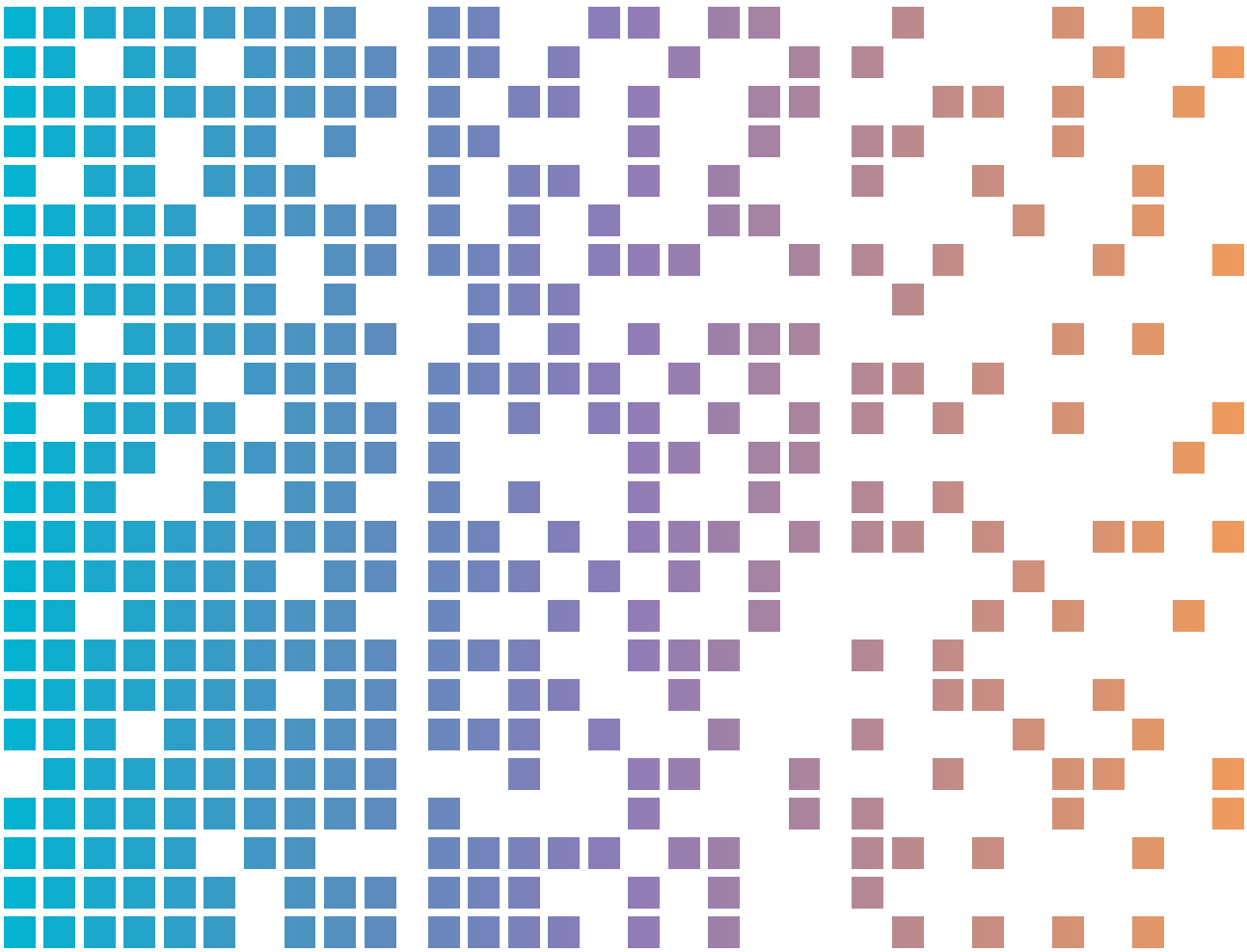
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

การปล้นเงียบ: อาชญากรไซเบอร์ใช้มัลแวร์ขโมยข้อมูลในการบุกรุกเครือข่ายขององค์กร



ระดับความซับซ้อนของเนื้อหา
ปานกลาง ● ● ○

สารบัญ

บริบท

มัลแวร์ขโมยข้อมูลจะขโมยข้อมูลประจำตัวของผู้ใช้และข้อมูลของระบบ ซึ่งอาชญากรไซเบอร์นำไปใช้ประโยชน์ โดยส่วนใหญ่เพื่อแสวงหาประโยชน์ทางการเงิน มีการพบว่ามัลแวร์ขโมยข้อมูลถูกใช้ในการโจมตีทางอาชญากรรมทางไซเบอร์ต่อองค์กรและภาคส่วนต่าง ๆ ทั่วโลก รวมถึงออสเตรเลียด้วย เอกสารเผยแพร่ฉบับนี้ให้คำแนะนำแก่ผู้อ่านในเรื่องความปลอดภัยทางไซเบอร์เกี่ยวกับมัลแวร์ขโมยข้อมูล รวมถึงข้อมูลเกี่ยวกับกิจกรรมที่เป็นภัยคุกคามและคำแนะนำในการบรรเทาปัญหาสำหรับองค์กรและพนักงานขององค์กร

