บันทึกข้อความ

ส่วนราชการ กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน โทร. ๐ ๒๕๒๑ ๖๕๕๐ ต่อ ๓๐๓

ที่ สธ ๐๙๓๕.๐๒/ว ๑๓๐ **วันที่** ๑๕ กุมภาพันธ์ ๒๕๖๗

เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๒/๖๗

เรียน รองผู้อำนวยการฯ / หัวหน้ากลุ่มงาน

ตามหนังสือกลุ่มอำนวยการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ที่ สธ ๐๙๔๙.๐๑/ว๑๓๐ ลงวันที่ ๖ กุมภาพันธ์ ๒๕๖๗ เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๒/๖๗ จากกรณีโปรแกรมควบคุมหน้าจอจากระยะไกล AnyDesk Remote Desktop ถูกแฮก โดยแนะนำให้ผู้ใช้งานเปลี่ยนรหัสผ่านและดาวน์โหลดซอฟแวร์เวอร์ชั่นล่าสุด และข่าวรายงานจำนวนผู้ตกเป็นเหยื่อกลโกงของการโจมตีแบบ Romance Scam หรือกลโกงโดยการหลอกให้เหยื่อหลงรัก มีจำนวนเพิ่มมากขึ้นในปี ๒๐๒๓ 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 ๒๗๐ **วันที่** ๒ กุมภาพันธ์ ๒๕๖๗

เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๒/๖๗

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ ผู้อำนวยการสำนักทุกสำนัก ผู้อำนวยการกองทุกกอง ผู้อำนวยการศูนย์ทุกศูนย์ ผู้อำนวยการกลุ่มทุกกลุ่ม ผู้อำนวยการสถาบันทุกสถาบัน เลขานุการกรม

ตามที่ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ได้รับมอบหมายให้มีการติดตาม เฝ้าระวังภัยคุกคามทางไซเบอร์ และเป็นศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์กรมอนามัย เพื่อเตรียมพร้อมรับมือ แก้ไขและป้องกันเหตุการณ์ภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานภายใต้สังกัดกรมอนามัย นั้น

ในการนี้ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ขอแจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ จากกรณี AnyDesk Remote Desktop Software ถูกแฮก โดยผู้ใช้งานควรเปลี่ยนรหัสผ่าน และข่าวเหยื่อกลโกงของการโจมตี Romance Scam ที่เพิ่มขึ้นในปี ๒๐๒๓ รายละเอียดตามเอกสารแนบ หากมีข้อสงสัยสามารถสอบถามได้ที่ นายภัทร์รพี สีบุตตะ หมายเลขโทรศัพท์ ๐ ๒๕๙๐ ๔๓๑๐

จึงเรียนมาเพื่อโปรดทราบ

(นางสาวชุลีวรรณ นพวิสุทธิสกุล)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ปฏิบัติหน้าที่ผู้อำนวยการกองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย

เรียน ผู้อำนวยการฯ
เพื่อโปรดพิจารณา เห็นควรมอบHR
ดำเนินการต่อไปด้วย จะเป็นพระคุณ

นางกนกลักษณ์ ตอนตง
เจ้าพนักงานธุรการ
13 กุมภาพันธ์ 2567

ทราบมอบ HR

ทราบ/ดำเนินการ
(นางสาวเกศรา โชคนำชัยสิริ)
(ลายเซ็นต์อิเล็กทรอนิกส์)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
รักษาราชการแทนผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง
13 กุมภาพันธ์ 2567

ทราบ
อ.ทยุพ
14/2/67

ทพพ
เพพ.
14/2/67

ทราบ
14 ก.พ. 67

(นางสาวเกศรา โชคนำชัยสิริ)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังค

ThaiCERT Infoshare

สรุปข่าวประชาสัมพันธ์ด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในรอบสัปดาห์

ประจำวันจันทร์ที่ 5 กุมภาพันธ์ 2567

สกมช

AnyDesk Remote Desktop Software ถูกแฮก ผู้ใช้งานควรเปลี่ยนรหัสผ่าน

AnyDesk ผู้ผลิต Remote desktop software เปิดเผยเมื่อวันศุกร์ว่าได้รับผลกระทบจาก cyber attack ที่ถูก compromise ที่ production systems โดยบริษัท German กล่าวถึงเหตุการณ์ดังกล่าวว่าได้ทำการตรวจสอบแล้วพบว่าไม่ใช่การโจมตีของ ransomware และได้ทำการแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ โดยทาง AnyDesk ได้ยกเลิกรหัสผ่านทั้งหมดไปยัง web portal, my.anydesk[.]com ซึ่งแนะนำให้ผู้ใช้งานเปลี่ยนรหัสผ่านและดาวน์โหลดซอฟต์แวร์เวอร์ชันล่าสุด

AnyDesk ไม่ได้เปิดเผยว่าระบบของบริษัทถูกละเมิดเมื่อใดและในขณะนี้ยังไม่ทราบว่ามีข้อมูลใดถูกขโมยไปหลังจากการโจมตีหรือไม่ ซึ่ง AnyDesk มีลูกค้ามากกว่า 170,000 ราย รวมถึง Amedes, AutoForm Engineering, LG Electronics, Samsung Electronics, Spidercam และ Thales จากการเปิดเผยดังกล่าวเกิดขึ้นหนึ่งวันหลังจากที่ Cloudflare กล่าวว่าถูกละเมิดโดยผู้โจมตีที่ต้องสงสัยโดยใช้ข้อมูลประจำตัวที่ถูกขโมยเพื่อเข้าถึงเซิร์ฟเวอร์ Atlassian โดยไม่ได้รับอนุญาต และท้ายที่สุดก็เข้าถึงเอกสารบางส่วนและซอร์สโค้ดได้

