอริทึม Curve25519 และ ChaCha20 ในการเข้ารหัส และจะต่อท้ายไฟล์ที่ถูกเข้ารหัสด้วยนามสกุล “.direwolf”

แรนซัมแวร์จะเข้ารหัสไฟล์ทั้งหมดที่พบบนเครื่อง “**ยกเว้น**” ไฟล์ที่มีนามสกุลดังต่อไปนี้

- .exe
- .dll
- .sys
- .drv
- .bin
- .tmp
- .iso
- .img
- .direwolf

[ภาพตัวอย่าง ransom note ของ Dire Wolf Ransomware]

# Indicator of Compromise (IOCs)

Indicators of Compromise (IOCs) คือ ร่องรอยหรือหลักฐานทางดิจิทัลที่บ่งชี้ว่าระบบหรือเครือข่ายอาจถูกบุกรุกโดยผู้ไม่หวังดี ซึ่งทาง สกมช. ได้มีการแบ่งปันข้อมูล IOCs เหล่านี้ผ่านทางแพลตฟอร์ม MISP (Malware Information Sharing Platform) เพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์เรียบร้อยแล้ว

**Host-based IOCs**

**Filename:**

data345.exe

**SHA256:**

- 8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
- 27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3

**File extension: หลังถูกเข้ารหัส**

ชื่อไฟล์.direwolf

**Contact (TOX ID):**

B344BECDC01A1282F69CB82979F40439E15E1FD1EF1FE9748EE467F5869E2148E6F1E55959E2

# แนวทางการเฝ้าระวัง ป้องกัน และรับมือ

### *การเฝ้าระวัง (Monitoring)*

- เฝ้าระวังการใช้ PowerShell และ WMI: ตรวจสอบและเฝ้าระวังการเรียกใช้คำสั่ง PowerShell และ WMI ที่ผิดปกติ โดยเฉพาะคำสั่งที่มีความพยายามในการปิดการทำงานของเซอร์วิส (Service) ต่างๆ, การลบ Shadow Copies , หรือการยุ่งเกี่ยวกับระบบบันทึกเหตุการณ์ (Event Logs)
- ตรวจสอบความสมบูรณ์ของ Log: เนื่องจาก Dire Wolf มีพฤติกรรมพยายามปิดการทำงานของ Windows Event Log ควรมีการเฝ้าระวังแจ้งเตือนเมื่อระบบ Event Log หยุดทำงานหรือถูกแก้ไข และควรส่ง Log ที่สำคัญไปยังระบบจัดเก็บ Log ส่วนกลาง (Centralized Log Management) ที่มีความปลอดภัยสูง
- เฝ้าระวัง IOCs ในระบบ: นำข้อมูล Indicators of Compromise (IOCs) เช่น ค่าแฮช (SHA256) และชื่อไฟล์ (data345.exe) ไปใช้ในระบบตรวจจับภัยคุกคาม เช่น EDR (Endpoint Detection and Response) หรือ SIEM (Security Information and Event Management) เพื่อค้นหาและแจ้งเตือนร่องรอยการโจมตี
- ติดตามการเปลี่ยนแปลงของไฟล์: เฝ้าระวังการเปลี่ยนแปลงนามสกุลไฟล์เป็น .direwolf และการสร้างไฟล์เรียกค่าไถ่ HowToRecoveryFiles.txt บนระบบไฟล์เซิร์ฟเวอร์และเครื่องคอมพิวเตอร์ของผู้ใช้งาน
- วิเคราะห์ปริมาณข้อมูลขาออก (Outbound Traffic): เนื่องจากกลุ่มผู้โจมตีใช้วิธีขู่กรรโชกซ้ำซ้อน (Double-Extortion) โดยการขโมยข้อมูลออกไปก่อนเข้ารหัส ควรมีการเฝ้าระวังปริมาณข้อมูลขาออกที่สูงผิดปกติไปยังปลายทางที่ไม่รู้จัก เพื่อตรวจจับขั้นตอนการลักลอบนำข้อมูลออกไป (Exfiltration)