ประเด็นสำคัญ

- มัลแวร์ขโมยข้อมูล หรือที่รู้จักกันอีกชื่อหนึ่งว่า อินโฟสตีลเลอร์ (Info stealer) ซึ่งเป็นมัลแวร์ประเภทหนึ่งที่ถูกออกแบบมาเพื่อเก็บรวบรวมข้อมูลจากอุปกรณ์ของผู้เสียหาย ข้อมูลที่ถูกขโมยอาจรวมถึงชื่อผู้ใช้และรหัสผ่าน รายละเอียดบัตรเครดิต กระเป๋าเงินคริปโต ไฟล์ในเครื่อง และข้อมูลจากเบราว์เซอร์ รวมถึงคุกกี้ ประวัติการใช้งานของผู้ใช้ และรายละเอียดในแบบฟอร์มที่กรอกโดยอัตโนมัติ
- อาชญากรไซเบอร์อาจพยายามซื้อและใช้ข้อมูลประจำตัวผู้ใช้ที่ถูกขโมยไป ซึ่งเชื่อมโยงกับบัญชีบริษัท เพื่อเข้าถึงอุปกรณ์ของนายจ้างของผู้เสียหาย ลูกค้าหรือระบบอื่น ๆ ของบริษัทได้ในขั้นต้น ผลกระทบที่ตามมาต่อองค์กรเหล่านี้อาจรวมถึง การโจมตีด้วยแรนซัมแวร์ การขู่กรรโชก การบุกรุกระบบอีเมลธุรกิจ และการขโมยทรัพย์สินทางปัญญา
- ศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลียของหน่วยข่าวกรองสัญญาณออสเตรเลีย (Australian Signals Directorate's Australian Cyber Security Centre - ASD's ACSC) ได้ตรวจพบกรณีการละเมิดเครือข่ายขององค์กรที่มีต้นเหตุมาจากการที่พนักงานเข้าถึงทรัพยากรของที่ทำงานผ่านอุปกรณ์ส่วนตัวที่ถูกบุกรุก ในหลายกรณี อาชญากรไซเบอร์ได้เข้าถึงเครือข่ายองค์กรในขั้นต้น โดยใช้ข้อมูลประจำตัวผู้ใช้ที่ขโมยมาและยังใช้งานได้อยู่ การตรวจสอบของเราพบว่าการบุกรุกอย่างกว้างขวางมักเกิดขึ้นหลังจากที่อาชญากรไซเบอร์สามารถเข้าถึงบัญชีผู้ใช้ที่มีสิทธิพิเศษได้สำเร็จ
- องค์กรที่อนุญาตให้พนักงาน ผู้รับเหมา ผู้ให้บริการด้านบริหารจัดการจากภายนอก หรือหน่วยงานอื่น ๆ เข้าถึงเครือข่ายของตนได้จากระยะไกล รวมถึงผ่านการใช้อุปกรณ์ส่วนตัว (Bring Your Own Device - BYOD) ควรตระหนักถึงความเสี่ยงจากมัลแวร์อินโฟสตีลเลอร์ และดำเนินการป้องกันตนเองจากภัยคุกคามนี้ อาชญากรไซเบอร์นำมัลแวร์อินโฟสตีลเลอร์ไปติดตั้งในอุปกรณ์ของผู้เสียหายโดยใช้เทคนิคหลากหลายรูปแบบ เช่น อีเมลฟิชชิ่ง การดาวน์โหลดซอฟต์แวร์เถื่อน เทคนิคปรับแต่งผลการค้นหา (Search engine optimisation - SEO) โฆษณาที่เป็นอันตราย หรือการโพสต์ลิงก์ที่เป็นอันตรายบนแพลตฟอร์มโซเชียลมีเดีย โดยทั่วไปแล้วอุปกรณ์ที่ใช้ทั้งในงานและส่วนตัวจะมีความเสี่ยงสูงกว่าที่จะติดมัลแวร์จากเทคนิคเหล่านี้ เนื่องจากพฤติกรรมผู้ใช้และการควบคุมความปลอดภัยที่ลดลง
- มัลแวร์อินโฟสตีลเลอร์เป็นรูปแบบที่น่าสนใจสำหรับอาชญากรไซเบอร์ในการสร้างรายได้จากกิจกรรมประเภทอาชญากรรมทางไซเบอร์ โดยเฉพาะอย่างยิ่งในกลุ่มอาชญากรไซเบอร์ที่เพิ่งเริ่มต้นเข้าสู่วงการและผู้ที่มีความชำนาญด้านเทคนิคที่จำกัด อาชญากรไซเบอร์บางรายจะจำหน่ายผลิตภัณฑ์มัลแวร์อินโฟสตีลเลอร์ในรูปแบบบริการ (Malware-as-a-Service หรือ MaaS) โดยเรียกเก็บค่าธรรมเนียมการใช้งานเป็นรายเดือน

ความเป็นมา

การที่อาชญากรไซเบอร์เลือกใช้มัลแวร์อินโฟสตีลเลอร์นั้นเป็นภัยคุกคามต่อความปลอดภัยและสุขภาวะขององค์กรในออสเตรเลีย การติดมัลแวร์อินโฟสตีลเลอร์มักเป็นกิจกรรมเบื้องต้นก่อนเกิดเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ร้ายแรง เนื่องจากอาชญากรไซเบอร์ใช้มัลแวร์เหล่านี้ในการรวบรวมข้อมูลประจำตัวของผู้ใช้ ข้อมูลประจำตัวของผู้ใช้เหล่านี้ โดยเฉพาะข้อมูลที่ให้สิทธิ์การเข้าถึงบริการจากระยะไกลที่เชื่อมต่อกับอินเทอร์เน็ตหรือบัญชีที่มีสิทธิพิเศษ จะถูกนำไปใช้ประโยชน์เพื่อให้สามารถเข้าถึงระบบและข้อมูลขององค์กรในขั้นต้น

หมายเหตุ ตัวกลางการเข้าถึงระบบในขั้นต้น (Initial access brokers) มีบทบาทเฉพาะทางในระบบนิเวศของอาชญากรรมทางไซเบอร์ โดยทำหน้าที่รับซื้อและตรวจสอบข้อมูลประจำตัวของผู้ใช้ที่ถูกขโมยมา จากนั้น พวกเขาจะนำข้อมูลประจำตัวของผู้ใช้ที่มีคุณภาพสูง ซึ่งสามารถเข้ากับสภาพแวดล้อมองค์กรที่เป็นเป้าหมายไปประมูลให้กับอาชญากรไซเบอร์ที่ต้องการนำข้อมูลประจำตัวของผู้ใช้เหล่านี้ไปใช้เจาะเครือข่ายองค์กรนั้น ๆ ต่อไป

ข้อมูลประจำตัวของผู้ใช้ที่ถูกขโมยและยังใช้งานได้อยู่ ถือว่ามีมูลค่าสูงสำหรับอาชญากรไซเบอร์ เนื่องจากช่วยให้สามารถเข้าถึงเครือข่ายและระบบขององค์กรในขั้นต้นได้อย่างรวดเร็ว ด้วยข้อมูลประจำตัวของผู้ใช้ที่ถูกขโมยและยังใช้งานได้อยู่นั้น อาชญากรไซเบอร์สามารถหลบเลี่ยงกลยุทธ์และเทคนิคทั่วไปได้หลายรูปแบบ เช่น

- การระบุและศึกษาข้อมูลเกี่ยวกับเป้าหมาย
- การสำรวจและเก็บรายละเอียดเครือข่ายของเป้าหมายเพื่อหาช่องโหว่
- การพัฒนาช่องทางในการเข้าถึงระบบในขั้นต้น เช่น
  - การสร้างเนื้อหาฟิชชิ่ง
  - การใช้ประโยชน์จากช่องโหว่ของซอฟต์แวร์
  - การมุ่งเป้าโจมตีบริการจากระยะไกล เช่น บริการ Remote Desktop Protocol (RDP) หรือบริการ Virtual Private Network (VPN)
  - การโจมตีแบบ Brute Force เพื่อเข้าระบบด้วยข้อมูลประจำตัวของผู้ใช้ (ด้วยการเดารหัสผ่าน)

ขั้นตอนเหล่านี้ต้องใช้การลงทุนด้านเวลาและทักษะทางเทคนิคในระดับหนึ่ง ซึ่งเป็นอุปสรรคสำหรับอาชญากรไซเบอร์บางกลุ่ม โดยเฉพาะอย่างยิ่งอาชญากรไซเบอร์ที่ไม่สามารถเจาะระบบป้องกันของเครือข่ายองค์กรได้ ยังอาจได้รับประโยชน์โดยตรงจากการติดมัลแวร์อินโฟสตีลเลอร์ เนื่องจากมัลแวร์เหล่านี้สามารถให้การเข้าถึงข้อมูลประจำตัวของผู้ใช้ในเครือข่ายองค์กรเป้าหมายได้อย่างรวดเร็วและง่ายดาย