ที่มาของข่าว : https://thehackernews.com/2024/02/anydesk-hacked-popular-remote-desktop.html

ThaiCERT Infoshare

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

ประจำเดือนกันยายน 2567

NCSA สกมช

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เหยื่อกลโกงของการโจมตี Romance Scam เพิ่มขึ้นในปี 2023

ข้อมูลจากธนาคาร Lloyds ของประเทศอังกฤษ พบว่ามีผู้ตกเป็นเหยื่อของ Romance Scam หรือกลโกงโดยการหลอกให้เหยื่อหลงรัก มีจำนวนเพิ่มขึ้นมากกว่า 22% ในปี 2023 เทียบกับปี 2022 ซึ่งจำนวนเงินที่สูญเสียโดยเฉลี่ยต่อเหตุการณ์คือ 6,937 ปอนด์ (315,943 บาท) ในปี 2022 ซึ่งมีเคสที่สูญเสียเงินน้อยกว่าปี 2023 โดยเฉลี่ยต่อเหตุการณ์อยู่ประมาณ 8,237 ปอนด์ (375,154 บาท) ซึ่ง Romance Scam หรือกลโกงการหลอกให้เหยื่อหลงรัก ถูกนำไปใช้เพื่อโจมตีอย่างแพร่หลายในช่วงไม่กี่ปีที่ผ่านมา โดยผู้โจมตีใช้ประโยชน์จากโปรไฟล์ปลอมที่สร้างขึ้นมาให้ดูดีและน่าเชื่อถือบนโซเชียลมีเดียและแอปหาคู่ออนไลน์ เพื่อล่อลวงผู้ที่อาจตกเป็นเหยื่อและถูกนำไปใช้เพื่อการฉ้อโกง และกิจกรรมทางไซเบอร์ที่เป็นอันตรายประเภทอื่น ๆ อีกด้วย โดยในเดือนธันวาคม 2023 Chainalysis พบว่าผู้โจมตีมักสร้างความสัมพันธ์กับเหยื่อโดยใช้เทคนิคการหลอกลวงแบบ Romance Scam เพื่อทำการโจมตีแบบฟิชชิ่งต่อไป

ตามรายงานของธนาคาร Lloyds ระบุว่าผู้หลอกลวงจะใช้เวลาเพื่อสร้างความสัมพันธ์ให้เหยื่อเชื่อใจและหลงรักทางออนไลน์ โดยโซเชียลมีเดียและโปรไฟล์เว็บไซต์หาคู่ของแก๊ง Romance Scam จะถูกสร้างขึ้นโดยใช้ภาพถ่ายและข้อมูลปลอม และนักต้มตุ๋นจะอ้างเหตุผลมากมายว่าทำไมพวกเขาไม่สามารถไปพบหน้าได้ หรือวิดีโอคอลได้ และจะอ้างว่ามีอาชีพทำงานในกองทัพหรืองานช่วยเหลือและการทูตระหว่างประเทศ หลังจากสร้างความไว้วางใจกับเหยื่อแล้ว พวกเขาจะขอเงินโดยการอ้างเหตุผล เช่น มีปัญหาครอบครัวหรือต้องการคำรักษาพยาบาล พวกเขามักจะเริ่มขอเงินจำนวนเล็กน้อยและเพิ่มขึ้นเรื่อย ๆ จากข้อมูลใหม่พบว่าผู้ชายมีแนวโน้มที่จะตกเป็นเหยื่อของการหลอกลวงเรื่องความรักมากกว่าเล็กน้อย ซึ่งคิดเป็น 52% ของเหตุการณ์ทั้งหมด แต่อย่างไรก็ตามเมื่อผู้หญิงตกเป็นเหยื่อ ในรายงานพบว่ามีมูลค่าความเสียหายโดยเฉลี่ย สูงกว่าผู้ชายอย่างมีนัยสำคัญอยู่ที่ประมาณ 9,083 ปอนด์ (413,865 บาท) เทียบกับ 5,145 ปอนด์ (234,413 บาท) และผู้ที่มีอายุระหว่าง 55 ถึง 64 ปี จะมีแนวโน้มที่ถูกหลอกโดยแก๊ง Romance Scam มากที่สุด และจำนวนเคสในกลุ่มอายุนี้เพิ่มขึ้น 49% เมื่อเทียบกับปี 2022 กลุ่มอายุที่สูญเสียเงินมากที่สุดจากการหลอกลวงเหล่านี้อยู่ระหว่าง 65 ถึง 74 ปี เหยื่อเหล่านี้สูญเสียเงินโดยเฉลี่ย 13,123 ปอนด์ (597,889 บาท) ต่อเหตุการณ์

มีการพบว่า AI ถูกใช้เพื่อเพิ่มประสิทธิภาพในการหลอกลวง Romance Scam โดยอาชญากรไซเบอร์ได้ใช้เครื่องมือ AI ทั่วไป เช่น ChatGPT เพื่อปรับปรุงการโจมตีทางวิศวกรรมสังคม รวมถึงการหลอกลวงเรื่องความรัก โดยในเดือนสิงหาคม ปี 2023 นักวิจัยของ Sophos ตั้งข้อสังเกตว่าแคมเปญ CryptoRom ที่โด่งดังได้ใช้วิธีหลอกลวงเรื่องความรักและการซื้อขาย crypto ปลอม โดยใช้เครื่องมือ AI ที่สร้างขึ้นมาเพื่อล่อลวงและโต้ตอบกับเหยื่อ ทำให้เหยื่อหลงเชื่อและตรวจจับการหลอกลวงดังกล่าวได้ยากขึ้น

ที่มาของข่าว https://www.infosecurity-magazine.com/news/romance-scam-victims-surge/