บันทึกข้อความ

ส่วนราชการ กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน โทร. ๐ ๒๕๒๑ ๖๕๕๐ ต่อ ๓๐๓

ที่ สธ ๐๙๓๕.๐๒/ว ๑๙๘ **วันที่** ๘ มีนาคม ๒๕๖๗

เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๔/๖๗

เรียน รองผู้อำนวยการฯ / หัวหน้ากลุ่มงาน

ตามหนังสือกลุ่มอำนวยการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ที่ สธ ๐๙๔๙.๐๑/ว๑๖๑ ลงวันที่ ๒๗ กุมภาพันธ์ ๒๕๖๗ เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๔/๖๗ จากกรณีนักวิจัยพบโทรจัน GoldPickaxe ขโมยใบหน้าและ CISA เตือนช่องโหว่ Cisco ASA/FTD ที่ CVE-๒๐๒๐-๓๒๕๙ ถูกใช้โจมตีจาก Ransomware โดยให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของหน่วยงานที่อาจเกี่ยวข้องกับเหตุการณ์ดังกล่าว เพื่อเป็นการยกระดับการเฝ้าระวังและป้องกันการโจมตีทางไซเบอร์ ความละเอียดแจ้งแล้วนั้น

ในการนี้ กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน จึงขอประชาสัมพันธ์และสื่อสารให้ท่านและบุคลากรในกลุ่มงานทุกท่าน ทราบถึงแนวทางการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ รายละเอียดตาม QR Code ที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อทราบและแจ้งบุคลากรในกลุ่มงานของท่านทราบและถือปฏิบัติอย่างเคร่งครัดต่อไปด้วย จะเป็นพระคุณ

(นางสาวเกศรา โชคนำชัยสิริ)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

บันทึกข้อความ

ส่วนราชการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ กลุ่มอำนวยการ โทร. ๐ ๒๕๙๐ ๔๓๑๐
ที่ สธ ๐๙๔๙.๐๑/ว ๑๖๑ **วันที่** ๒๗ กุมภาพันธ์ ๒๕๖๗
เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๔/๖๗

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ ผู้อำนวยการสำนักทุกสำนัก ผู้อำนวยการกองทุกกอง ผู้อำนวยการศูนย์ทุกศูนย์ ผู้อำนวยการกลุ่มทุกกลุ่ม ผู้อำนวยการสถาบันทุกสถาบัน เลขานุการกรม

ตามที่ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ได้รับมอบหมายให้มีการติดตาม เฝ้าระวังภัยคุกคามทางไซเบอร์ และเป็นศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์กรมอนามัย เพื่อเตรียมพร้อมรับมือ แก้ไขและป้องกันเหตุการณ์ภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานภายใต้สังกัดกรมอนามัย นั้น

ในการนี้ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ขอแจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ จากกรณีนักวิจัยพบโทรจัน GoldPickaxe ขโมยใบหน้า และ CISA เตือนช่องโหว่ Cisco ASA/FTD ที่ CVE-๒๐๒๐-๓๒๕๙ ถูกใช้โจมตีจาก Ransomware ทั้งนี้ ให้ท่านดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานที่อาจเกี่ยวข้องกับเหตุการณ์ดังกล่าว เพื่อเป็นการยกระดับการเฝ้าระวังและป้องกันการโจมตี รายละเอียดตามเอกสารแนบ หากมีข้อสงสัยสามารถสอบถามได้ที่ นายภัทร์รพี สีบุตตะ หมายเลขโทรศัพท์ ๐ ๒๕๙๐ ๔๓๑๐

จึงเรียนมาเพื่อโปรดทราบ

มอบ HR

(นางสาวชุลีวรรณ นพวิสุทธิสกุล)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ปฏิบัติหน้าที่ผู้อำนวยการกองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย

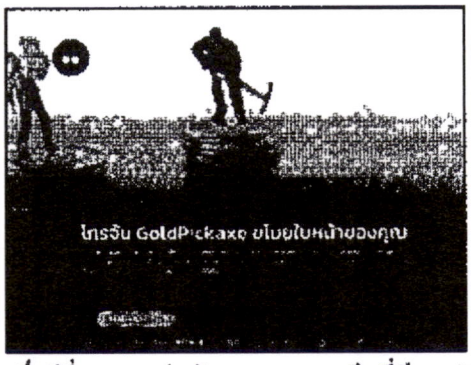
(นางสาวเกศรา โชคนำชัยสิริ)
(ลายเซ็นต์อิเล็กทรอนิกส์)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
รักษาราชการแทนผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง

27 กุมภาพันธ์ 2567

(นางสาวเกศรา โชคนำชัยสิริ)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

ThaiCERT Infoshare
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
ประจำวันจันทร์ที่ 19 กุมภาพันธ์ 2567
สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

โทรจัน GoldPickaxe ขโมยใบหน้าของคุณ



นักวิจัยได้พบตระกูลโทรจัน ซึ่งมีที่มาจากกลุ่มภัยคุกคามชาวจีนที่มีจุดประสงค์ทางการเงิน ซึ่งมีทั้งในเวอร์ชันสำหรับ iOS และ Android โดยอาชญากรไซเบอร์จะพยายามหลอกล่อผู้ที่ตกเป็นเหยื่อให้ทำการสแกนใบหน้าพร้อมกับบัตรประจำตัว ซึ่งผู้ตกเป็นเหยื่อจะได้รับการติดต่อผ่านข้อความพิชชิ่งหรือการหลอกลวงทางโทรศัพท์ โดยอ้างว่าติดต่อมาจากหน่วยงานของรัฐบาลหรือหน่วยงานที่น่าเชื่อถืออื่น ๆ และเมื่อเป้าหมายหลงเชื่อกลุ่มมิจฉาชีพก็จะให้เหยื่อทำการติดตั้งแอปพลิเคชันที่ปลอมเป็นแอปพลิเคชันบริการของหน่วยงานภาครัฐ ซึ่งในขั้นตอนนี้ เหยื่อที่ใช้ระบบปฏิบัติการ Android และ iOS จะแตกต่างกัน เนื่องจากผู้ใช้งาน Android จะสามารถดาวน์โหลดแอปที่เป็นอันตรายได้ทันที แต่เนื่องจาก Apple มีมาตรการสำหรับความปลอดภัย อาชญากรจึงต้องขอให้ผู้ใช้งาน iOS ทำการติดตั้งโปรไฟล์ Mobile Device Management (MDM) ซึ่ง MDM จะอนุญาตให้ผู้ควบคุมทำการตั้งค่าอุปกรณ์จากระยะไกล โดยการส่งโปรไฟล์และคำสั่งไปยังอุปกรณ์ โดย MDM จะมีคุณสมบัติที่หลากหลาย เช่น การสร้างข้อมูลระยะไกล การติดตามอุปกรณ์ และการจัดการแอปพลิเคชัน ซึ่งอาชญากรไซเบอร์จะใช้ประโยชน์จากการติดตั้งแอปพลิเคชันที่เป็นอันตรายและรับข้อมูลที่ต้องการ

หลังจากนั้น อาชญากรไซเบอร์จะขอให้เหยื่อถ่ายรูปบัตรประจำตัวประชาชน และทำการสแกนใบหน้าด้วยแอป นอกจากนี้ คนร้ายยังขอหมายเลขโทรศัพท์ของเหยื่อ เพื่อที่จะสามารถได้รับข้อมูลรายละเอียดเพิ่มเติมเกี่ยวกับพวกเขา โดยเฉพาะข้อมูลบัญชีธนาคารของพวกเขา เมื่อคนร้ายสแกนใบหน้าได้แล้ว พวกเขาสามารถใช้โปรแกรม AI เพื่อทำการสลับหน้า ซึ่งการสลับใบหน้าเป็นเทคนิคที่ช่วยให้ใครก็ตามสามารถแทนที่ใบหน้าในรูปภาพด้วยใบหน้าอื่น ๆ ได้ ด้วยการสลับใบหน้าและรูปถ่ายบัตรประจำตัว อาชญากรจะสามารถปลอมเป็นลูกค้าธนาคารของผู้ตกเป็นเหยื่อและทำการถอนเงินออกจากบัญชีของพวกเขาได้ เพราะองค์กรทางการเงินหลายแห่งได้ใช้วิธีการจดจำใบหน้า เพื่อยืนยันการทำธุรกรรมและรับรองความถูกต้องในการเข้าสู่ระบบ แม้ว่านักวิจัยยังไม่พบหลักฐานว่าการฉ้อโกงทางธนาคารคือเป้าหมายหลักของกลุ่มอาชญากรไซเบอร์ แต่เรื่องราวการฉ้อโกงดังกล่าวก็ได้รับการยืนยันจากคำเตือนจากตำรวจของประเทศไทย