ในสภาพแวดล้อมการทำงานจากระยะไกล พนักงานบางคนใช้อุปกรณ์ส่วนตัวทั้งในการทำงานและการท่องอินเทอร์เน็ตส่วนตัว การทำเช่นนี้ พนักงานอาจเลือกที่จะจัดเก็บข้อมูลประจำตัวของผู้ใช้ไว้ในตัวจัดเก็บรหัสผ่านหรือเอ็กเทนชันของเว็บเบราว์เซอร์ หรืออาจใช้ฟีเจอร์กรอกข้อมูลอัตโนมัติของเว็บเบราว์เซอร์ มัลแวร์อินโฟสตีลเลอร์จะมุ่งเป้าไปที่ที่จัดเก็บรหัสผ่านเหล่านี้ รวมถึงคุกกี้สำหรับการยืนยันตัวตนและข้อมูลส่วนตัวอื่น ๆ ภายในเว็บเบราว์เซอร์

ซึ่งต่างจากอุปกรณ์ขององค์กร อุปกรณ์ส่วนตัวมักไม่มีการบังคับใช้นโยบายความปลอดภัยที่เข้มงวดอย่างเช่นขององค์กร จึงเป็นเหตุให้เกิดความเสี่ยงที่สูงกว่าต่อระบบขององค์กร ตัวอย่างเช่น พนักงานอาจมีส่วนทำกิจกรรมบางอย่าง เช่นการดาวน์โหลดซอฟต์แวร์เถื่อนหรือท่องเว็บไซต์ที่มีความเสี่ยงสูง ซึ่งไปเพิ่มโอกาสในการเผชิญกับภัยคุกคามทางไซเบอร์และการติดมัลแวร์

ในปัจจุบัน มัลแวร์อินโฟสตีลเลอร์ ตัวกลางการเข้าถึงระบบในขั้นต้น และพันธมิตรร่วมของกลุ่มแรนซัมแวร์ได้กลายเป็นส่วนสำคัญของระบบนิเวศอาชญากรรมทางไซเบอร์ที่ขับเคลื่อนด้วยแรงจูงใจจากผลกำไรทางการเงิน ระบบนิเวศนี้จะยิ่งมีประสิทธิภาพมากขึ้นเมื่ออาชญากรไซเบอร์มีความเชี่ยวชาญและพัฒนาขีดความสามารถเฉพาะด้านในแต่ละขั้นตอนของการโจมตี แล้วนำความสามารถเหล่านั้นไปจำหน่ายเป็นบริการให้กับเครือข่ายอาชญากรรมอื่น ๆ

กิจกรรมที่เป็นภัยคุกคาม

ACSC ของ ASD กำลังติดตามและเฝ้าระวังการเพิ่มขึ้นของกิจกรรมมัลแวร์อินโฟสตีลเลอร์ทั่วโลก ซึ่งถือเป็นภัยคุกคามที่ทวีความรุนแรงต่อเครือข่ายของออสเตรเลีย รายงานจากภาคอุตสาหกรรมระบุว่ามัลแวร์อินโฟสตีลเลอร์เป็นมัลแวร์ที่ได้รับความนิยมมากที่สุดในบรรดากิจกรรมประเภทอาชญากรรมทางไซเบอร์ตลอดปี 2023 ปริมาณข้อมูลที่ถูกขโมยและนำมาจำหน่ายในตลาดมืดที่เพิ่มขึ้น รวมถึงกิจกรรมของตัวกลางการเข้าถึงระบบในขั้นต้นที่นำข้อมูลเหล่านี้ไปใช้ เป็นภาพสะท้อนของแนวโน้มดังกล่าวที่เพิ่มขึ้นอย่างต่อเนื่อง และยังคงเร่งตัวขึ้นในปี 2024

ระบบนิเวศของมัลแวร์ขโมยข้อมูล

ขั้นตอนที่ 1 การเข้าถึงมัลแวร์

มัลแวร์อินโฟสตีลเลอร์มักถูกมาเสนอขายในตลาดของอาชญากรไซเบอร์ในรูปแบบบริการมัลแวร์ หรือ MaaS (Malware-as-a-Service) หรือบริการขโมยข้อมูล (Stealer-as-a-Service) หรือขายเป็นซอร์สโค้ด MaaS หมายถึงรูปแบบทางธุรกิจที่ผู้พัฒนาโปรแกรมมัลแวร์ขายการสมัครใช้งาน (Subcription) ซอฟต์แวร์ที่เป็นอันตรายของตนให้กับบุคคลอื่นผ่านแพลตฟอร์มบนเว็บ โดยมีลักษณะคล้ายกับบริการซอฟต์แวร์ (Software-as-a-Service หรือ SaaS) แบบถูกกฎหมาย รูปแบบ MaaS ได้ลดอุปสรรคในการเข้าสู่วงการอาชญากรไซเบอร์ลง เนื่องจากเปิดโอกาสให้บุคคลที่ไม่มีทักษะทางเทคนิคขั้นสูงสามารถเผยแพร่มัลแวร์และรวบรวมข้อมูลที่ถูกขโมยไปใช้ในการโจมตีทางไซเบอร์ได้

มัลแวร์อินโฟสตีลเลอร์ที่มาเสนอขายในรูปแบบ MaaS มักจะโฆษณาด้วยค่าบริการรายเดือนที่ไม่แพงนัก และจะมาพร้อมกับแดชบอร์ดอินโฟสตีลเลอร์สำหรับให้อาชญากรไซเบอร์เข้าถึงเพื่อใช้งานได้ แดชบอร์ดจะช่วยอำนวยความสะดวกในการสร้างมัลแวร์อินโฟสตีลเลอร์ จัดระเบียบข้อมูลที่ขโมยมาและติดตามจำนวนระบบที่ถูกบุกรุก ผู้ให้บริการ MaaS จะนำเสนอการอัปเดตฟีเจอร์ จัดหาเครื่องมือและการสนับสนุนทางเทคนิค เพื่อหลีกเลี่ยงการตรวจจับโดยซอฟต์แวร์แอนติไวรัส รวมถึงการดึงดูดและรักษาสมาชิกผู้สมัครใช้งานไว้ มัลแวร์อินโฟสตีลเลอร์จำนวนมากสามารถลบตัวเองออกจากอุปกรณ์ของผู้เสียหายได้หลังจากที่ลักลอบนำข้อมูลออกไปเรียบร้อยแล้ว

ขั้นตอนที่ 2 การแพร่กระจายมัลแวร์

อาชญากรไซเบอร์ที่แพร่กระจายมัลแวร์อินโฟสตีลเลอร์และรวบรวมข้อมูลจากอุปกรณ์ที่ถูกบุกรุกเรียกว่า 'แทรฟเฟอร์' หรือ 'Traffers' (ซึ่งมาจากคำว่า Traffic distributors หรือผู้แพร่กระจายข้อมูลที่ไหลเวียนในระบบ) แทรฟเฟอร์ชี้เป้าให้ผู้เสียหายไปลิงก์ที่เป็นอันตราย ซึ่งจะช่วยอำนวยให้มัลแวร์อินโฟสตีลเลอร์แพร่กระจายออกไปโดยที่เป็นส่วนหนึ่งของการโจมตีขนาดใหญ่ การโจมตีส่วนใหญ่มักไม่ได้เลือกเป้าหมายอย่างเฉพาะเจาะจง แต่จะอาศัยการติดมัลแวร์แบบฉวยโอกาส อย่างไรก็ตาม การโจมตีบางส่วนมีการปรับแต่งให้เหมาะกับอุตสาหกรรมเฉพาะประเภท และใช้วิธีการโจมตีแบบสเปียร์ฟิชชิงที่เจาะจงเป้าหมายผู้เสียหายเฉพาะราย แทรฟเฟอร์ดำเนินการโจมตีที่มีเป้าหมายเจาะจงมากขึ้นเช่นนี้ เพื่อตอบสนองความต้องการของลูกค้า ตัวอย่างเช่น ในกรณีที่ผู้ซื้อกำลังมองหาการเข้าถึงองค์กรหรือภาคส่วนที่มีมูลค่าสูงแบบเฉพาะเจาะจง

