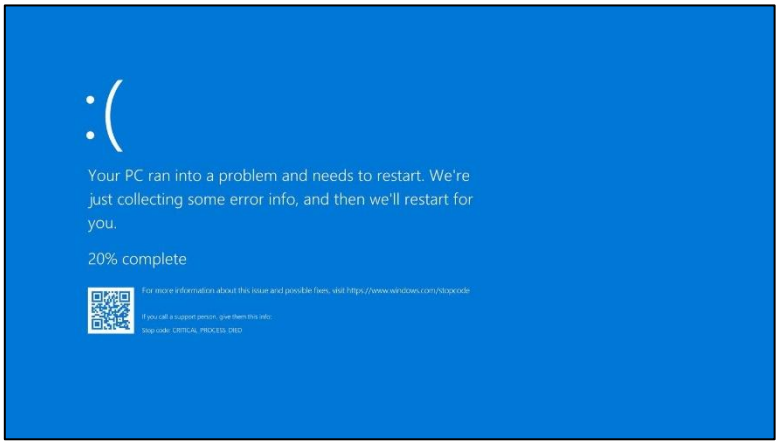
เมื่อวันที่ ๑๙ กรกฎาคม ๒๕๖๗ สกมช. ได้ตรวจพบข่าวผลกระทบระบบปฏิบัติการ Windows ที่มีการติดตั้ง Falcon Sensor ของ CrowdStrike เกิด Blue Screen แบบวนลูปดังภาพ



จากการตรวจสอบพบว่า บริษัท CrowdStrike ได้ระบุสาเหตุของการอัปเดตที่ผิดพลาดว่าเป็นข้อบกพร่องในการอัปเดตเนื้อหา (content update) ซึ่งไม่ได้เป็นเหตุการณ์การโจมตีทางไซเบอร์แต่อย่างใด ในการนี้จึงขอสรุปเหตุการณ์และแจ้งวิธีแก้ไข ดังนี้

สรุปเหตุการณ์

อาการที่พบคือโฮสต์ Windows มีหน้าจอสีฟ้า (BSOD) ที่เกี่ยวข้องกับ Falcon Sensor ณ เวลา 4:09 น. UTC ทีมวิศวกรรมของ CrowdStrike ได้อัปเดตเนื้อหาในส่วนที่เกี่ยวข้องกับปัญหานี้และได้ดำเนินการ ย้อนกลับ (revert) การเปลี่ยนแปลงเหล่านั้นแล้ว ดังนั้น โฮสต์ที่บูตหลังจากเวลา 5:27 น. UTC ไม่ควรพบปัญหาใดๆ โดยปัญหานี้จะไม่ส่งผลกระทบต่อโฮสต์ที่ใช้งานบนระบบปฏิบัติการ Mac หรือ Linux

วิธีการแก้ไขในเบื้องต้น

ขั้นตอนที่ควรทำหากคุณยังประสบปัญหาการ Reboot ซ้ำๆ

- บูตเข้าสู่ Safe Mode (ตามคำแนะนำอย่างเป็นทางการของ CrowdStrike) ขั้นตอนต่อไปนี้ทำได้ทุกกรณี แม้ว่าระบบจะไม่มี local admin account ในเครื่องและไม่มีการเชื่อมต่ออินเทอร์เน็ต
- ให้ระบบบูตและ crash สามครั้ง ซึ่งจะทำให้เมนูปรากฏ
- คลิก Troubleshoot
- คลิก Advanced Options
- คลิก Command Prompt
- หากระบบของคุณได้รับการป้องกันด้วย BitLocker คุณจะต้องป้อนรหัสการกู้คืน BitLocker ของคุณ

