Indicator of Compromise
เดือนกุมภาพันธ์ ปี 2025

คำนำ

จากการรวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) ในเดือนกุมภาพันธ์ ปี 2025 พบว่ามีการโจมตีที่เพิ่มขึ้นอย่างมีนัยสำคัญในหลายภาคส่วนฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ได้จัดทำรายงานสรุปผลการวิเคราะห์นี้ขึ้นเพื่อให้เห็นภาพรวมของข้อมูลสถานการณ์การโจมตีในเดือนกุมภาพันธ์ ปี 2025

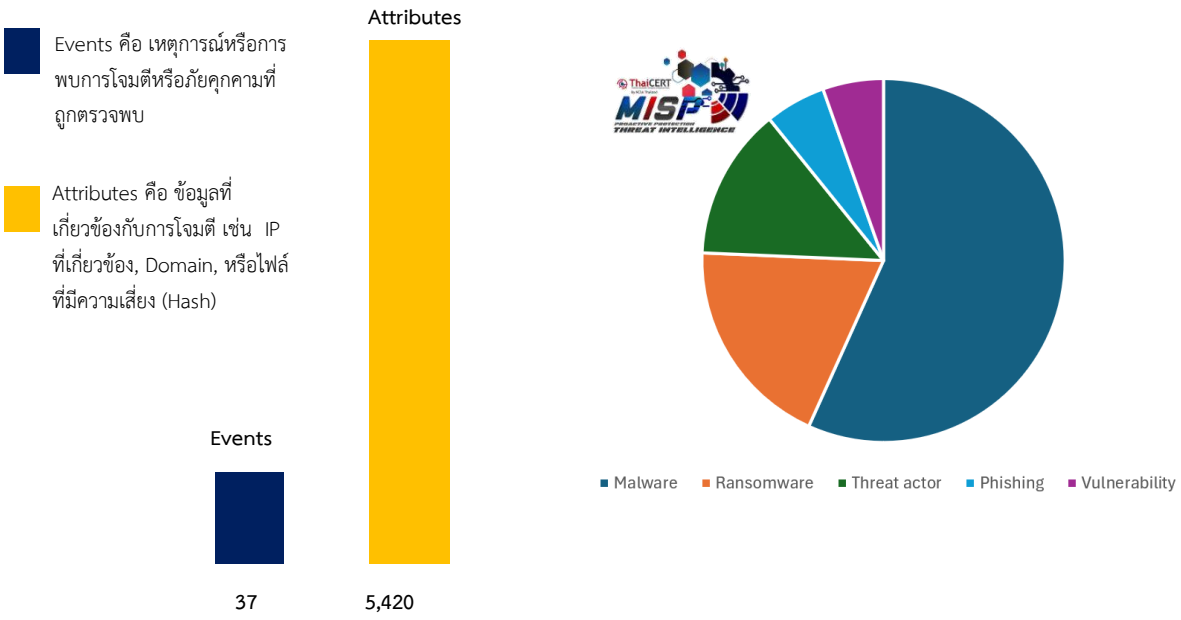
รายงานนี้มีวัตถุประสงค์เพื่อให้ข้อมูลที่เป็นประโยชน์แก่ผู้ที่เกี่ยวข้องในการป้องกันและรับมือกับการโจมตีจากภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพโดยเน้นถึงความสำคัญของการเตรียมความพร้อมและการตอบสนองต่อภัยคุกคามที่เกิดขึ้นอย่างรวดเร็วและมีประสิทธิภาพ

ทั้งนี้ หวังเป็นอย่างยิ่งว่ารายงานนี้จะเป็นประโยชน์ในการเสริมสร้างความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่กำลังเพิ่มขึ้นในปัจจุบัน รวมถึงวิธีการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์สำหรับทุกภาคส่วนได้อย่างมีประสิทธิภาพและปลอดภัย

ภาพรวม การวิเคราะห์ Indicator of Compromise (IoCs)

ในเดือนกุมภาพันธ์ ปี 2025 ในระบบ MISP

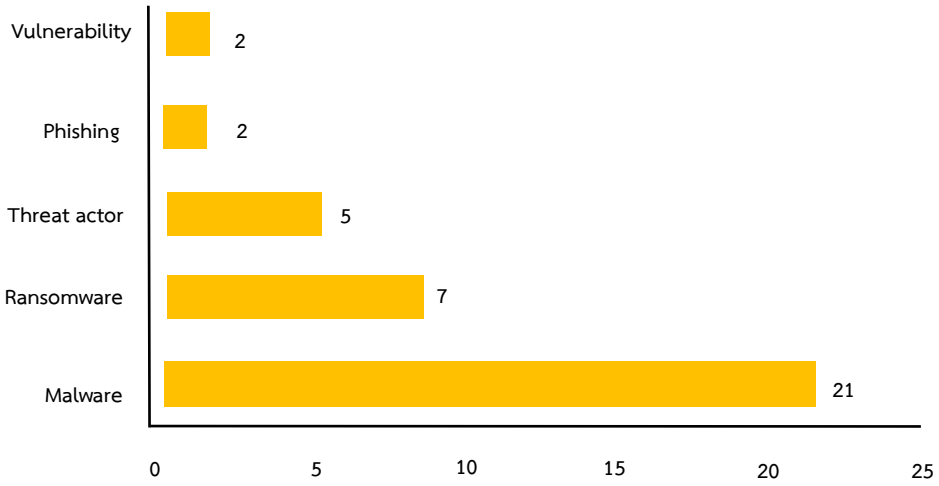
ในเดือนกุมภาพันธ์ ปี 2025 พบว่าสถิติการรวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) จากการโจมตีของภัยคุกคามทางไซเบอร์ มีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง ดังนั้น ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ จึงได้จัดประเภทหมวดหมู่ของ Indicator of Compromise (IoCs) ที่ได้วิเคราะห์ลงในระบบ MISP (Malware Information Sharing Platform and Threat Sharing) สำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์ เป็นดังนี้



จากภาพ แสดงให้เห็นว่า ในแต่ละ Events ที่ได้วิเคราะห์นั้น จะมี จำนวน Attributes ที่หลากหลายและแตกต่างกันไป ซึ่งในเดือนกุมภาพันธ์ ปี 2025 ได้รวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) จำนวน 37 Events และ 5,420 Attributes

ประเภทของภัยคุกคามทางไซเบอร์ ที่ได้จากการวิเคราะห์ Indicator of Compromise (IoCs) ในเดือนกุมภาพันธ์ ปี 2025

แบ่งออกเป็น 5 ประเภทดังนี้



จัดลำดับ ดังนี้

- ลำดับที่ 1 Malware 21 จำนวน
- ลำดับที่ 2 Ransomware 7 จำนวน
- ลำดับที่ 3 Threat actor 5 จำนวน
- ลำดับที่ 4 Phishing 2 จำนวน