แทรฟเฟอร์จะส่งมัลแวร์อินโฟสตีลเลอร์ไปติดตั้งบนอุปกรณ์ของผู้เสียหายโดยใช้เทคนิคหลากหลายรูปแบบ รวมถึง

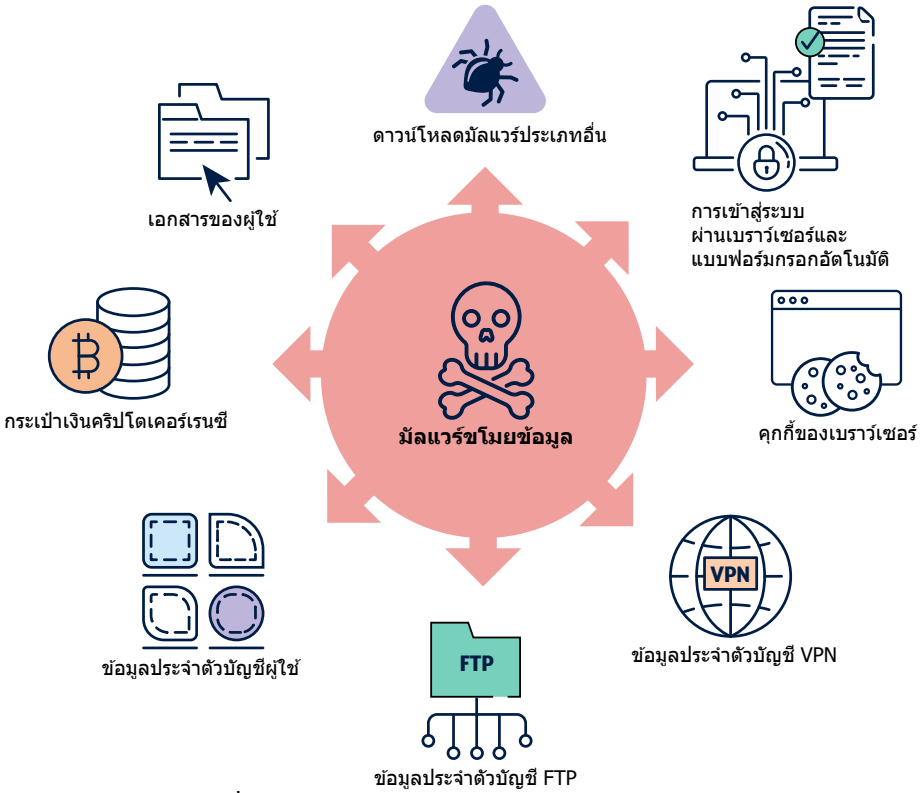
- **บ็อตเน็ต (Botnet)** ได้แก่เครือข่ายของระบบคอมพิวเตอร์ที่ถูกบุกรุกและควบคุมโดยอาชญากรไซเบอร์ เพื่อนำไปใช้ทำกิจกรรมที่เป็นอันตราย เช่น การส่งข้อความฟิชชิงหรือมัลแวร์

- **ฟิชชิง (Phishing)** ได้แก่ความพยายามในการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลสำคัญ รวมถึงการใช้อีเมลหรือข้อความถึงตรงในโซเชียลมีเดีย ฟอรั่ม และแอปส่งข้อความ ซึ่งเป็นวิธีการแพร่กระจายที่พบบ่อย ซึ่งช่วยลดอุปสรรคในการเข้าสู่วงการสำหรับอาชญากรไซเบอร์ นั่นคือ
  - ข้อความเหล่านี้มักจะมีลิงก์ที่เป็นอันตรายแนบมาด้วย แทนที่จะแนบไฟล์ที่เป็นอันตรายไปกับอีเมลโดยตรง
- **ผลการค้นหาที่เป็นอันตราย** ถูกสร้างขึ้นผ่านเทคนิคปรับแต่งผลการค้นหา (Search engine optimisation - SEO) ที่ชี้เป้าไปยังเว็บไซต์ที่ให้บริการมัลแวร์ซึ่งปลอมตัวเป็นซอฟต์แวร์หรือเนื้อหาที่ดูเหมือนถูกกฎหมาย
- **มัลเวอร์ไทซิง (Malvertising)** ได้แก่การใช้โค้ดที่เป็นอันตราย ซึ่งถูกแทรกเข้าไปอยู่ในโฆษณาออนไลน์ที่ถูกต้องตามกฎหมายเพื่อใช้ในการเผยแพร่มัลแวร์
- **ซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์** ไม่ว่าจะผ่านการดาวน์โหลดเช่น วิดีโอเกมที่ถูกแชร์ผ่านวิดีโอบนยูทูป (YouTube) โดยมีลิงก์ที่เป็นอันตรายอยู่ในคำอธิบายวิดีโอหรือช่องความคิดเห็นหรือมาจากเว็บไซต์ดาวน์โหลดที่ไม่น่าเชื่อถือ
- **โฆษณาและโพสต์บนโซเชียลมีเดีย**ที่ชี้เป้าไปยังไฟล์มัลแวร์ที่ปลอมตัวมา
- **การอัปเดตซอฟต์แวร์ที่เป็นอันตราย** มักปลอมตัวเป็นการอัปเดตเว็บเบราว์เซอร์มาหลอกผู้เสียหาย

ขั้นตอนที่ 3 การเก็บเกี่ยวข้อมูล

เมื่อมัลแวร์อินโฟสตีลเลอร์เริ่มทำงานบนอุปกรณ์ของผู้เสียหาย มันจะเริ่มเก็บรวบรวมข้อมูลที่สำคัญจากเครื่องที่ถูกบุกรุก นอกเหนือจากการขโมยข้อมูลประจำตัวของผู้ใช้แล้ว ในกรณีที่มัลแวร์อินโฟสตีลเลอร์เป็นส่วนหนึ่งของบ็อตเน็ต อาชญากรไซเบอร์ยังสามารถควบคุมอุปกรณ์ที่ถูกบุกรุกจากระยะไกลได้ โดยส่งคำสั่งการตั้งค่าเพื่อเปิดใช้งานความสามารถเพิ่มเติมหรือส่งมัลแวร์อื่นเข้าไปได้อีก โดยทั่วไป มัลแวร์อินโฟสตีลเลอร์สามารถขโมยข้อมูลได้ดังนี้

