แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนเพื่อเฝ้าระวังกลุ่ม CL-STA-1062 มุ่งโจมตีหน่วยงานสำคัญในเอเชียตะวันออกเฉียงใต้

วันที่แจ้งเตือน 2 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานกรณีกลุ่ม CL-STA-1062 มุ่งเป้าโจมตีหน่วยงานสำคัญในเอเชียตะวันออกเฉียงใต้ โดยมีรายละเอียดดังนี้

การโจมตี	รายละเอียด
• Unit 42 ของ Palo Alto Networks รายงานกรณีกลุ่มผู้โจมตี CL-STA-1062 มุ่งโจมตีหน่วยงานภาครัฐและโครงสร้างพื้นฐานสำคัญ โดยเฉพาะภาคพลังงานในภูมิภาคเอเชียตะวันออกเฉียงใต้ • Unit 42 ประเมินว่ากลุ่มดังกล่าวมีความเชื่อมโยงกับกลุ่ม UAT-7237 ที่เคยถูกรายงานว่ามุ่งโจมตี Web Hosting และมีการดำเนินการโจมตีอย่างต่อเนื่องในเอเชียตั้งแต่ปี พ.ศ. 2565 • ผู้โจมตีใช้ทั้งเครื่องมือโอเพนซอร์ส และ มัลแวร์ที่พัฒนาขึ้นเอง ชื่อว่า TinyRCT ซึ่งทำหน้าที่เป็น Backdoor/RAT ที่ถูกค้นพบใหม่ พัฒนาด้วยภาษา C# บน .NET Framework โดยมีความสามารถในการสั่งรันคำสั่งบนเครื่องที่ถูกโจมตี สำรวจไฟล์ ขโมยข้อมูล จับภาพหน้าจอ และสามารถลบตัวเองออกจากระบบเพื่อลบร่องรอยการโจมตี	รูปแบบการโจมตี 1. ผู้โจมตีใช้ช่องโหว่บน Web Application เพื่อติดตั้ง ASPX Web Shell สำหรับควบคุมเครื่องเหยื่อ 2. ใช้ PowerShell และ curl รวบรวมข้อมูล เช่น Hostname, Domain, IP Address, Domain Admins, System Information แล้วส่งกลับไปยังเซิร์ฟเวอร์ของผู้โจมตี 3. สร้างช่องทางลับ (Tunnel) เครื่องมือที่ใช้บ่อย ได้แก่ SoftEther VPN, VNT และ yuze VPN โดยปลอมตัวเป็นไฟล์ของ VMware หรือ XDR Agent เพื่อหลบเลี่ยงการตรวจจับ 4. ยกระดับสิทธิใช้เครื่องมือโอเพนซอร์ส เช่น JuicyPotato, Mimikatz เป็นต้น 5. ขโมยข้อมูลออกจากองค์กรโดยจะบีบอัดเป็นไฟล์ RAR ที่ตั้งรหัสผ่าน

แนวทางดำเนินการสำหรับผู้ดูแลระบบ:

1. ตรวจสอบเว็บเซิร์ฟเวอร์ โดยเฉพาะไฟล์นามสกุล .aspx, .ashx, .asmx, php หรือไฟล์ที่ถูกเพิ่ม/แก้ไข
2. ตรวจสอบการเชื่อมต่อออกไปยัง IP หรือ URL ที่เกี่ยวข้องกับ C2 ของผู้โจมตี (**ดู IoCs เพิ่มเติมได้จาก อ้างอิง 2**)
3. ตรวจสอบไฟล์ต้องสงสัย เช่น chrome_setup.zip, PerfWatson2.exe, MyAppDomainManager.dll และไฟล์ที่ปลอมชื่อเป็นเครื่องมือระบบ เช่น VMware หรือ Google Updater เป็นต้น
4. ตรวจสอบ Scheduled Task ที่ผิดปกติ โดยเฉพาะชื่อที่คล้าย GoogleUpdaterTaskSystem ...หรือ Task ที่รันไฟล์จาก %LOCALAPPDATA%
5. ตรวจสอบการใช้งานเครื่องมือที่อาจถูกใช้ผิดวัตถุประสงค์ เช่น SoftEther VPN, VNT, Mimikatz,fscan, JuicyPotato และ WinRAR สำหรับบีบอัดข้อมูล
6. ใช้ EDR/XDR, Application Control, Least Privilege และ Network Segmentation เพื่อลดความเสี่ยงการเคลื่อนย้ายภายในเครือข่าย
7. ตรวจสอบ Log ของ Web Server, Firewall, Proxy, DNS, EDR และ Windows Event Log เพื่อหาพฤติกรรมผิดปกติ เช่น การรัน cmd.exe, powershell.exe, curl, rar.exe หรือการเชื่อมต่อออกไปยังปลายทางที่ไม่คุ้นเคย เป็นต้น
8. หากพบความผิดปกติควรแยกเครื่องออกจากเครือข่าย เก็บหลักฐาน Log/Memory/Disk Image และประสานทีม Incident Respond ทันที

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 2 ก.ค. 2569
2. https://unit42.paloaltonetworks.com/cl-sta-1062-tinyrct-backdoor/?