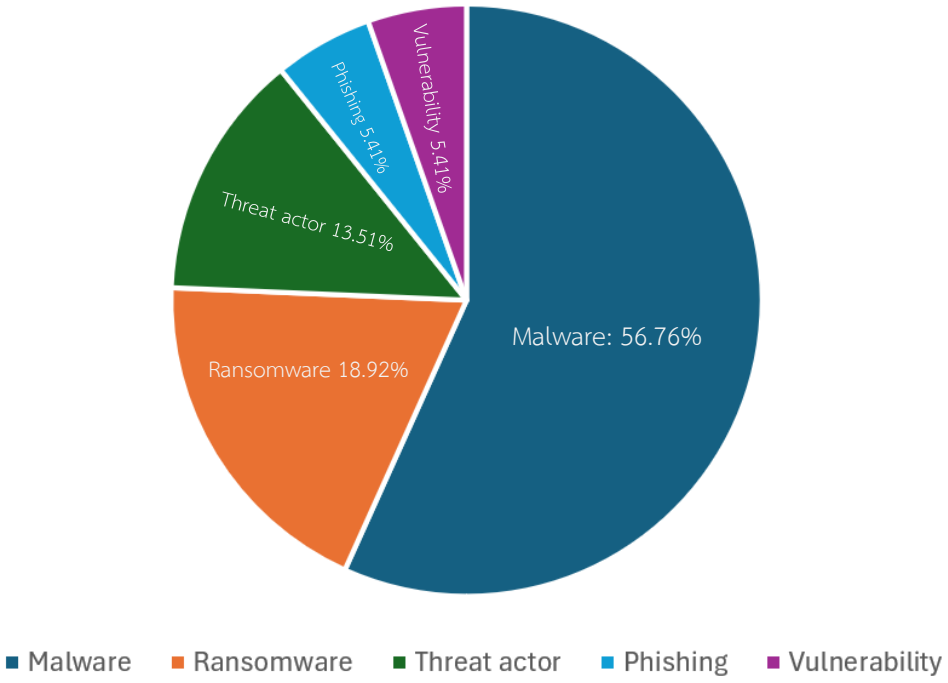
อื่น ๆ

- Vulnerability 2 จำนวน

Malware เป็นประเภทที่พบมากที่สุด (มากกว่าครึ่งหนึ่งของทั้งหมด) ตามด้วย Ransomware และ Threat actor ก็นับเป็นกลุ่มที่มีสัดส่วนสูง ประเภททั่วไป เช่น Vulnerability มีจำนวนค่อนข้างน้อย

ประเภทของภัยคุกคามทางไซเบอร์ ที่ได้จากการวิเคราะห์ Indicator of Compromise (IoCs) ในเดือนกุมภาพันธ์ ปี 2025

สรุปภาพรวมดังนี้



จากภาพ สรุปได้ว่า จำนวน Malware ที่ได้ถูกรวบรวมและวิเคราะห์ข้อมูล Indicator of Compromise (IoCs) ในเดือนมกราคม ปี 2025 นั้น มีจำนวนที่สูงที่สุด เป็นเปอร์เซ็นที่ 56.76% ต่อด้วยจำนวน Ransomware เป็นเปอร์เซ็นที่ 18.92% ตามมาด้วยจำนวน Threat actor เป็นเปอร์เซ็นที่ 13.51%, Phishing เป็นเปอร์เซ็นที่ 5.41%, และ Vulnerability 5.41%

ภัยคุกคามที่น่าสนใจจากการวิเคราะห์ลงระบบ MISP

ประจำเดือน กุมภาพันธ์ 2025

Lynx ransomware

ได้ค้นพบมัลแวร์เรียกค่าไถ่ตัวใหม่ชื่อ Lynx ซึ่งเป็นทายาทของ INC ransomware กลุ่มที่อยู่เบื้องหลัง Lynx ได้มุ่งเป้าโจมตีองค์กรในหลายภาคส่วน เช่น ค้าปลีก อสังหาริมทรัพย์ สถาปัตยกรรม การเงิน และบริการด้านสิ่งแวดล้อม ในสหรัฐอเมริกาและสหราชอาณาจักร

ความเชื่อมโยงระหว่าง Lynx และ INC Ransomware

Lynx ransomware มีส่วนแบ่งของซอร์สโค้ดร่วมกับ INC ransomware อย่างมีนัยสำคัญ INC ransomware ปรากฏครั้งแรกในเดือนสิงหาคม 2023 และมีเวอร์ชันที่รองรับทั้ง Windows และ Linux แม้ว่าในปัจจุบันจะยังไม่มีการยืนยันตัวอย่างของ Lynx บนระบบ Linux แต่มีการพบตัวอย่างบนระบบ Windows ทั้งนี้ Lynx ransomware ดำเนินการในรูปแบบ Ransomware-as-a-Service (RaaS)

กลไกการแพร่กระจาย

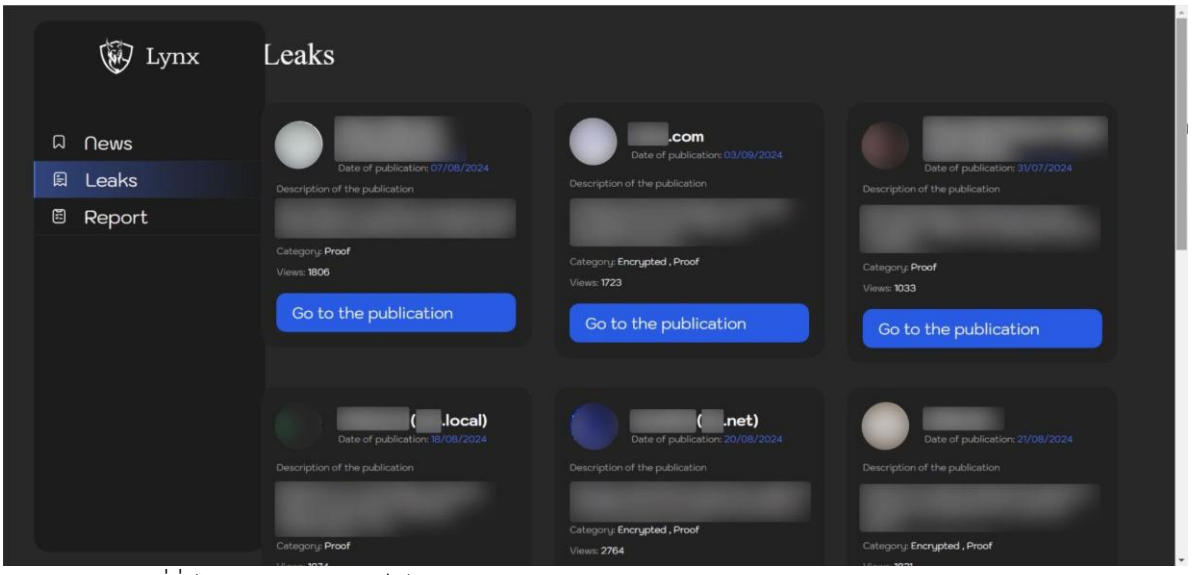
กลุ่มที่อยู่เบื้องหลัง Lynx ransomware ใช้กลยุทธ์การขู่กรรโชกสองชั้น (double extortion) ที่ซับซ้อน พวกเขาแพร่กระจายมัลแวร์ผ่านหลายวิธี เช่น

- อีเมลฟิชชิ่งที่หลอกลวงให้ผู้ใช้เปิดเผยข้อมูลสำคัญ
- การดาวน์โหลดที่เป็นอันตรายซึ่งติดตั้งมัลแวร์โดยไม่รู้ตัว
- ฟอรัมแฮ็กเกอร์ที่แบ่งปันข้อมูลและทรัพยากร