- ชื่อผู้ใช้และรหัสผ่าน โดยเฉพาะอย่างยิ่งข้อมูลที่จัดเก็บไว้ในเซสชันผู้ใช้ (User session) หรือโทเคน (Token) ของการยืนยันตัวตนแบบหลายปัจจัย (MFA) ที่อยู่ในเว็บเบราว์เซอร์
- คุกกี้สำหรับการยืนยันตัวตน (Authentication cookies)
- ข้อมูลที่กรอกอัตโนมัติในแบบฟอร์มของเว็บเบราว์เซอร์
- ข้อมูลประจำตัว เนื้อหาอีเมล และรายชื่อผู้ติดต่อในอีเมล
- ประวัติการเข้าชมเว็บไซต์
- เอกสารของผู้ใช้
- รายละเอียดบัตรเครดิต
- บันทึกการสนทนาจากแอปส่งข้อความบนเดสก์ท็อป
- ข้อมูลระบบ
- กระเป๋าเงินคริปโตเคอร์เรนซี
- ข้อมูลประจำตัวบัญชี VPN หรือโปรโตคอลการถ่ายโอนไฟล์ (File Transfer Protocol - FTP)



ภาพที่ 1. ความสามารถของมัลแวร์อินโฟสตีลเลอร์

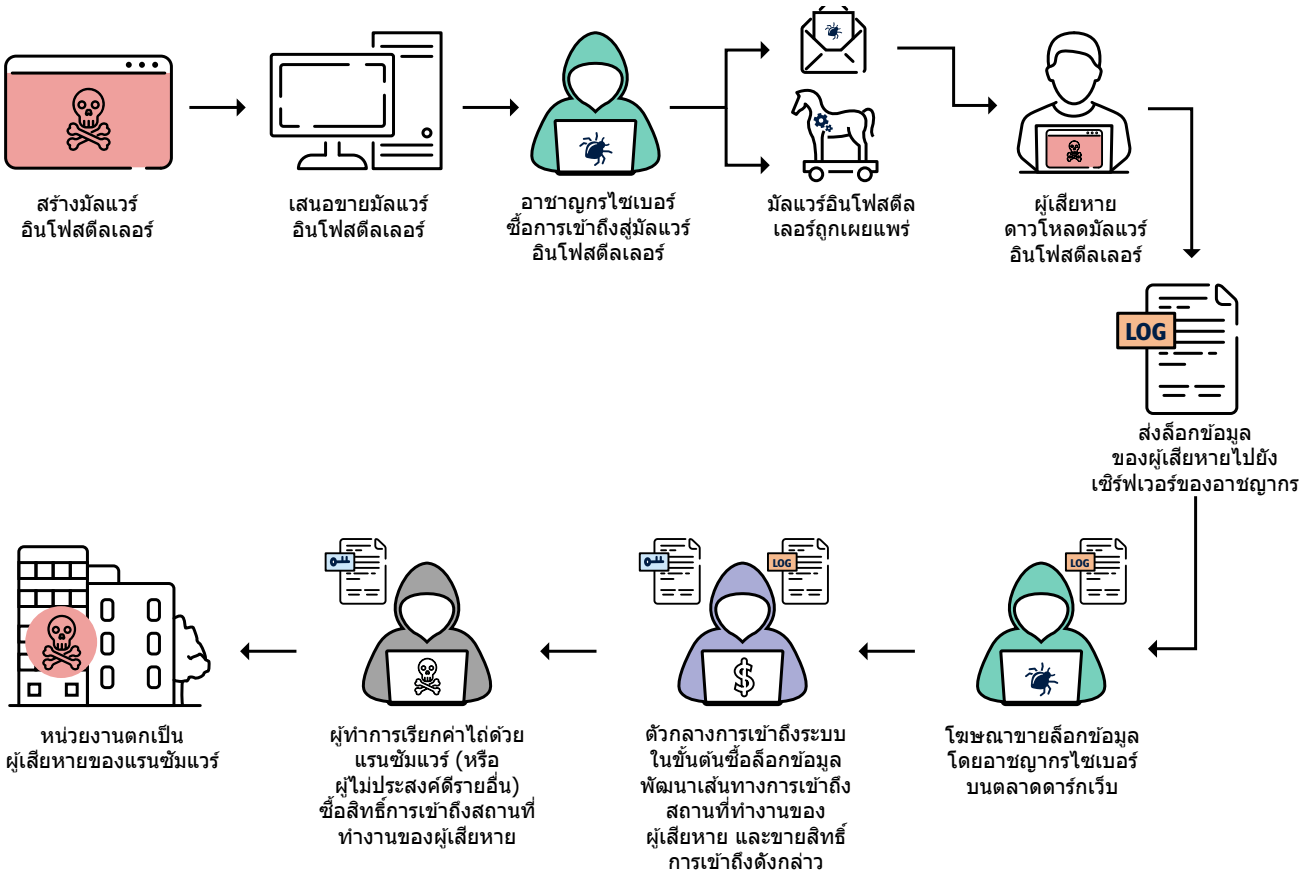
คุกกี้สำหรับการยืนยันตัวตนของเว็บเบราว์เซอร์บางตัวสามารถช่วยให้ผู้ใช้งานใช้บัญชีหรือบริการเป็นเวลาหลายวันได้ในการเข้าสู่ระบบแต่ละครั้ง โดยที่ไม่จำเป็นต้องยืนยันตัวตนใหม่ แต่หากคุกกี้สำหรับการยืนยันตัวตนเหล่านี้ถูกขโมยไป ก็อาจเปิดโอกาสให้เลี่ยงข้อกำหนดการยืนยันตัวตนแบบหลายปัจจัย (MFA) อย่างมีประสิทธิภาพเช่นกัน และอำนวยให้อาชญากรไซเบอร์เข้าถึงบัญชีผู้ใช้ของผู้เสียหาย เครือข่ายองค์กร และระบบของบริษัทได้

ขั้นตอนที่ 4 การรวบรวมและสร้างรายได้จากข้อมูล

มัลแวร์อินโฟสตีลเลอร์ถูกตั้งค่าให้ลักลอบนำข้อมูลของผู้เสียหายที่เรียกว่า 'ล็อกข้อมูล หรือ Logs' ออกไปแล้วส่งไปยังเซิร์ฟเวอร์ระบบสั่งการและควบคุมที่เป็นอันตราย โดยทั่วไป มัลแวร์อินโฟสตีลเลอร์จะใช้แอปส่งข้อความยอดนิยม เช่น Telegram และ Discord ในการแชร์ฟีดล็อกข้อมูลกับอาชญากรไซเบอร์

การซื้อขายและแลกเปลี่ยนล็อกข้อมูลหาได้จากตลาดเฉพาะทางเช่น Telegram และตามดาร์กเว็บ อาชญากรไซเบอร์สร้างรายได้จากล็อกข้อมูลเหล่านี้ในหลายรูปแบบ รวมถึง

- การขายล็อกข้อมูลบนตลาดมืดของอาชญากร รวมถึงการขายให้กับตัวกลางการเข้าถึงระบบในขั้นต้น
- การใช้ข้อมูลเหล่านั้นในการโจมตีผู้เสียหายโดยตรง ผ่านการโจรกรรมอัตลักษณ์บุคคลหรือการขู่กรรโชก
- การใช้ข้อมูลเพื่อเข้าถึงเครือข่ายองค์กรในขั้นต้นเพื่อดำเนินกิจกรรมเรียกค่าไถ่ด้วยแรมซัมแวร์