ที่มาของข่าว https://www.malwarebytes.com/blog/news/2024/02/goldpickaxe-trojan-steals-your-face

ThaiCERT Infoshare

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

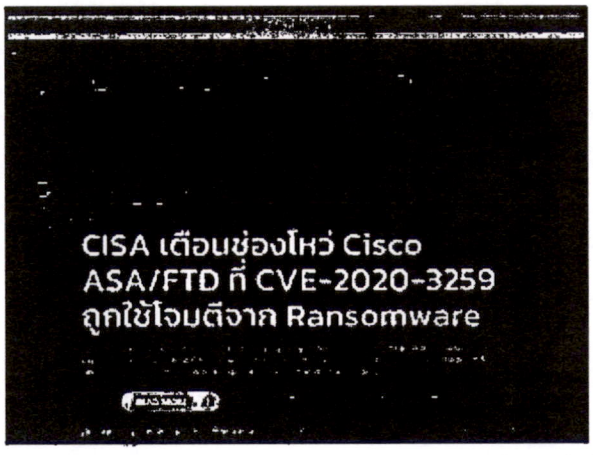
ประจำวันจันทร์ที่ 19 กุมภาพันธ์ 2567

68/67 (11)

NCSA สกมช

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

CISA เตือนช่องโหว่ Cisco ASA/FTD ที่ CVE-2020-3259 ถูกใช้โจมตีจาก Ransomware



U.S. Cybersecurity and Infrastructure Security Agency (CISA) เตือนว่ามีกลุ่ม Akira Ransomware ได้กำลัง exploit ช่องโหว่ Cisco ASA/FTD ที่ CVE-2020-3259 (CVSS score: 7.5) ที่มีการใช้โจมตีโดยทั่วไปและ CISA ได้เพิ่มช่องโหว่ Cisco ASA/FTD ลงใน Known Exploited Vulnerabilities catalog โดยช่องโหว่ CVE-2020-3259 เป็นช่องโหว่การเปิดเผยข้อมูลที่อยู่ใน web services interface ของ Cisco ASA/FTD ซึ่ง CISA ได้กล่าวถึงช่องโหว่ดังกล่าวว่าถูกใช้ในแคมเปญของ Ransomware แต่ไม่ได้มีการเปิดเผยว่ากลุ่ม Ransomware ใดที่ใช้ประโยชน์จากช่องโหว่นี้

โดยเมื่อเดือนมกราคม นักวิจัยจากบริษัทรักษาความปลอดภัยทางไซเบอร์ Truesec ได้รายงานว่าพบข้อมูล forensic ที่มีกลุ่ม Akira Ransomware ได้ใช้ประโยชน์จากช่องโหว่ Cisco ASA (Adaptive Security Appliance) และ FTD (Firepower Threat Defence) ซึ่งผู้โจมตีสามารถใช้ช่องโหว่ดังกล่าวในการดึงข้อมูลที่ละเอียดอ่อนออกจากหน่วยความจำของอุปกรณ์ รวมถึงชื่อผู้ใช้และรหัสผ่าน

ทาง CISA ได้สั่งให้หน่วยงานรัฐบาลแก้ไขช่องโหว่ CVE-2020-3259 ภายในวันที่ 7 มีนาคม 2024 และให้หน่วยงานเอกชนตรวจสอบและแก้ไขช่องโหว่ในโครงสร้างพื้นฐานด้วย

ที่มาของข่าว https://securityaffairs.com/159244/cyber-crime/cisa-cisco-cve-2020-3259-akira-ransomware.html