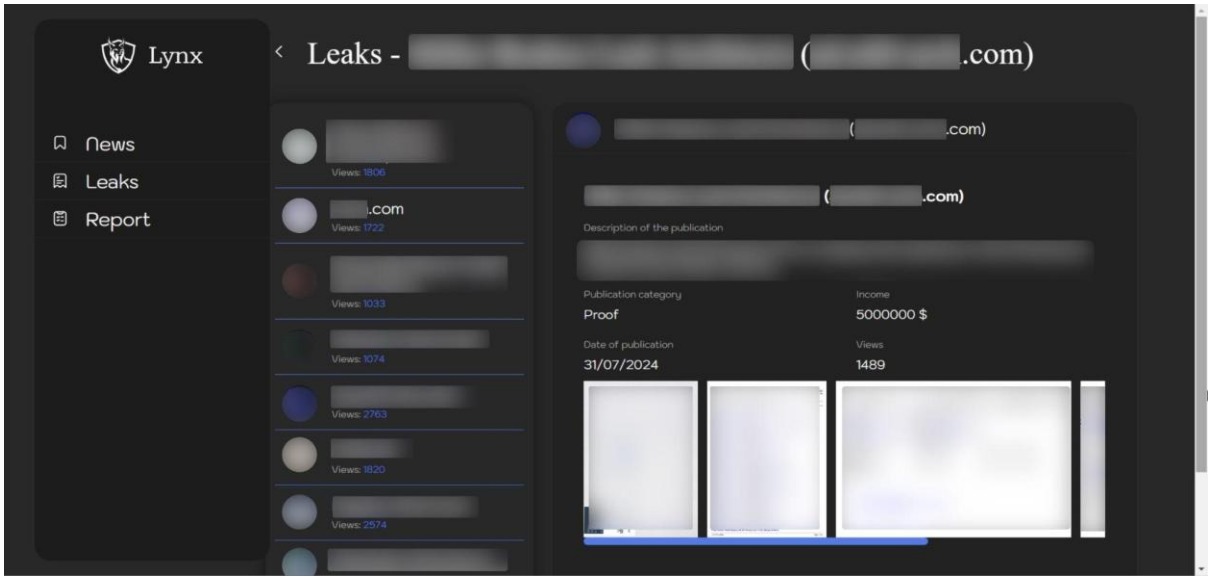
กลยุทธ์ double extortion ของ Lynx ransomware คือการขโมยข้อมูลของเหยื่อก่อนที่จะเข้ารหัส ซึ่งนอกจากจะทำให้ข้อมูลไม่สามารถเข้าถึงได้แล้ว ยังเปิดโอกาสให้กลุ่มมัลแวร์เผยแพร่หรือขายข้อมูลหากเหยื่อไม่จ่ายค่าไถ่

เว็บไซต์เผยแพร่ข้อมูลที่ถูกขโมย

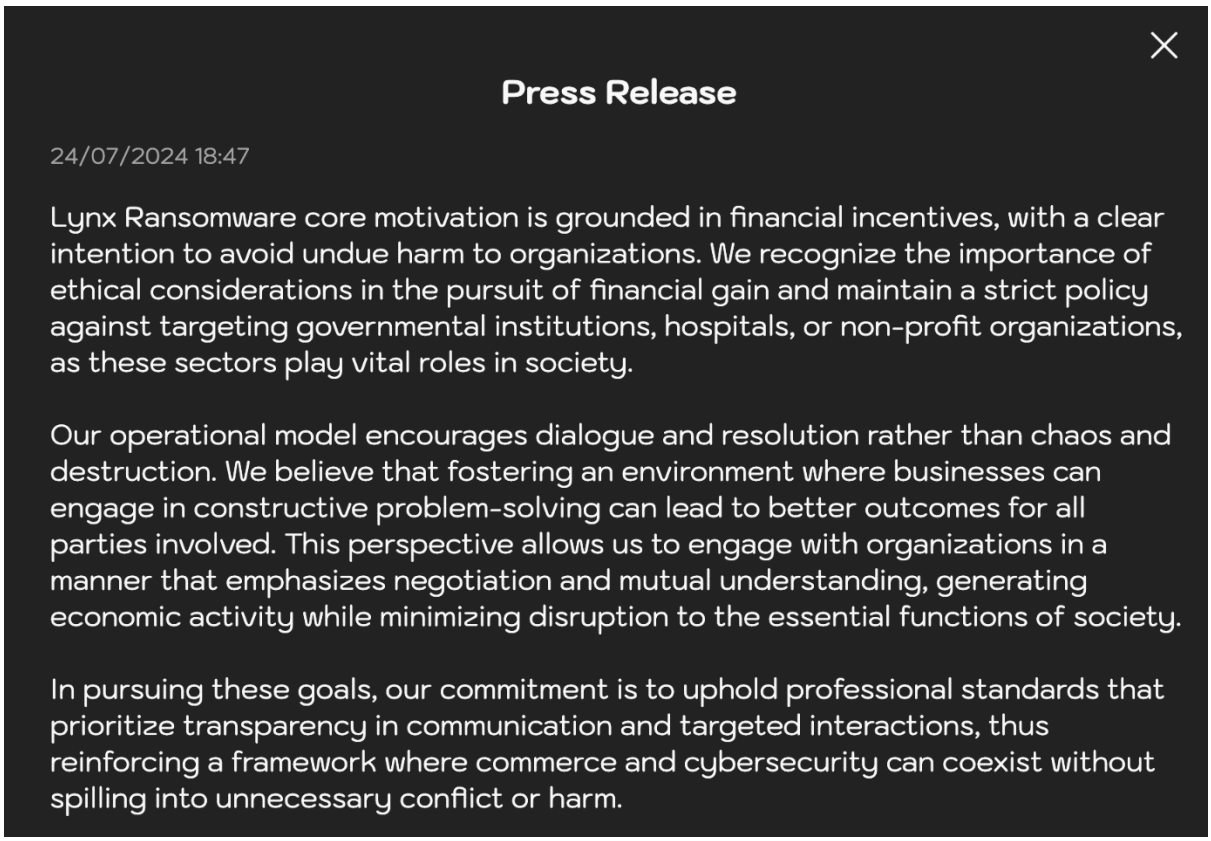
กลุ่ม Lynx อ้างว่าพวกเขาได้ละเมิดข้อมูลจากหลายบริษัท และได้แสดงข้อมูลที่ถูกขโมยบนเว็บไซต์ของพวกเขาที่ http[:]//lynxblog[.]net



รูปภาพ ข้อมูลที่รั่วไหลเผยแพร่บนเว็บไซต์ Lynx ransomware



รูปภาพ ข้อมูลที่รั่วไหลพร้อมรายได้รวมวันที่และขนาดของข้อมูล



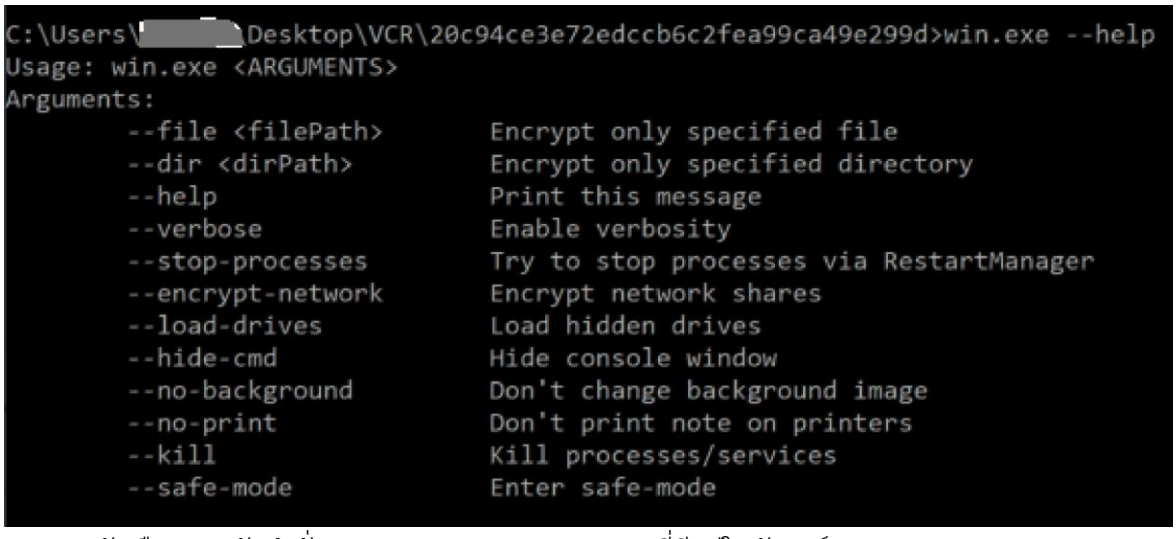
รูปภาพ แถลงการณ์ของ Lynx Ransomware (24 กรกฎาคม 2024 - 18:47)