ภาพที่ 2. ระบบนิเวศมัลแวร์อินโฟสตีลเลอร์และผลกระทบที่อาจเกิดขึ้นกับองค์กร

ผลกระทบ

มัลแวร์อินโฟสตีลเลอร์อาจส่งผลกระทบรุนแรงทั้งต่อบุคคลและองค์กร เมื่อมัลแวร์อินโฟสตีลเลอร์ขโมยข้อมูลประจำตัวผู้ใช้ได้แล้ว อาชญากรไซเบอร์อาจนำข้อมูลประจำตัวเหล่านี้ไปใช้ในการเข้าถึงเครือข่ายองค์กรหรือระบบของบริษัทด้วยบัญชีผู้ใช้ที่ยังใช้งานได้อยู่ ซึ่งมักจะทำให้เจ้าของระบบไม่สามารถตรวจพบได้ในทันที

สำหรับ**องค์กร**ที่ได้รับผลกระทบจากมัลแวร์อินโฟสตีลเลอร์ ผลที่ตามมาอาจรวมถึง

- การถูกโจมตีด้วยแรนซัมแวร์
- การรั่วไหลของข้อมูล
- อีเมลทางธุรกิจถูกบุกรุก
- การขโมยทรัพย์สินทางปัญญา
- การขโมยข้อมูลสำคัญ

สำหรับ**บุคคล**ที่ได้รับผลกระทบจากมัลแวร์อินโฟสตีลเลอร์ ผลที่ตามมาอาจรวมถึง

- การเข้าถึงบัญชีอีเมลหรือโซเชียลมีเดียโดยไม่ได้รับอนุญาต
- ความเสี่ยงต่อการถูกโจรกรรมอัตลักษณ์บุคคลที่เพิ่มขึ้น
- ความเสี่ยงจากการถูกโจมตีแบบฟิชชิงเพิ่มขึ้น
- การสูญเสียเงินหรือถูกเข้าถึงบัญชีการเงินโดยไม่ได้รับอนุญาต
- การสูญเสียความเป็นส่วนตัว

กรณีศึกษา

กรณีศึกษานี้ได้รับการปกปิดข้อมูลที่ระบุตัวตนไว้ เพื่อให้สามารถเผยแพร่สู่สาธารณะได้ กรณีศึกษานี้อ้างอิงเหตุการณ์ความปลอดภัยทางไซเบอร์หลายกรณีที่ส่งผลกระทบต่อหน่วยงานในออสเตรเลีย ซึ่งได้มีการรายงานต่อ ACSC ของ ASD แล้ว ต่อไปนี้จะเรียกหน่วยงานที่ได้รับผลกระทบว่า 'องค์กร' ชื่อบุคคลในกรณีศึกษานี้เป็นนามสมมติ และมีการตัดรายละเอียดบางส่วนออกไปเพื่อปกป้องตัวตนของผู้เสียหาย

องค์กรแห่งนี้เป็นธุรกิจในออสเตรเลียที่อนุญาตให้พนักงานเข้าถึงระบบส่วนกลางได้จากอุปกรณ์ส่วนตัว อลิซเป็นพนักงานขององค์กร ซึ่งทำงานจากระยะไกล

เวลาที่เธอทำงานจากที่บ้าน อลิซจะเชื่อมต่อเข้ากับเครือข่ายส่วนกลางขององค์กรผ่านแล็ปท็อปส่วนตัวของเธอ อลิซได้**ดาวน์โหลด**โปรแกรม Notepad++ (ซึ่งเป็นซอฟต์แวร์สำหรับจดบันทึกประเภทหนึ่ง) ลงใน**แล็ปท็อปส่วนตัว**ของเธอจากเว็บไซต์ที่เชื่อว่าถูกกฎหมาย **มัลแวร์อินโฟสตีลเลอร์**ปลอมตัวเป็นไฟล์ติดตั้งของโปรแกรม Notepad++

เมื่ออลิซพยายามติดตั้งซอฟต์แวร์ดังกล่าว มัลแวร์อินโฟสตีลเลอร์ก็เริ่มทำงานและเริ่ม**เก็บเกี่ยวข้อมูลประจำตัวของผู้ใช้**จากแล็ปท็อปของเธอ ซึ่งรวมถึงชื่อผู้ใช้และรหัสผ่านสำหรับการทำงานที่เธอได้จัดเก็บไว้ในฟีเจอร์บันทึกข้อมูลอัตโนมัติที่ใช้เข้าสู่ระบบของเว็บเบราว์เซอร์ จากนั้น มัลแวร์อินโฟสตีลเลอร์ได้ส่งข้อมูลประจำตัวของผู้ใช้เหล่านั้นไปยังเซิร์ฟเวอร์ระบบสั่งการและควบคุมจากระยะไกลที่ควบคุมโดยกลุ่มอาชญากรไซเบอร์

ล็อกข้อมูลที่ถูกขโมยไปจะถูกบรรจุรวมพร้อมกับล็อกข้อมูลอื่น ๆ และนำไป**ขายให้กับอาชญากรไซเบอร์**ผ่านตลาดมืดในดาร์กเว็บ

อาชญากรไซเบอร์รายหนึ่งที่ชื่อว่า บ๊อบ ซื้อข้อมูลประจำตัวผู้ใช้ของอลิซ ซึ่งระบุถึงข้อมูลประจำตัวผู้ใช้เพื่อเข้าสู่ระบบของบริการต่าง ๆ บนเครือข่ายขององค์กรที่อลิซทำงานอยู่ องค์กรของอลิซ**ไม่ได้ตั้งค่าการยืนยันตัวตนแบบหลายปัจจัย (MFA)** สำหรับบริการเหล่านี้ ซึ่งหมายความว่าบ๊อบสามารถใช้ข้อมูลประจำตัวของผู้ใช้ที่ถูกขโมยมาเพียงอย่างเดียวเพื่อที่จะ**ยืนยันตัวตนและเข้าถึง**เครือข่ายส่วนกลางได้อย่างสำเร็จ

บ๊อบสามารถเข้าถึงเครือข่ายส่วนกลางขององค์กรของอลิซได้โดยไม่ถูกตรวจจับด้วยการใช้ข้อมูลประจำตัวของผู้ใช้ที่ถูกขโมยมา**ซึ่งยังสามารถใช้งานได้อยู่** หลังจากนั้น บ๊อบสามารถเคลื่อนย้ายภายในเครือข่ายส่วนกลาง เพื่อค้นหาข้อมูลสำคัญขององค์กร และลักลอบนำข้อมูลออกเพื่อนำไปใช้ในการเรียกค่าไถ่จากบริษัท

หลังจากขโมยข้อมูลสำคัญได้แล้ว บ๊อบ**ได้ทำการเข้ารหัสฐานข้อมูลและระบบไฟล์**ขององค์กร เพื่อกันไม่ให้ผู้อื่นเข้าถึงข้อมูลเหล่านั้นได้อีก