        - หาก BitLocker ถูกจัดการผ่าน Microsoft Intune สามารถค้นข้อมูลได้ที่ https://myaccount.microsoft.com ภายใต้เมนู "device" ตรวจสอบให้แน่ใจว่าได้จับคู่ชื่อโฮสต์ของอุปกรณ์และ ID ของคีย์
        - หากไม่สามารถค้นหาข้อมูลใน Microsoft Intune ได้ให้ติดต่อเพื่อขอรับ Recovery Key BitLocker จากผู้ดูแลระบบ IT ของหน่วยงาน
    - ในหน้าต่าง Command Prompt ให้พิมพ์คำสั่งต่อไปนี้ ตามด้วยปุ่ม Enter:
        - คำเตือน: Command Prompt เริ่มต้นที่ไดรฟ์ X:\ กรุณาอย่าลืมเปลี่ยนเป็น c:\ โดยพิมพ์คำสั่งเหล่านี้อย่างถูกต้อง
        - c:
        - cd windows
        - cd system32
        - cd drivers
        - cd crowdstrike
        - del C-00000291*
        - exit
    - คลิก continue to Windows

ขั้นตอนสำหรับผู้ใช้งานระบบ Cloud สาธารณะหรือคล้ายคลึง รวมถึง Virtual Machines

ตัวเลือกที่ 1:

- Detach Volume disk ระบบปฏิบัติการออกจาก virtual server ที่ได้รับผลกระทบ
- Create a snapshot or backup of the disk volume ก่อนดำเนินการต่อไปเพื่อเป็นการป้องกันการเปลี่ยนแปลงที่ไม่ตั้งใจ
- Attach/mount volume กับ virtual server ใหม่
- ไปที่ไดเรกทอรี C:\Windows\System32\drivers\CrowdStrike
- ค้นหาไฟล์ที่ตรงกับ “C-00000291*.sys” และลบมันออก
- Detach volume ออกจาก virtual server ใหม่
- Reattach volume ที่ได้รับการแก้ไขกลับไปยัง virtual server ที่ได้รับผลกระทบ

ตัวเลือกที่ 2:

- ย้อนกลับไป snapshot ก่อนเวลา 04:09 UTC

ขั้นตอนสำหรับ Azure ผ่านทางซีเรียลเพื่อเข้าสู่ Safe Mode

- เข้าสู่ระบบคอนโซล Azure --> ไปที่ Virtual Machines --> Select the VM
- ด้านซ้ายบนของคอนโซล --> คลิก: "Connect" --> คลิก --> Connect --> คลิก "More ways to Connect" --> คลิก: "Serial Console"
- เมื่อ SAC โหลดแล้ว ให้พิมพ์ 'cmd' และกด Enter
    - พิมพ์คำสั่ง 'cmd'
    - พิมพ์: ch -si 1
- กดปุ่มใดก็ได้ (หรือกดแป้น space bar) ใส่ Credential ของผู้ดูแลระบบ
- ป้อนคำสั่งดังนี้:
    - bcdedit /set {current} safeboot minimal
    - bcdedit /set {current} safeboot network
- Restart VM
- ตัวเลือกเพิ่มเติม: วิธีตรวจสอบสถานะการบูต รันคำสั่ง:
    - wmic COMPUTERSYSTEM GET BootupState

ข้อมูลเพิ่มเติม

การทำตามขั้นตอนเหล่านี้จะทำให้ความปลอดภัยของฉันลดลงหรือไม่?

ตอบ : ไม่ หลังจากทำตามขั้นตอนข้างต้น CrowdStrike จะกลับมาทำงานตามปกติในระบบและระบบของคุณยังคงได้รับการป้องกัน

นี่เป็นผลจากการโจมตีทางไซเบอร์หรือไม่?

ตอบ : CrowdStrike ได้ระบุสาเหตุของการอัปเดตที่ผิดพลาดว่าเป็นข้อบกพร่องในการอัปเดตเนื้อหา (content update) ไม่มีข้อบ่งชี้ว่าเกิดจากการโจมตีทางไซเบอร์

ฉันจำเป็นต้องถอดถอน CrowdStrike หรือไม่?

ตอบ : หากระบบของคุณบูตแล้วและ (กลับมา) ออนไลน์ ไม่มีความจำเป็นต้องถอดถอน CrowdStrike

อ้างอิงจาก

https://www.eye.security/blog/crowdstrike-falcon-blue-screen-issue-updates