ผลการวิเคราะห์มัลแวร์

ตัวอย่างของ Lynx Ransomware ที่ถูกวิเคราะห์ใช้ AES-128 ในโหมด CTR และ Curve25519 Donna ในการเข้ารหัสข้อมูล

- ไฟล์ทั้งหมดที่ถูกเข้ารหัสจะถูกเติม นามสกุล .lynx ต่อท้าย
- มัลแวร์เวอร์ชันนี้ออกแบบมา สำหรับระบบปฏิบัติการ Windows
- เขียนขึ้นด้วย ภาษา C++

ผู้โจมตีสามารถปรับแต่งการทำงานของ Lynx Ransomware ได้โดยใช้ พารามิเตอร์ที่กำหนดขณะรันมัลแวร์ ซึ่งช่วยให้พวกเขาควบคุมและกำหนดพฤติกรรมของมัลแวร์ตามต้องการ



รูปภาพ ตัวเลือกบรรทัดคำสั่ง (Command-line options) ที่มีอยู่ในมัลแวร์

คุณสมบัติของแรนซัมแวร์ Lynx มีดังนี้

- กำหนดไดเรกทอรี/ไฟล์ที่ต้องการเข้ารหัส
- ยุติ (Terminate) บริการหรือโปรเซสที่ทำงานอยู่
- เข้ารหัสไดรฟ์ที่เชื่อมต่อผ่านเครือข่าย
- เมานต์ (Mount) ดิสก์ที่ถูกซ่อนไว้
- เปิดหรือปิดการเปลี่ยนภาพพื้นหลังของระบบ
- บันทึกและแสดงผลล็อกทั้งหมดบนคอนโซล

โค้ดตัวอย่างแสดงพารามิเตอร์ต่าง ๆ ที่ใช้กับ Lynx Ransomware มัลแวร์นี้สามารถ โหลดไดรฟ์ที่ถูกซ่อนไว้ และเข้ารหัสไดรฟ์ที่แชร์ผ่านเครือข่ายได้

```
.text:00407723 E8 08 9C FF FF                  call    sub_401330
.text:00407728 68 B8 4D 42 00                  push    offset aFileFilepathEn ; "\t--file <filePath> \tEncrypt only spec"...
.text:0040772D E8 FE 9B FF FF                  call    sub_401330
.text:00407732 68 EC 4D 42 00                  push    offset aDirDirpathEncr ; "\t--dir <dirPath> \tEncrypt only specif"...
.text:00407737 E8 F4 9B FF FF                  call    sub_401330
.text:0040773C 68 20 4E 42 00                  push    offset aHelpPrintThisM ; "\t--help \t\t\tPrint this message\n"
.text:00407741 E8 EA 9B FF FF                  call    sub_401330
.text:00407746 68 40 4E 42 00                  push    offset aVerboseEnableV ; "\t--verbose \t\tEnable verbosity\n"
.text:0040774B E8 E0 9B FF FF                  call    sub_401330
.text:00407750 68 60 4E 42 00                  push    offset aStopProcessesT ; "\t--stop-processes \tTry to stop proces"...
.text:00407755 E8 D6 9B FF FF                  call    sub_401330
.text:0040775A 68 A0 4E 42 00                  push    offset aEncryptNetwork_0 ; "\t--encrypt-network \tEncrypt network s"...
.text:0040775F E8 CC 9B FF FF                  call    sub_401330
.text:00407764 68 CC 4E 42 00                  push    offset aLoadDrivesLoad ; "\t--load-drives \t\tLoad hidden drives"...
.text:00407769 E8 C2 9B FF FF                  call    sub_401330
.text:0040776E 68 F4 4E 42 00                  push    offset aHideCmdHideCon ; "\t--hide-cmd \t\tHide console window\n"
.text:00407773 E8 B8 9B FF FF                  call    sub_401330
.text:00407778 68 18 4F 42 00                  push    offset aNoBackgroundDo ; "\t--no-background \tDon't change backgr"...
.text:0040777D E8 AE 9B FF FF                  call    sub_401330
.text:00407782 68 4C 4F 42 00                  push    offset aNoPrintDonTPri ; "\t--no-print \t\tDon't print note on pr"...
.text:00407787 E8 A4 9B FF FF                  call    sub_401330
.text:0040778C 68 78 4F 42 00                  push    offset aKillKillProces ; "\t--kill \t\t\tKill processes/services"...
.text:00407791 E8 9A 9B FF FF                  call    sub_401330
.text:00407796 68 9C 4F 42 00                  push    offset aSafeModeEnterS ; "\t--safe-mode \t\tEnter safe-mode\n"
```

รูปภาพ Encryption mode ของมัลแวร์

หากไม่ระบุพารามิเตอร์ใด ๆ แรนซัมแวร์จะทำการเข้ารหัสไฟล์และไดรฟ์ทั้งหมดในระบบโดยอัตโนมัติ นอกจากนี้ ยังลบสำเนาเงาและไดรฟ์พาร์ติชันสำหรับแบ็คอัพตามที่แสดงไว้

```
C:\Users\[redacted]\Desktop\[redacted]\20c94ce3e72edccb6c2fea99ca49e299d>win.exe --verbose
Settings:
        [-] Try to stop processes via RestartManager
        [-] Encrypt network shares
        [-] Load hidden drives
        [-] Kill processes and services
        [-] Enter safe-mode

[+] Successfully decoded readme!
[+] Threads are initialized!
[+] Recycling bin...
[*] Starting full encryption in 5s.....
[+] Found drive: \\?\C:\
[+] Successfully delete shadow copies from C:/
[+] Encrypting: \\?\C:\$GetCurrent\Logs\downlevel_2023_04_12_17_47_09_172.log
[+] Encrypting: \\?\C:\$GetCurrent\Logs\oobe_2023_04_12_20_44_50_152.log
[+] Encrypting: \\?\C:\$GetCurrent\Logs\PartnerSetupCompleteResult.log
[+] Encrypting: \\?\C:\$GetCurrent\SafeOS\GetCurrentRollback.ini
[+] Encrypting: \\?\C:\$GetCurrent\SafeOS\PartnerSetupComplete.cmd
[+] Encrypting: \\?\C:\$GetCurrent\SafeOS\preoobe.cmd
[+] Encrypting: \\?\C:\$GetCurrent\SafeOS\SetupComplete.cmd
[+] Encrypting: \\?\C:\$WINRE_BACKUP_PARTITION.MARKER
[+] Encrypting: \\?\C:\MSOCache\All Users\{90140000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.
[+] Encrypting: \\?\C:\MSOCache\All Users\{90140000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI
```

รูปภาพ รันตัวอย่าง Lynx Ransomware ด้วยค่าพารามิเตอร์เริ่มต้นในหน้าต่างคำสั่ง (Command Terminal)

จากผลการดีบักในรูป พบว่าแรนซัมแวร์จะ สแกนไดรฟ์ทั้งหมดในระบบ พยายาม เมานต์ไดรฟ์เหล่านั้น จากนั้น เข้ารหัสข้อมูลที่อยู่ภายใน

```
33 FF                                   xor     edi, edi
C7 85 84 FB FF FF 30 51 42 00           mov     [ebp+lpRootPathName], offset aQ ; "Q:\\"
C7 85 88 FB FF FF 38 51 42 00           mov     [ebp+var_478], offset aW ; "W:\\"
33 F6                                   xor     esi, esi
C7 85 8C FB FF FF 40 51 42 00           mov     [ebp+var_474], offset aE ; "E:\\"
C7 85 90 FB FF FF 48 51 42 00           mov     [ebp+var_470], offset aR ; "R:\\"
C7 85 94 FB FF FF 50 51 42 00           mov     [ebp+var_46C], offset aT ; "T:\\"
C7 85 98 FB FF FF 58 51 42 00           mov     [ebp+var_468], offset aY ; "Y:\\"
C7 85 9C FB FF FF 60 51 42 00           mov     [ebp+var_464], offset aU ; "U:\\"
C7 85 A0 FB FF FF 68 51 42 00           mov     [ebp+var_460], offset aI ; "I:\\"
C7 85 A4 FB FF FF 70 51 42 00           mov     [ebp+var_45C], offset aO ; "O:\\"
C7 85 A8 FB FF FF 78 51 42 00           mov     [ebp+var_458], offset aP ; "P:\\"
C7 85 AC FB FF FF 80 51 42 00           mov     [ebp+var_454], offset aA ; "A:\\"
C7 85 B0 FB FF FF 88 51 42 00           mov     [ebp+var_450], offset aS ; "S:\\"
C7 85 B4 FB FF FF 90 51 42 00           mov     [ebp+var_44C], offset aD ; "D:\\"
C7 85 B8 FB FF FF 98 51 42 00           mov     [ebp+var_448], offset asc_425198 ; "F:\\"
C7 85 BC FB FF FF A0 51 42 00           mov     [ebp+var_444], offset aG ; "G:\\"
C7 85 C0 FB FF FF A8 51 42 00           mov     [ebp+var_440], offset asc_4251A8 ; "H:\\"
C7 85 C4 FB FF FF B0 51 42 00           mov     [ebp+var_43C], offset aJ ; "J:\\"
C7 85 C8 FB FF FF B8 51 42 00           mov     [ebp+var_438], offset aK ; "K:\\"
C7 85 CC FB FF FF C0 51 42 00           mov     [ebp+var_434], offset asc_4251C0 ; "L:\\"
C7 85 D0 FB FF FF C8 51 42 00           mov     [ebp+var_430], offset aZ ; "Z:\\"
C7 85 D4 FB FF FF D0 51 42 00           mov     [ebp+var_42C], offset asc_4251D0 ; "X:\\"
C7 85 D8 FB FF FF D8 51 42 00           mov     [ebp+var_428], offset aC ; "C:\\"
C7 85 DC FB FF FF E0 51 42 00           mov     [ebp+var_424], offset aV ; "V:\\"
C7 85 E0 FB FF FF E8 51 42 00           mov     [ebp+var_420], offset aB ; "B:\\"
C7 85 E4 FB FF FF F0 51 42 00           mov     [ebp+var_41C], offset aN ; "N:\\"
C7 85 E8 FB FF FF F8 51 42 00           mov     [ebp+var_418], offset aM ; "M:\\"
89 BD F0 FB FF FF                       mov     [ebp+cchReturnLength], edi
0F 1F 40 00                             nop     dword ptr [eax+00h]
0F 1F 84 00 00 00 00 00                 nop     dword ptr [eax+eax+00000000h]
```

รูปภาพ ตัวอย่าง Lynx Ransomware กำลังตรวจสอบตัวอักษรไดรฟ์ (Drive Letters)

ก่อนเริ่มกระบวนการเข้ารหัส ตัวอย่างของ Lynx Ransomware จะ ยุติ (Kill) โปรเซสที่ทำงานอยู่ในระบบ ตามรายการที่กำหนดไว้

```
.rdata:00424C34                                         ; "sql"
.rdata:00424C38                 dd offset aVeeam        ; "veeam"
.rdata:00424C3C                 dd offset aBackup       ; "backup"
.rdata:00424C40                 dd offset aExchange     ; "exchange"
.rdata:00424C44                 dd offset aJava         ; "java"
.rdata:00424C48                 dd offset aNotepad      ; "notepad"
```

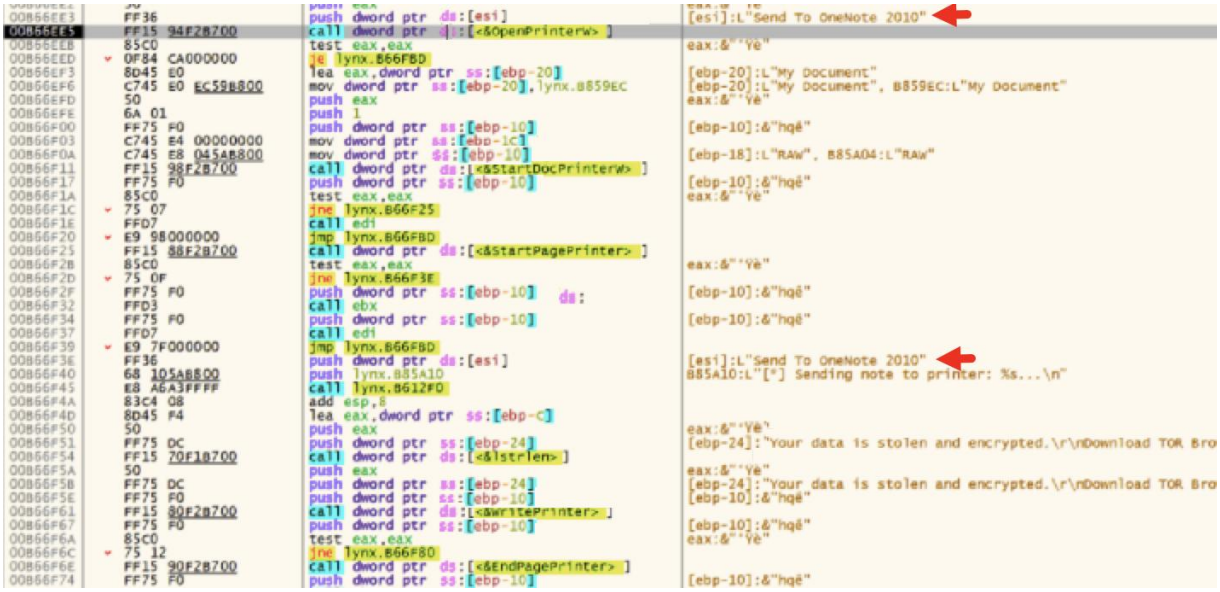
รูปภาพ Lynx กำลังตรวจสอบโปรเซสต่าง ๆ ในระบบ

รูปภาพ ตัวอย่างโค้ดสำหรับตรวจสอบและยุติโปรเซส (Process Checking & Termination)

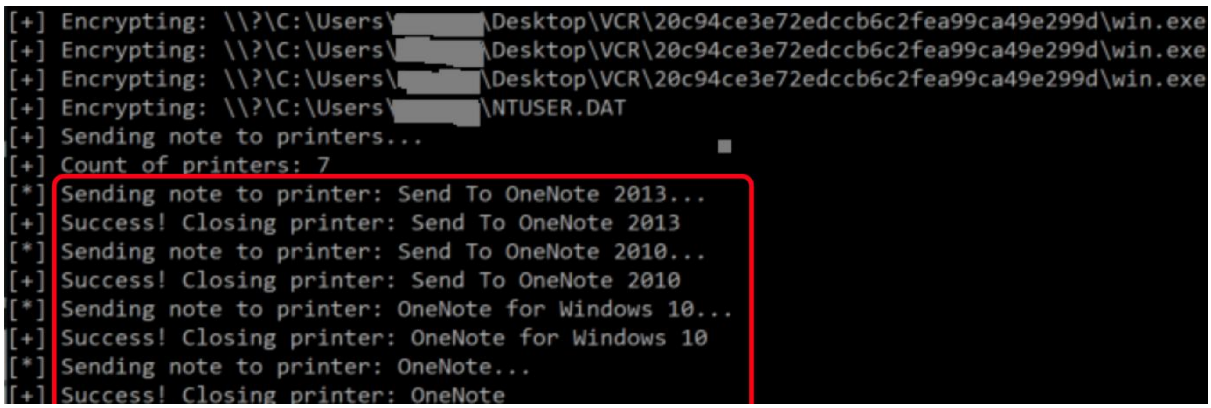
Lynx Ransomware ใช้ Restart Manager API (RstrtMgr) เพื่อเพิ่มประสิทธิภาพการเข้ารหัสและสร้างผลกระทบสูงสุดต่อระบบของเหยื่อ

- โดยการใช้ RstrtMgr ในกระบวนการโจมตี Lynx สามารถเข้ารหัสไฟล์ที่กำลังถูกใช้งานหรือถูกล็อกโดยแอปพลิเคชันอื่น
- RstrtMgr ช่วยให้แรนซัมแวร์ระบุได้ว่าไฟล์ใดกำลังถูกใช้งาน และสามารถปิดแอปพลิเคชันที่ล็อกไฟล์นั้น เพื่อดำเนินการเข้ารหัสได้
- เทคนิคนี้เคยถูกใช้โดย แรนซัมแวร์ Conti, Cactus และ BiBi Wiper เช่นกัน

หลังจากที่แรนซัมแวร์เข้ารหัสไฟล์ทั้งหมดเสร็จแล้วมันจะพยายาม พิมพ์รายงานผ่าน Microsoft OneNote ตามที่แสดงในผลการดีบัก

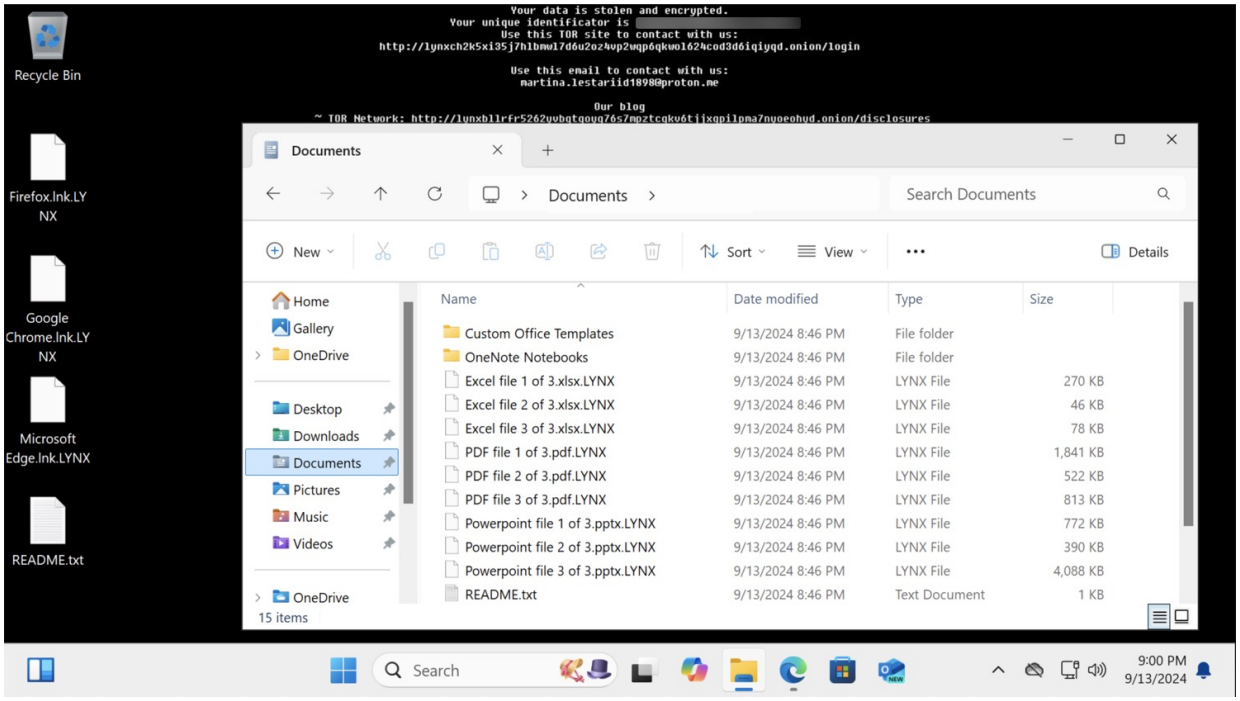


รูปภาพ ผลการดีบักแสดงให้เห็นว่า ตัวอย่างของ Lynx Ransomware กำลังส่งบันทึกไปยัง OneNote



รูปภาพ หลังจากรัน Lynx Ransomware ผ่าน Command Line ผลลัพธ์แสดงให้เห็นว่า มันส่งบันทึกไปยัง OneNote หลังจากเสร็จสิ้นกระบวนการเข้ารหัส

ด้านล่างแสดงให้เห็นว่าแรนซัมแวร์เพิ่มนามสกุล .lynx ต่อท้ายชื่อไฟล์ที่ถูกเข้ารหัสทั้งหมด

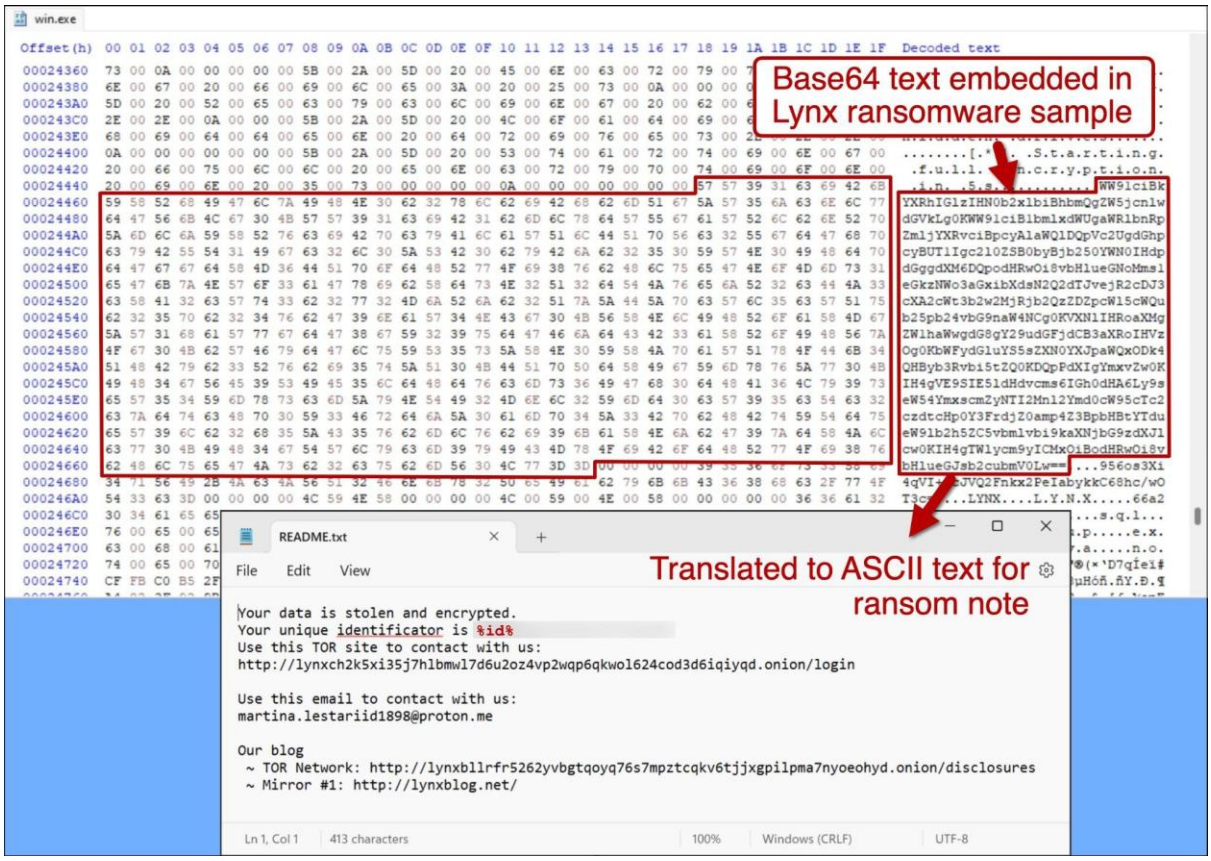


รูปภาพ หน้าจอเดสก์ท็อปจากระบบที่ติด Lynx Ransomware โดยไฟล์ที่ถูกเข้ารหัสจะมีนามสกุล .lynx ต่อท้าย

การพบเส้นทางของ Program Database (PDB) ที่มีชื่อ "Lynx" ยืนยันว่าแรนซัมแวร์นี้เป็นเวอร์ชันหนึ่งของ Lynx ตามที่แสดงในผลลัพธ์ของ เครื่องมือวิเคราะห์ไฟล์ปฏิบัติการ (PE Analyzer Tool)

รูปภาพ Lynx sample .pdb path

Lynx ยังสร้างไฟล์ README.txt เป็นข้อความเรียกค่าไถ่ ภาพแสดงเนื้อหาที่ถูกเข้ารหัสแบบ Base64 ในส่วนข้อมูลตัวอย่างของ Lynx Ransomware และข้อความเรียกค่าไถ่ที่ถูกถอดรหัสแล้ว



รูปภาพ ข้อความเรียกค่าไถ่ที่ถูกเข้ารหัสแบบ Base64 จากตัวอย่าง Lynx Ransomware และข้อความเรียกค่าไถ่ที่ถูกถอดรหัสแล้ว

Indicator of compromise (IoCs)

Indicator of compromise (IoCs) คือ หลักฐานทางนิติวิทยาศาสตร์ของการบุกรุกที่อาจเกิดขึ้นในระบบโฮสต์หรือเครือข่ายและผู้ดูแล ระบบสามารถตรวจจับความพยายามในการบุกรุกหรือกิจกรรมที่เป็นอันตรายอื่น ๆ

Filename

- svhost.exe

Hash

- c468e34eafc037eb563b245fb751310a90bab35c
- 6012a489883017a92c3745f267be6b49228e2ff41ae749d127b1f6fa78152aaf
- 571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
- 82eb1910488657c78bef6879908526a2a2c6c31ab2f0517fcc5f3f6aa588b513
- 31de5a766dca4eaae7b69f807ec06ae14d2ac48100e06a30e17cc9acccfd5193
- 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e
- 432f549e9a2a76237133e9fe9b11fbb3d1a7e09904db5ccace29918e948529c6
- 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
- 4e5b9ab271a1409be300e5f3fd90f934f317116f30b40eddc82a4dfd18366412
- 571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
- 589ff3a5741336fa7c98dbcef4e8aecea347ea0f349b9949c6a5f6cd9d821a2
- 80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441
- 85699c7180ad77f2ede0b15862bb7b51ad9df0478ed394866ac7fa9362bf568
- 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0
- 9a47ab27d50df1faba1dc5777bdcfff576524424bc4a3364d33267bbcf8a3896
- b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee
- d5ca3e0e25d768769e4afda209aca1f563768dae79571a38e3070428f8adf031
- eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
- ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49
- f71fc818362b1465fc1deb361de36badc73ac4dd9e815153c9022f82c4062787

MITRE ATT&CK

คือ กลยุทธ์ เทคนิค และกระบวนการทำงาน หรือเรียกว่า TTP (Tactics, Technique และ Procedures) ของแฮกเกอร์ที่ใช้ในการโจมตีองค์กรต่างๆ ทั่วโลก โดยจะมี MITRE ATT&CK ที่เกี่ยวข้องดังนี้

Technique Title	ID
Access Token Manipulation	T1134
System Information Discovery	T1082
Virtualization/Sandbox Evasion: System Checks	T1497.001
Hide Artifacts: Hidden Window	T1564.003
System Location Discovery: System Language Discovery	T1614.001
Virtualization/Sandbox Evasion: Time Based Evasion	T1497.003
Service Stop	T1489
Data Encrypted for Impact	T1486
Defacement: Internal Defacement	T1491.001
Hide Artifacts: Hidden Files and Directories	T1564.001
Peripheral Device Discovery	T1120
Native API	T1106
Process Discovery	T1057
Debugger Evasion	T1622
Inhibit System Recovery	T1490
System Time Discovery	T1124
Network Share Discovery	T1135
Query Registry	T1012
Data from Local System	T1005
Screen Capture	T1113
Modify Registry	T1112
System Service Discovery	T1007
File and Directory Discovery	T1083
Command and Scripting Interpreter: Window	T1059.003

คำแนะนำ

1. มาตรการป้องกัน (Prevention)

1.1) สำรองข้อมูลอย่างสม่ำเสมอ (Regular Backup)

- สำรองข้อมูลไว้ บนอุปกรณ์ที่แยกจากระบบหลัก (Offline Backup) หรือ บน Cloud ที่ปลอดภัย
- ตรวจสอบว่า ไฟล์สำรองสามารถกู้คืนได้จริง

1.2) อัปเดตซอฟต์แวร์และระบบปฏิบัติการ (Patch & Update)

- ติดตั้ง แพตช์ความปลอดภัย และอัปเดตระบบปฏิบัติการเป็นเวอร์ชันล่าสุด
- ปิด Remote Desktop Protocol (RDP) หากไม่มีความจำเป็น

1.3) เสริมความปลอดภัยของบัญชีผู้ใช้ (Account Security)

- เปิดใช้งาน Multi-Factor Authentication (MFA)
- ใช้รหัสผ่านที่แข็งแรงและไม่ซ้ำกันในแต่ละบัญชี

1.4) ตรวจจับและป้องกันภัยคุกคาม (Threat Detection & Protection)

- ใช้ Endpoint Detection & Response (EDR) หรือ Next-Gen Antivirus (NGAV)
- เปิดใช้งาน Windows Defender หรือ Security Software อื่น ๆ
- ใช้ Firewall และ Intrusion Detection System (IDS) เพื่อตรวจจับกิจกรรมที่น่าสงสัย

1.5) เฝ้าระวังพฤติกรรมต้องสงสัย (User Awareness & Monitoring)

- ฝึกอบรมให้พนักงานรู้จัก Phishing และ Social Engineering Attacks
- หลีกเลี่ยงการเปิดไฟล์แนบจากอีเมลที่ไม่รู้จัก
- ใช้ Application Whitelisting เพื่อลดความเสี่ยงจากการรันไฟล์ที่ไม่พึงประสงค์

2. มาตรการรับมือเมื่อถูกโจมตี (Incident Response)

2.1) ตัดการเชื่อมต่อจากเครือข่าย (Isolate Infected Systems)

- ถอดปลั๊กเครื่องที่ติดไวรัส จากเครือข่ายทันที
- ปิด Wi-Fi และ Bluetooth เพื่อป้องกันการแพร่กระจาย

2.2) ระบุขอบเขตของการโจมตี (Identify & Assess Impact)

- ตรวจสอบ ไฟล์ที่ถูกเข้ารหัส และดูว่ามีไฟล์ที่ถูกลบหรือถูกเปลี่ยนชื่อหรือไม่
- วิเคราะห์ ไฟล์ล็อกและพฤติกรรมของมัลแวร์

2.3) พยายามกู้คืนข้อมูล (Attempt Data Recovery)

- หากมี Backup ให้ใช้สำเนาที่ปลอดภัยเพื่อกู้คืนข้อมูล
- ทดลองใช้ Ransomware Decryption Tools ที่มีอยู่ เช่นจาก No More Ransom (nomoreransom.org)

2.4) ห้ามจ่ายค่าไถ่ (Do Not Pay Ransom)

- การจ่ายค่าไถ่ ไม่รับประกันว่าจะได้ข้อมูลคืน และยังสนับสนุนอาชญากรไซเบอร์
- รายงานเหตุการณ์ไปยังหน่วยงานที่เกี่ยวข้อง เช่น CERT หรือตำรวจไซเบอร์

2.5) กำจัดมัลแวร์และเสริมความปลอดภัย (Remove Malware & Strengthen Security)

- ใช้ Malware Removal Tools เพื่อล้างระบบ
- ปรับนโยบายด้านความปลอดภัย เพื่อป้องกันการโจมตีในอนาคต
- ตรวจสอบว่า Shadow Copies และ System Restore Points ถูกลบไปหรือไม่

2.6) แจ้งเตือนและแบ่งปันข้อมูล (Report & Share Intel)

- แจ้งให้พนักงานและหน่วยงานที่เกี่ยวข้องรับทราบเพื่อป้องกันการโจมตีซ้ำ
- แบ่งปันข้อมูล Indicators of Compromise (IoCs) กับแพลตฟอร์ม Threat Intelligence เช่น MISP

แนวทางการป้องกันและรับมือภัยคุกคามทางไซเบอร์

การป้องกันและรับมือกับภัยคุกคามไซเบอร์ที่มีความหลากหลาย เช่น Malware, Ransomware, Threat Actors, Tool-based Attacks, Vulnerabilities, Phishing, Campaign Attacks, และ Data Leaks จำเป็นต้องมีแนวทางที่ครอบคลุมและสอดคล้องกับประเภทของภัยคุกคามนั้น ๆ ด้านล่างนี้ คือแนวทางที่สามารถนำไปปรับใช้ได้

1. Malware

- ป้องกัน:
  - ใช้ซอฟต์แวร์ป้องกันไวรัสที่อัปเดตล่าสุดในทุกอุปกรณ์
  - ปรับปรุงระบบปฏิบัติการและซอฟต์แวร์ให้ทันสมัยเสมอ
  - ใช้ระบบไฟร์วอลล์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- รับมือ:
  - แยกอุปกรณ์ที่ติดมัลแวร์ออกจากเครือข่ายทันที
  - สแกนอุปกรณ์ทั้งหมดเพื่อหาการติดเชื้อเพิ่มเติม
  - สำรองข้อมูลอย่างสม่ำเสมอเพื่อกู้คืนข้อมูลในกรณีที่จำเป็น

2. Ransomware

- ป้องกัน:
  - ใช้ระบบสำรองข้อมูลอัตโนมัติและเก็บข้อมูลสำรองไว้นอกเครือข่าย
  - บังคับใช้นโยบายการรักษาความปลอดภัย เช่น การจำกัดสิทธิ์ของผู้ใช้งาน
  - ฝึกอบรมพนักงานให้ระมัดระวังไฟล์แนบในอีเมลและลิงก์ที่ไม่ชัดเจน
- รับมือ:
  - อย่าชำระค่าไถ่เด็ดขาด (ยกเว้นกรณีมีคำสั่งเฉพาะ)
  - แจ้งเหตุการณ์ให้กับเจ้าหน้าที่ไซเบอร์หรือ CERT ของประเทศ
  - ฟื้นฟูระบบจากข้อมูลสำรอง

3. Threat Actors

- ป้องกัน:
  - ใช้การพิสูจน์ตัวตนแบบหลายชั้น (Multi-Factor Authentication)
  - ตรวจสอบกิจกรรมในระบบเครือข่ายเพื่อตรวจจับพฤติกรรมที่ผิดปกติ
  - ติดตั้งระบบ SIEM (Security Information and Event Management) เพื่อแจ้งเตือนภัยคุกคาม
- รับมือ:
  - บันทึกข้อมูลที่เกี่ยวข้องกับการโจมตีเพื่อนำไปวิเคราะห์
  - ใช้ระบบ EDR (Endpoint Detection and Response) เพื่อจัดการกับภัยคุกคามในจุดเชื่อมต่อ

4. Tool-based Attacks

- ป้องกัน:
  - ตรวจสอบและบันทึกการใช้งานเครื่องมือหรือซอฟต์แวร์ที่อาจถูกนำไปใช้โจมตี
  - จำกัดการเข้าถึงเครื่องมือที่อาจเป็นอันตรายให้เฉพาะผู้ที่ได้รับอนุญาต
- รับมือ:
  - ยกเลิกสิทธิ์การใช้งานเครื่องมือที่ถูกใช้ในทางที่ไม่เหมาะสม
  - อัปเดตระบบตรวจจับภัยคุกคาม (IDS/IPS) เพื่อรองรับรูปแบบใหม่

5. Vulnerabilities

- ป้องกัน:
  - ทำการทดสอบเจาะระบบ (Penetration Testing) เป็นประจำ
  - แก้ไขช่องโหว่ในซอฟต์แวร์ทันทีที่มีแพตช์อัปเดต
- รับมือ:
  - ปิดการเข้าถึงส่วนที่มีช่องโหว่จนกว่าจะมีการแก้ไข
  - แจ้งเตือนผู้ใช้ในเครือข่ายเกี่ยวกับช่องโหว่ที่ตรวจพบ

6. Phishing

- ป้องกัน:
  - ใช้โซลูชันอีเมลที่สามารถกรองสแปมและฟิชชิงได้
  - สร้างความตระหนักรู้ให้ผู้ใช้ในการตรวจจับอีเมลฟิชชิง
- รับมือ:
  - ยกเลิกการเข้าถึงบัญชีที่ตกเป็นเหยื่อ
  - ตรวจสอบกิจกรรมที่น่าสงสัยที่เกิดขึ้นหลังการโจมตี

7. Campaign Attacks

- ป้องกัน:
  - ตรวจสอบการเข้าถึงและกิจกรรมที่ผิดปกติในโครงสร้างพื้นฐาน IT
  - ใช้ Threat Intelligence เพื่อระบุและป้องกันแคมเปญที่เป็นอันตราย
- รับมือ:
  - ประสานงานกับผู้เชี่ยวชาญด้านความปลอดภัยเพื่อวิเคราะห์และตอบโต้การโจมตี
  - แจ้งองค์กรอื่น ๆ ในวงการเกี่ยวกับการโจมตีเพื่อป้องกันการแพร่กระจาย

8. Data Leaks

- ป้องกัน:
  - เข้ารหัสข้อมูลสำคัญทั้งในระหว่างการส่งและการเก็บรักษา
  - ใช้ DLP (Data Loss Prevention) เพื่อป้องกันการรั่วไหลของข้อมูล
- รับมือ:
  - แจ้งลูกค้าหรือผู้ที่ได้รับผลกระทบทันที
  - วิเคราะห์แหล่งที่มาของการรั่วไหลและอุดช่องโหว่ที่เกิดขึ้น

อ้างอิงจาก

Threat Intelligence ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์

https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/

https://www.fortinet.com/blog/threat-research/ransomware-roundup-lynx

https://blackpointcyber.com/wp-content/uploads/2025/01/Lynx-2.pdf

https://www.broadcom.com/support/security-center/protection-bulletin/lynx-ransomware-established-in-2024

จัดทำโดย

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