แนวทางบรรเทาปัญหา

องค์กรอาจไม่สามารถบังคับใช้มาตรการควบคุมกับอุปกรณ์ที่เชื่อมต่อเข้ากับเครือข่ายส่วนกลางของตนได้ โดยเฉพาะอุปกรณ์ส่วนตัวของพนักงานที่ทำงานจากระยะไกล ACSC ของ ASD ขอแนะนำให้องค์กรให้ความสำคัญกับการนำมาตรการเพื่อป้องกันตนเองจากความเสี่ยงที่เกิดจากมัลแวร์อินโฟสตีลเลอร์ ซึ่งมุ่งเป้าไปยังข้อมูลประจำตัวของผู้ใช้ออกใช้งาน แนวทางในการบรรเทาปัญหานี้ ได้แก่

ให้การฝึกอบรมความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์แก่พนักงาน

- ป้องกันมิให้การโจมตีทางวิศวกรรมสังคม (Social engineering) ที่มีเป้าหมายเฉพาะประสบผลสำเร็จ และป้องกันการดาวน์โหลดไฟล์ที่เป็นอันตรายโดยให้การฝึกอบรมที่มีประสิทธิภาพกับพนักงาน
- ยกระดับความตระหนักรู้เกี่ยวกับมัลแวร์อินโฟสตีลเลอร์ วิธีการแพร่กระจาย และภัยคุกคามจากฟิชชิงที่อาจส่งผลกระทบต่อองค์กร

รักษาความปลอดภัยให้กับบัญชีองค์กร

- นำ MFA ออกใช้งาน
- นำ MFA ออกใช้งานกับบริการภายนอกและภายใน ระบบต่าง ๆ และแหล่งเก็บข้อมูลสำคัญ โดยเฉพาะอีเมลผ่านเว็บ (Webmail) บริการ VPN และบัญชีผู้ใช้งานที่มีสิทธิพิเศษซึ่งสามารถเข้าถึงระบบสำคัญได้ แนวทางปฏิบัติที่ดีที่สุดคือการใช้ MFA ที่ทนทานต่อการโจมตีแบบฟิชชิงกับทุกบัญชี
- ปิดใช้งานบัญชีผู้ใช้เมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว
- จำกัดสิทธิพิเศษผู้ดูแลระบบ
- ทำงานด้านการจัดการดูแลเครือข่ายและงานที่ต้องใช้สิทธิพิเศษโดยใช้คอมพิวเตอร์ที่จำกัดเฉพาะการใช้งานและปลอดภัยเท่านั้น (เช่น เวิร์กสเตชันสำหรับผู้ดูแลระบบที่ตั้งค่าความปลอดภัยไว้แล้ว)
- ปฏิบัติตามแนวทางที่ดีโดยให้สิทธิพิเศษเท่าที่จำเป็น (Least-privilege) ด้วยการกำหนดให้ผู้ดูแลระบบใช้บัญชีผู้ใช้ที่มีสิทธิพิเศษเฉพาะในการจัดการระบบ และใช้บัญชีผู้ใช้ทั่วไปในการทำงานอื่นที่ไม่ใช่งานดูแลระบบ
- ป้องกันไม่ให้บัญชีผู้ใช้ที่มีสิทธิพิเศษ (ยกเว้นบัญชีที่ได้รับอนุญาตเป็นกรณีพิเศษ) เข้าถึงอินเทอร์เน็ต อีเมล และบริการเว็บต่าง ๆ
- พิจารณานำการบริหารจัดการแบบทันเวลาพอดี (Just-in-time) ออกใช้งานสำหรับระบบและแอปพลิเคชัน โดยให้สิทธิ์เฉพาะเมื่อจำเป็นในช่วงเวลาที่กำหนดเท่านั้น
- บังคับใช้นโยบายการจัดการและตรวจสอบบัญชีผู้ใช้ที่มีสิทธิพิเศษ
- เปลี่ยนรหัสผ่านเป็นระยะ ๆ โดยเฉพาะบัญชีที่ใช้เข้าระบบจากภายนอกที่ผ่านการเข้าถึงจากระยะไกลด้วยอินเทอร์เน็ต
- บังคับใช้การหมดอายุของเซสชัน และนโยบายการยุติการใช้งาน (Sunset policies) สำหรับโทเคนและคุกกี้

เสริมสร้างความปลอดภัยให้กับอุปกรณ์เคลื่อนที่ขององค์กร

- ดำเนินการประเมินความเสี่ยงด้านการใช้งานอุปกรณ์เคลื่อนที่ในองค์กร และนำแนวทางเสริมสร้างความปลอดภัยให้กับอุปกรณ์เคลื่อนที่ขององค์กรออกใช้งาน
- หากองค์กรอนุญาตให้พนักงานใช้อุปกรณ์ส่วนตัวในการทำงาน ควรนำนโยบายการใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device - BYOD) ออกใช้งาน เนื่องจากอุปกรณ์ที่องค์กรบริหารจัดการจะมีความปลอดภัยมากกว่าอุปกรณ์ส่วนตัวที่ไม่ได้รับการจัดการ

ตรวจสอบและประเมินความเสี่ยงในห่วงโซ่อุปทานจากผู้ให้บริการภายนอกที่เข้าถึงเครือข่ายขององค์กร รวมถึงผู้ให้บริการซอฟต์แวร์ (Software-as-a-Service หรือ SaaS) และผู้ให้บริการแบบมีการจัดการ (Managed Service Providers)

วิธีบริหารจัดการความปลอดภัยเมื่อใช้งานผู้ให้บริการแบบมีการจัดการ (How to Manage Your Security When Engaging a Managed Service Provider)

ปกป้องเครือข่ายส่วนกลางขององค์กร

- อัปเดตแอปพลิเคชันและระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดอยู่เสมอ
- ใช้นโยบายความปลอดภัยภายในเครื่องเพื่อบังคับใช้นโยบายควบคุมแอปพลิเคชันด้วยการกำหนดรายการที่อนุญาตอย่างเข้มงวด (Strict allow list)
- นำการแบ่งส่วนเครือข่าย (Network segmentation) ออกใช้งาน เพื่อแยกส่วนเครือข่ายตามบทบาทและหน้าที่การทำงาน
- ตรวจสอบและเฝ้าระวังกิจกรรมของผู้ใช้งานโดยเฉพาะพนักงานที่ทำงานจากระยะไกล
- การเฝ้าระวังบัญชีที่มีสิทธิพิเศษสามารถช่วยตรวจจับการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต หรือกิจกรรมการโอนถ่ายข้อมูลที่ผิดปกติ เช่น การอัปโหลดข้อมูลจำนวนมากไปยังเครือข่ายภายนอก
- นำนโยบายและเครื่องมือป้องกันการรั่วไหลของข้อมูล (Data-loss prevention) ออกใช้งานเพื่อป้องกันการส่งข้อมูลโดยไม่ได้รับอนุญาต เพื่อป้องกันการถ่ายโอนข้อมูลโดยไม่ได้รับอนุญาต

เข้าร่วมเป็นพันธมิตรเครือข่ายการรักษาความปลอดภัยทางไซเบอร์ของ ASD (ASD Cyber Security Network Partner) และเข้าร่วมใช้บริการแบ่งปันข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence Sharing - CTIS) ของ ASD