### *การป้องกัน (Prevention)*

- เสริมความแข็งแกร่งให้ Endpoint: ติดตั้งและปรับปรุงโปรแกรม Antivirus/EDR ที่มีความสามารถในการตรวจจับมัลแวร์ที่ถูกบีบอัดด้วย UPX และมัลแวร์ที่พัฒนาด้วยภาษา Golang พร้อมทั้งเปิดใช้งานคุณสมบัติป้องกันการแก้ไขหรือปิดการทำงานของโปรแกรม (Anti-tampering)
- จำกัดการใช้เครื่องมือของระบบ: จำกัดการใช้งาน PowerShell และ WMI สำหรับผู้ใช้งานทั่วไปที่ไม่จำเป็นต้องใช้ และใช้หลักการสิทธิ์น้อยที่สุด (Principle of Least Privilege) เพื่อลดผลกระทบหากบัญชีถูกยึดครอง
- สำรองข้อมูลอย่างสม่ำเสมอ: จัดทำนโยบายสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ โดยปฏิบัติตามกฎ 3-2-1 (มีข้อมูล 3 ชุด, เก็บในสื่อ 2 ชนิดที่แตกต่างกัน, และเก็บ 1 ชุดไว้นอกสถานที่หรือแบบออฟไลน์) เพื่อให้แน่ใจว่าสามารถกู้คืนข้อมูลได้ในกรณีที่ Shadow Copies ถูกลบ

- ปรับปรุงและอัปเดตแพตช์ (Patch Management): อัปเดตแพตช์ความปลอดภัยของระบบปฏิบัติการและซอฟต์แวร์ต่างๆ อย่างสม่ำเสมอ เพื่อลดช่องโหว่ที่ผู้โจมตีอาจใช้เป็นช่องทางในการเข้าสู่ระบบในขั้นตอนแรก
- สร้างความตระหนักรู้ให้ผู้ใช้งาน: จัดอบรมให้ความรู้แก่ผู้ใช้งานเกี่ยวกับภัยคุกคามจากแรนซัมแวร์ การสังเกตอีเมลหลอกลวง (Phishing) และแนวทางการปฏิบัติเมื่อต้องสงสัยว่าถูกโจมตี

### *การรับมือ (Response)*

- แยกอุปกรณ์ที่ติดเชื้อออกจากระบบเครือข่าย (Isolate): เมื่อตรวจพบการติดเชื้อ ให้รีบตัดการเชื่อมต่ออุปกรณ์ดังกล่าวออกจากเครือข่ายทันที (ทั้งสาย LAN และ Wi-Fi) เพื่อป้องกันการแพร่กระจายไปยังอุปกรณ์อื่น
- เก็บหลักฐานทางดิจิทัล (Preserve Evidence): ไม่ปิดเครื่องที่ติดเชื้อทันทีหากไม่จำเป็น และดำเนินการเก็บข้อมูลเพื่อการสืบสวนทางดิจิทัล (Digital Forensics) เช่น Memory dump และ Image ของดิสก์ เพื่อวิเคราะห์หาสาเหตุและขอบเขตความเสียหาย
- กู้คืนข้อมูลจากข้อมูลสำรอง (Restore from Backup): หลังจากยืนยันว่าได้กำจัดมัลแวร์ออกจากระบบทั้งหมดแล้ว ให้ทำการกู้คืนข้อมูลจากข้อมูลสำรองที่ตรวจสอบแล้วว่าปลอดภัยและไม่ติดเชื้อ
- ตรวจสอบและกำจัดภัยคุกคาม: ใช้ข้อมูล TTPs และ IOCs เพื่อตรวจสอบร่องรอยการโจมตีในระบบเครือข่ายทั้งหมด และกำจัดช่องทางที่ผู้โจมตีใช้ในการเข้าถึงและคงอยู่ (Persistence) ในระบบ
- รายงานเหตุการณ์: รายงานเหตุการณ์ละเมิดไปยังหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อรับการสนับสนุนและแจ้งเตือนหน่วยงานอื่นให้เฝ้าระวังต่อไป

# อ้างอิง (References)

1. Cyble Vision
2. MITRE ATT&CK
3. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors/

แบบประเมินรายงานข่าวกรองไซเบอร์

https://dg.th/nsexlfob51

จัดทำโดย

ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ สำนักประสานงาน
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทร: 02 114 3531 อีเมล: cti_misp@ncsa.or.th