- CTIS เป็นแพลตฟอร์มแบ่งปันข้อมูลแบบสองทาง ซึ่งเปิดโอกาสให้พันธมิตรจากภาครัฐและภาคอุตสาหกรรมให้สามารถรับและแบ่งปันข้อมูลเกี่ยวกับกิจกรรมทางไซเบอร์ที่เป็นอันตรายได้
- ACSC ของ ASD กำลังติดตามกิจกรรมการเคลื่อนไหวของมัลแวร์อินโฟสตีลเลอร์และแบ่งปันรายละเอียดเกี่ยวกับโครงสร้างพื้นฐานของเซิร์ฟเวอร์ระบบสั่งการและควบคุมมัลแวร์ที่ทำงานอยู่ผ่านแพลตฟอร์ม CTIS
- สมัครเข้าร่วมเป็นพันธมิตรและช่วยปกป้องค์กรของคุณ รวมถึงข้อมูลลูกค้าจากภัยคุกคามของอาชญากรไซเบอร์

เตรียมพร้อมรับมือเมื่อระบบถูกบุกรุก

- จัดทำแผนรับมือเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ เพื่อใช้ในกรณีที่ถูกมัลแวร์อินโฟสตีลเลอร์บุกรุกระบบ ให้แน่ใจว่าพนักงานรู้ว่าจะต้องทำอย่างไร และควรติดต่อใครหากสงสัยว่าตนได้ดาวน์โหลดไฟล์ที่ต้องสงสัยมาแล้ว

การนำแนวทาง Essential Eight จาก ACSC ของ ASD ออกใช้งาน

- นอกเหนือจากแนวทางบรรเทาปัญหาที่กล่าวมาข้างต้น ACSC ของ ASD ขอแนะนำให้นำแนวทางสำคัญแปดประการ หรือ Essential Eight ที่เหลือออกใช้งาน

คำแนะนำสำหรับพนักงานเมื่อต้องทำงานจากระยะไกล

- ปกป้องข้อมูลของคุณบนอุปกรณ์ส่วนตัว
  - พัฒนาให้มีกิจวัตรความปลอดภัยทางไซเบอร์ที่ดี เช่น หลีกเลี่ยงการคลิกลิงก์หรือป๊อปอัปที่น่าสงสัย หรือไม่ดาวน์โหลดไฟล์หรือซอฟต์แวร์จากแหล่งข้อมูลที่ไม่รู้จักหรือไม่น่าเชื่อถือ
  - ใช้รหัสผ่านที่แตกต่างกันสำหรับบัญชีงานและบัญชีส่วนตัว เปิดใช้งาน MFA สำหรับบัญชีส่วนตัวหากเป็นไปได้
  - อย่าบันทึกข้อมูลประจำตัวที่เกี่ยวกับงานไว้ในตัวจัดการรหัสผ่านส่วนบุคคล ยกเว้นได้รับอนุญาตจากนายจ้างอย่างชัดเจน ซึ่งรวมถึงฟีเจอร์จัดการรหัสผ่านของเว็บเบราว์เซอร์ด้วย **หากไม่แน่ใจ ควรขอให้นายจ้างของคุณจัดหาเครื่องมือจัดการรหัสผ่านที่องค์กรให้การสนับสนุน**
  - หลีกเลี่ยงการเข้าสู่ระบบบัญชีงานจากคอมพิวเตอร์สาธารณะหรือเครื่องที่ใช้ร่วมกัน
  - ระวังข้อมูลที่ถูกบันทึกอยู่ในฟีเจอร์กรอกอัตโนมัติของเว็บเบราว์เซอร์ของคุณ เนื่องจากมัลแวร์อินโฟสตีลเลอร์จะมุ่งเป้าไปที่ข้อมูลซึ่งเว็บเบราว์เซอร์บันทึกไว้เพื่อใช้กรอกแบบฟอร์มอัตโนมัติ หากต้องกรอกแบบฟอร์มบนเว็บไซต์ ควรกรอกข้อมูลสำคัญด้วยตัวเองทุกครั้ง เช่น หมายเลขบัตรเครดิต แทนที่จะบันทึกไว้ในฟีเจอร์กรอกข้อมูลแบบอัตโนมัติของเว็บเบราว์เซอร์
  - ออกจากระบบจากทุกบริการออนไลน์และล้างคุกกี้ของเว็บเบราว์เซอร์หลังการใช้งาน เพื่อช่วยลดข้อมูลที่มัลแวร์อินโฟสตีลเลอร์สามารถขโมยไปได้
  - ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานโปรแกรมป้องกันไวรัสที่ติดมากับระบบปฏิบัติการ หากใช้โปรแกรมป้องกันไวรัสจากผู้ให้บริการภายนอก ควรตรวจสอบให้แน่ใจได้ว่ามีการอัปเดตอยู่เสมอ และเป็นซอฟต์แวร์จากผู้ให้บริการที่เชื่อถือได้

ความช่วยเหลือ

องค์กรในออสเตรเลียที่ได้รับผลกระทบหรือต้องการความช่วยเหลือเกี่ยวกับเหตุการณ์ถูกโจมตีจากมัลแวร์อินโฟสตีลเลอร์ สามารถติดต่อ ACSC ของ ASD ได้ที่หมายเลข **1300 CYBER1 (1300 292 371)** หรือโดยการส่งรายงานผ่านเว็บเซต์ cyber.gov.au/report

ACSC ของ ASD ขอสนับสนุนให้องค์กรรายงานกิจกรรมเครือข่ายที่น่าสงสัยและตัวบ่งชี้การถูกโจมตีที่เกี่ยวข้องกับมัลแวร์ขโมยอินโฟสตีลเลอร์ แม้ว่าเหตุการณ์นั้นจะอยู่ในขอบเขตที่ควบคุมได้หรือยุติลงแล้วก็ตาม เราใช้ข้อมูลที่คุณให้มาเพื่อพัฒนาความเข้าใจของเราเกี่ยวกับกลยุทธ เทคนิค และวิธีการที่ผู้ปฏิบัติที่เป็นภัยคุกคามทางไซเบอร์ใช้ ซึ่งจะช่วยให้เราสามารถแจ้งเตือนองค์กรอื่นในออสเตรเลียที่อาจตกเป็นเป้าหมายในลักษณะเดียวกันได้

ข้อจำกัดความรับผิดชอบ

เนื้อหาในคู่มือนี้มีลักษณะทั่วไปและไม่ควรยึดถือว่าเป็นคำแนะนำทางกฎหมายหรือเป็นที่พึ่งสำหรับความช่วยเหลือในสถานการณ์เฉพาะหรือสถานการณ์ฉุกเฉินใด ๆ ในเรื่องที่สำคัญใด ๆ คุณควรขอคำแนะนำจากผู้เชี่ยวชาญอิสระที่เหมาะสมกับสถานการณ์ของคุณเอง

เครือรัฐจะไม่รับผิดชอบหรือมีส่วนรับผิดต่อความเสียหาย การสูญเสีย หรือค่าใช้จ่ายที่เกิดขึ้นจากการพึ่งพาข้อมูลที่มีอยู่ในคู่มือนี้

สงวนลิขสิทธิ์

สำหรับข้อมูลเพิ่มเติมหรือรายงานเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ ติดต่อเราที่

เว็บไซต์ cyber.gov.au | โทร 1300 CYBER1 (1300 292 371)

หมายเลขนี้มีไว้สำหรับใช้ภายในออสเตรเลียเท่านั้น

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre