ข้อแนะนำเกี่ยวกับ APT40

กลยุทธ์ของกระทรวงความมั่นคงแห่งรัฐ (MSS) สาธารณรัฐประชาชนจีน (PRC)

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

สารบัญ

ภาพรวม 5

ความเป็นมา 5

บทสรุปกิจกรรม 5

กลยุทธ์ที่ควรสังเกต 6

การใช้เครื่องมือ 7

กรณีศึกษา 7

กรณีศึกษาที่ 1 8

บทสรุปสำหรับผู้บริหาร 8

ผลการสืบสวน 9

รายละเอียด 9

แผนภาพลำดับเหตุการณ์ 9

รายละเอียดการลำดับเหตุการณ์ 10

กลยุทธ์และเทคนิคของผู้ปฏิบัติการ 11

การสอดแนม 11

การเข้าถึงในขั้นต้น 11

การดำเนินการ 11

การเข้าถึงข้อมูลประจำตัว 11

การแทรกซึมต่อภายในเครือข่าย 11

การรวบรวมข้อมูล 11

การลักลอบนำข้อมูลออก 11

กรณีศึกษาที่ 2 12

บทสรุปสำหรับผู้บริหาร 12

ผลการสืบสวน 13
สรุปผลการสืบสวน 13
โฮสต์ภายในระบบเครือข่าย 13
ลำดับเหตุการณ์การสืบสวน 14
กลยุทธ์และเทคนิคของผู้ปฏิบัติการ 15
การเข้าถึงในขั้นต้น 15
การดำเนินการ 15
การฝังตัวในระบบ 15
การยกระดับสิทธิพิเศษ 15
การเข้าถึงข้อมูลประจำตัว 15
การค้นพบ 16
การรวบรวมข้อมูล 16
ระบบสั่งการและควบคุม 16
คำแนะนำด้านการตรวจจับและบรรเทาปัญหา 17
การตรวจจับ 17
การบรรเทาปัญหา 20
MITRE ATT&CK – ประวัติย้อนหลัง กลยุทธ์ที่น่าสนใจของ APT40 22

ภาพรวม

ความเป็นมา

ข้อแนะนำฉบับนี้ จัดทำโดยศูนย์รักษาความปลอดภัยทางไซเบอร์ออสเตรเลียของหน่วยข่าวกรองสัญญาณออสเตรเลีย (Australian Signals Directorate's Australian Cyber Security Centre - ASD's ACSC) หน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานสหรัฐอเมริกา (United States Cybersecurity and Infrastructure Security Agency - CISA) หน่วยงานรักษาความปลอดภัยแห่งชาติสหรัฐอเมริกา (United States National Security Agency - NSA) สำนักงานสอบสวนกลางสหรัฐอเมริกา (Federal Bureau of Investigation - FBI) ศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งชาติสหราชอาณาจักร (United Kingdom National Cyber Security Centre - NCSC-UK) ศูนย์รักษาความปลอดภัยทางไซเบอร์แคนาดา (Canadian Centre for Cyber Security - CCCS) ศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งชาตินิวซีแลนด์ (New Zealand National Cyber Security Centre - NCSC-NZ) สำนักงานข่าวกรองกลางแห่งสหพันธรัฐเยอรมัน (German Federal Intelligence Service - BND) และสำนักงานสหพันธรัฐเพื่อการปกป้องรัฐธรรมนูญ (Federal Office for the Protection of the Constitution - BfV) สำนักงานข่าวกรองแห่งชาติของสาธารณรัฐเกาหลี (Republic of Korea's National Intelligence Service - NIS) และศูนย์ความปลอดภัยทางไซเบอร์แห่งชาติของ NIS (NIS' National Cyber Security Center) และศูนย์เตรียมความพร้อมต่อเหตุการณ์และยุทธศาสตร์ด้านความปลอดภัยไซเบอร์แห่งชาติของญี่ปุ่น (Japan's National Center of Incident Readiness and Strategy for Cybersecurity - NISC) และสำนักงานตำรวจแห่งชาติของญี่ปุ่น (National Police Agency - NPA) ซึ่งต่อไปนี้จะเรียกรวมว่า "หน่วยงานผู้ร่วมจัดทำ" โดยที่เอกสารจะมีเนื้อหาเกี่ยวกับกลุ่มปฏิบัติการไซเบอร์ที่ได้รับการสนับสนุนจากรัฐบาลรัฐของสาธารณรัฐประชาชนจีน (People's Republic of China - PRC) และภัยคุกคามที่กลุ่มดังกล่าวมีต่อเครือข่ายของออสเตรเลียในปัจจุบัน ข้อแนะนำฉบับนี้อ้างอิงจากความเข้าใจเกี่ยวกับภัยคุกคามที่หน่วยงานผู้ร่วมจัดทำมีร่วมกัน ตลอดจนผลการสืบสวนด้านการตอบสนองต่อเหตุการณ์ภายใต้ ACSC ของ ASD

กลุ่มปฏิบัติการไซเบอร์ที่ได้รับการสนับสนุนจากรัฐบาลรัฐของสาธารณรัฐประชาชนจีน (PRC) เคยโจมตีองค์กรในหลายประเทศ รวมถึงออสเตรเลียและสหรัฐอเมริกา และกลุ่มผู้ปฏิบัติการอื่น ๆ ที่ได้รับการสนับสนุนจากรัฐบาลรัฐของสาธารณรัฐประชาชนจีนก็ยังคงใช้เทคนิคที่ระบุไว้ด้านล่างนี้ในการปฏิบัติการทั่วโลกอย่างสม่ำเสมอ ดังนั้น หน่วยงานผู้ร่วมจัดทำจึงเชื่อว่ากลุ่มดังกล่าว รวมถึงเทคนิคในลักษณะที่คล้ายคลึงกันนี้ ยังคงเป็นภัยคุกคามต่อเครือข่ายของประเทศผู้ร่วมจัดทำเช่นกัน

หน่วยงานผู้ร่วมจัดทำประเมินว่า กลุ่มนี้ดำเนินการปฏิบัติการทางไซเบอร์ที่เป็นอันตรายให้กับกระทรวงความมั่นคงแห่งรัฐ (Ministry of State Security - MSS) ของสาธารณรัฐประชาชนจีน กิจกรรมและเทคนิคที่ใช้มีความทับซ้อนกับกลุ่มที่ถูกติดตามในชื่อ Advanced Persistent Threat (APT) 40 (ยังรู้จักกันในชื่อ Kryptonite Panda, GINGHAM TYPHOON, Leviathan และ Bronze Mohawk ตามรายงานจากภาคอุตสาหกรรม) มีการรายงานว่ากลุ่มนี้เคยมีฐานปฏิบัติการอยู่ในเมืองไหโข่ว (Haikou) มณฑลไห่หนาน (Hainan) ของสาธารณรัฐประชาชนจีน และได้รับภารกิจจากกระทรวงความมั่นคงแห่งรัฐ (MSS) สาธารณรัฐประชาชนจีนผ่านทางสำนักงานความมั่นคงมณฑลไห่หนาน (Hainan State Security Department)[2] ข้อแนะนำต่อไปนี้นำเสนอกรณีศึกษาตัวอย่างที่มีนัยสำคัญ ซึ่งแสดงให้เห็นถึงเทคนิคที่กลุ่มภัยคุกคามนี้ใช้ดำเนินการกับเครือข่ายของผู้เสียหายสองราย กรณีศึกษาทั้งสองนี้มีความสำคัญต่อผู้ปฏิบัติงานด้านความมั่นคงทางไซเบอร์เพื่อใช้ในการระบุ ป้องกัน และแก้ไขปัญหาการบุกรุกจากกลุ่ม APT40 ที่อาจเกิดขึ้นกับเครือข่ายของตนเอง กรณีศึกษาที่เลือกมานี้เป็นเหตุการณ์ที่ได้มีการดำเนินการแก้ไขอย่างเหมาะสมแล้ว ซึ่งช่วยลดความเสี่ยงในการถูกผู้ปฏิบัติการที่เป็นภัยคุกคามดังกล่าวหรือกลุ่มอื่นที่เกี่ยวข้องมาหาประโยชน์ด้วยการโจมตีซ้ำอีก แม้ว่ากรณีศึกษาจะเป็นเหตุการณ์ในอดีต แต่นำมาเผยแพร่เพื่อให้องค์กรต่าง ๆ มีเวลาเพียงพอในการดำเนินการแก้ไขปัญหาได้อย่างเหมาะสม

บทสรุปกิจกรรม

กลุ่ม APT40 ได้โจมตีเครือข่ายของออสเตรเลีย รวมถึงเครือข่ายของรัฐบาลและภาคเอกชนในภูมิภาคซ้ำแล้วซ้ำเล่า และภัยคุกคามที่กลุ่มนี้ก่อให้กับเครือข่ายของเรายังคงดำเนินต่อไป กลยุทธ์ที่อธิบายไว้ในข้อแนะนำฉบับนี้สังเกตพบได้เป็นประจำในการโจมตีเครือข่ายของออสเตรเลีย

สิ่งที่น่าสังเกตคือ กลุ่ม APT40 สามารถดัดแปลงและประยุกต์หาประโยชน์จากโค้ดต้นแบบสำหรับการโจมตีช่องโหว่ (Proof-of-Concept หรือ POC) ได้อย่างรวดเร็ว และนำมาใช้โจมตีเครือข่ายเป้าหมายที่มีโครงสร้างพื้นฐานเกี่ยวข้องกับช่องโหว่นั้นได้อย่างทันทีทันใด กลุ่ม APT40 มักดำเนินการสอดแนม (Reconnaissance) เครือข่ายที่ตนสนใจ รวมถึงเครือข่ายในประเทศของหน่วยงานผู้ร่วมจัดทำเพื่อหาช่องทางในการบุกรุกเป้าหมาย การสอดแนมเป็นประจำเช่นนี้ ช่วยให้กลุ่มสามารถระบุอุปกรณ์ที่มีช่องโหว่ อุปกรณ์ที่หมดอายุการใช้งาน หรือไม่มีการดูแลรักษาแล้วของเครือข่ายเป้าหมาย และเพื่อดำเนินการหาประโยชน์ด้วยการโจมตีอย่างรวดเร็ว กลุ่ม APT40 ยังคงประสบความสำเร็จในการหาประโยชน์จากช่องโหว่ที่มีมานานตั้งแต่ปี 2017 เป็นต้นมา

กลุ่ม APT40 มักจะหาประโยชน์จากช่องโหว่ที่มีการเปิดเผยต่อสาธารณะใหม่ ๆ อย่างรวดเร็วในซอฟต์แวร์ที่ใช้งานกันอย่างแพร่หลาย เช่น Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) และ Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473) ACSC ของ ASD และหน่วยงานผู้ร่วมจัดทำข้อแนะนำนี้ คาดว่ากลุ่มดังกล่าวจะยังใช้โค้ดต้นแบบ (POC) สำหรับช่องโหว่ที่มีความสำคัญสูงทันทีที่มีการเปิดเผยต่อสาธารณะภายในไม่กี่ชั่วโมงหรือไม่กี่วัน

2 กระทรวงยุติธรรมของสหรัฐอเมริกา 2021 ประชาชนสัญชาติจีน 4 คนที่ทำงานร่วมกับกระทรวงความมั่นคงแห่งรัฐ ถูกตั้งข้อหาปฏิบัติการแฮกเครือข่ายคอมพิวเตอร์ในระดับโลกที่มุ่งเป้าข้อมูลทรัพย์สินทางปัญญาและข้อมูลทางธุรกิจที่เป็นความลับ รวมถึงงานวิจัยด้านโรคติดต่อ

ภาพที่ 1. แผนผังกลยุทธ์ เทคนิค และขั้นตอนปฏิบัติ (TTP) สำหรับกิจกรรมของกลุ่ม APT40

กลุ่มนี้ดูเหมือนจะให้ความสำคัญกับการหาประโยชน์จากระบบโครงสร้างพื้นฐานที่เปิดเผยต่อสาธารณะและมีช่องโหว่มากกว่าการใช้เทคนิคที่ต้องอาศัยการโต้ตอบกันของผู้ใช้ เช่น การโจมตีแบบฟิชชิง และให้ลำดับความสำคัญสูงกับการขโมยข้อมูลประจำตัวที่ยังใช้งานได้อยู่ เพื่อนำไปใช้ในการดำเนินการอื่น ๆ ต่อไป กลุ่ม APT40 มักใช้เว็บเชลล์ (Web shells) (T1505.003) เสมอเพื่อฝังตัวในระบบ โดยเฉพาะในระยะแรกของวงจรการบุกรุก โดยปกติแล้วหลังจากเข้าถึงระบบของผู้เสียหายได้สำเร็จ กลุ่ม APT40 จะมุ่งเน้นฝังตัวในระบบเพื่อรักษาการเข้าถึงในสภาพแวดล้อมของผู้เสียหาย อย่างไรก็ตาม เนื่องจากการฝังตัวในระบบมักเกิดขึ้นในช่วงเริ่มต้นของการบุกรุก จึงมีแนวโน้มที่จะถูกสังเกตพบได้ในการบุกรุกทุกกรณี ไม่ว่าขอบเขตการโจมตีจะเป็นเช่นไรหรือมีการเข้าควบคุมระบบมากน้อยเพียงใด

กลยุทธ์ที่ควรสังเกต

แม้ว่ากลุ่ม APT40 เคยใช้เว็บไซต์ของออสเตรเลียที่ถูกบุกรุกเป็นโฮสต์สำหรับระบบสั่งการและควบคุม (Command and control - C2) ในปฏิบัติการของตนมาก่อน แต่ปัจจุบันกลุ่มนี้ได้พัฒนาเทคนิคดังกล่าวให้ก้าวหน้าไปอีกขั้นแล้ว (T1594)

กลุ่ม APT40 ได้ปรับใช้แนวโน้มระดับโลก คือ การใช้เครื่องอุปกรณ์ที่ถูกบุกรุก รวมถึงอุปกรณ์ในสำนักงานขนาดเล็กหรือสำนักงานในบ้าน (Small-office/home-office - SOHO) เป็นโครงสร้างพื้นฐานสำหรับปฏิบัติการและเป็นตัวเปลี่ยนทิศทางสุดท้าย (Last-hop redirectors) (T1584.008) ในการปฏิบัติการในออสเตรเลีย เทคนิคนี้ช่วยให้หน่วยงานผู้ร่วมจัดทำสามารถระบุและติดตามการเคลื่อนไหวของกลุ่มนี้ได้ดีขึ้น

อุปกรณ์ SOHO จำนวนมากเหล่านี้หมดอายุการใช้งานหรือยังไม่ได้รับการอัปเดตแพตช์ ทำให้ตกเป็นเป้าหมายที่ง่ายต่อการหาประโยชน์จากการโจมตีแบบ N-day เมื่ออุปกรณ์ SOHO ถูกบุกรุก อุปกรณ์เหล่านี้จะกลายเป็นจุดเริ่มต้นของการโจมตีที่ถูกออกแบบมาให้กลมกลืนกับปริมาณการรับส่งข้อมูลที่ถูกต้องจริง และสร้างความยากลำบากให้กับผู้ดูแลป้องกันระบบเครือข่าย (T1001.003)

เทคนิคนี้ยังถูกใช้อย่างสม่ำเสมอในกลุ่มผู้ปฏิบัติการรายอื่นทั่วโลกที่ได้รับการสนับสนุนจากรัฐบาลรัฐของสาธารณรัฐประชาชนจีน และหน่วยงานผู้ร่วมจัดทำข้อแนะนำนี้มองว่าเป็นภัยคุกคามร่วมกัน สำหรับข้อมูลเพิ่มเติม โปรดดูข้อแนะนำร่วมที่ชื่อว่า กลุ่มผู้ปฏิบัติการไซเบอร์ที่ได้รับการสนับสนุนโดยรัฐบาลรัฐของสาธารณรัฐประชาชนจีนเพื่อหาประโยชน์จากผู้ให้บริการเครือข่ายและอุปกรณ์ และ กลุ่มผู้ปฏิบัติการที่ได้รับการสนับสนุนโดยรัฐบาลรัฐของสาธารณรัฐประชาชนจีนเพื่อบุกรุกและฝังตัวในระบบโครงสร้างพื้นฐานสำคัญของสหรัฐฯ อย่างต่อเนื่อง

กลุ่ม APT40 ใช้โครงสร้างพื้นฐานที่จัดซื้อหรือเช่าเป็นโครงสร้างพื้นฐาน C2 ที่ใช้ติดต่อกับผู้เสียหายในการปฏิบัติการของตนเป็นครั้งคราว อย่างไรก็ตาม กลยุทธ์นี้ดูเหมือนจะมีการใช้น้อยลงเมื่อเปรียบเทียบกับในอดีต

การใช้เครื่องมือ

ACSC ของ ASD กำลังแบ่งปันไฟล์อันตรายบางไฟล์ที่ตรวจพบในระหว่างการสืบสวนตามที่แจกแจงไว้ด้านล่างนี้ ไฟล์เหล่านี้ถูกอัปโหลดไปยัง VirusTotal เพื่อให้ชุมชนในวงกว้างด้านการป้องกันเครือข่ายและความปลอดภัยทางไซเบอร์สามารถเข้าใจภัยคุกคามที่จำเป็นต้องรับมือได้ดียิ่งขึ้น

กรณีศึกษา

ACSC ของ ASD กำลังเผยแพร่รายงานการสืบสวนที่ได้รับการปกปิดข้อมูลที่ระบุตัวตนไว้จำนวนสองฉบับเพื่อให้เกิดความตระหนักรู้เกี่ยวกับวิธีที่กลุ่มผู้ปฏิบัติการใช้เครื่องมือและกลยุทธ์ของตน

MD5	ชื่อไฟล์	ข้อมูลเพิ่มเติม
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

กรณีศึกษาที่ 1

รายงานฉบับนี้ได้รับการปกปิดข้อมูลที่ระบุตัวตนไว้ เพื่อให้สามารถเผยแพร่อย่างกว้างขวางได้ ต่อไปนี้จะเรียกองค์กรที่ได้รับผลกระทบว่า 'องค์กร' รายละเอียดบางส่วนได้ถูกลบออกเพื่อปกป้องตัวตนของผู้เสียหายและวิธีการรับมือเหตุการณ์ภายใต้ ACSC ของ ASD

บทสรุปสำหรับผู้บริหาร

รายงานฉบับนี้ให้รายละเอียดผลการสืบสวนภายใต้ ACSC ของ ASD เกี่ยวกับเหตุการณ์ที่เครือข่ายขององค์กรแห่งหนึ่งถูกบุกรุกระบบจนสำเร็จ ระหว่างเดือนกรกฎาคมถึงกันยายน ปี 2022 รายงานการสืบสวนฉบับนี้จัดทำขึ้นเพื่อมอบให้กับองค์กรดังกล่าว โดยสรุปกิจกรรมที่เป็นอันตราย ซึ่งสังเกตพบ และให้กรอบคำแนะนำการแก้ไขปัญหา ผลการตรวจสอบบ่งชี้ว่าการบุกรุกระบบครั้งนี้ดำเนินการโดยกลุ่ม APT40

ช่วงกลางเดือนสิงหาคม ACSC ของ ASD ได้แจ้งให้องค์กรทราบถึงการโต้ตอบที่เป็นอันตรายต่อเครือข่ายขององค์กรจากอุปกรณ์ที่น่าจะถูกบุกรุกซึ่งกลุ่มดังกล่าวใช้ในช่วงปลายเดือนสิงหาคม และด้วยความยินยอมจากองค์กร ทาง ACSC ของ ASD จึงได้นำเซ็นเซอร์ที่ติดกับโฮสต์ (Host-based sensors) ไปลงในอุปกรณ์โฮสต์ที่คาดว่าน่าจะได้รับผลกระทบบนเครือข่ายขององค์กร เซ็นเซอร์เหล่านี้ช่วยให้นักวิเคราะห์ตอบสนองต่อเหตุการณ์ภายใต้ ACSC ของ ASD ดำเนินการสืบสวนด้วยนิติเวชดิจิทัล (Digital forensics) อย่างละเอียดได้ นักวิเคราะห์จาก ACSC ของ ASD ประสบความสำเร็จในการทำแผนที่กิจกรรมของกลุ่มผู้โจมตี และสร้างลำดับเหตุการณ์ที่สังเกตพบได้อย่างละเอียดโดยอาศัยข้อมูลจากเซ็นเซอร์ที่มีอยู่

ตั้งแต่เดือนกรกฎาคมถึงสิงหาคม กิจกรรมหลักของผู้ปฏิบัติการที่ ACSC ของ ASD สังเกตพบได้แก่

- การแจงนับข้อมูลโฮสต์ (Host enumeration) ซึ่งช่วยให้ผู้ปฏิบัติการสามารถสร้างแผนที่เครือข่ายของตนเองได้
- การใช้เว็บเชลล์ ซึ่งช่วยให้ผู้ปฏิบัติการมีที่มั่นเข้าถึงเครือข่ายในขั้นต้นและสามารถดำเนินการสั่งการได้ และ
- การติดตั้งเครื่องมืออื่น ๆ ซึ่งปรับใช้โดยผู้ปฏิบัติการสำหรับดำเนินกิจกรรมตามวัตถุประสงค์ที่เป็นอันตรายได้

จากการสืบสวนพบว่ามีหลักฐานการเข้าถึงข้อมูลสำคัญจำนวนมาก และมีหลักฐานที่บ่งชี้ว่ากลุ่มผู้ปฏิบัติการได้มีการแทรกซึมต่อภายในเครือข่าย (T1021.002) การบุกรุกส่วนใหญ่เกิดจากการที่กลุ่มนี้สามารถสร้างช่องทางการเข้าถึงได้หลายจุดในเครือข่าย โดยที่เครือข่ายมีโครงสร้างแบบแบนราบ (Flat network structure) และมีการใช้ซอฟต์แวร์ที่พัฒนาขึ้นเองภายในองค์กรซึ่งขาดความปลอดภัย จึงอาจนำไปใช้อัปโหลดไฟล์ได้โดยไม่มีข้อจำกัด ข้อมูลที่ถูกลักลอบนำออก (Exfiltrated data) รวมถึงข้อมูลประจำตัวของการยืนยันตัวตนแบบสิทธิพิเศษ ซึ่งช่วยให้กลุ่มผู้ปฏิบัติการสามารถใช้เข้าสู่ระบบได้ รวมทั้งข้อมูลเครือข่ายที่กลุ่มผู้ปฏิบัติการอาจนำไปใช้เพื่อเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาตได้อีก หากช่องทางเข้าถึงเดิมที่ใช้อยู่ถูกปิดกั้นไป แม้ว่าจะไม่พบการใช้เครื่องมืออันตรายเพิ่มเติมนอกเหนือจากที่อยู่บนเครื่องที่ถูกบุกรุกในขั้นต้น แต่การที่กลุ่มปฏิบัติการหนึ่งสามารถเข้าถึงข้อมูลประจำตัวที่ถูกต้องจริงและมีสิทธิพิเศษก็เพียงพอแล้วที่จะไม่ต้องใช้เครื่องมือเพิ่มเติม ผลการสืบสวนบ่งชี้ว่าองค์กรนี้น่าจะตกเป็นเป้าหมายของกลุ่ม APT40 โดยเจตนามากกว่าที่จะตกเป็นผู้เสียหายด้วยการฉวยโอกาสจากช่องโหว่ที่เปิดเผยต่อสาธารณะ

ผลการสืบสวน

ในช่วงกลางเดือนสิงหาคม ปี 2022 ทาง ACSC ของ ASD ได้แจ้งเตือนองค์กรว่ามีที่อยู่ IP ที่ยืนยันแล้วว่าเป็นอันตราย ซึ่งเชื่อว่าเกี่ยวข้องกับกลุ่มไซเบอร์ที่ได้รับการสนับสนุนจากรัฐบาล ได้เข้ามามีส่วนร่วมโต้ตอบกับเครือข่ายคอมพิวเตอร์ขององค์กรอย่างน้อยในระหว่างเดือนกรกฎาคมถึงสิงหาคม อุปกรณ์ที่ถูกบุกรุกน่าจะเป็นของธุรกิจขนาดเล็กหรือผู้ใช้งานตามบ้าน

ในช่วงปลายเดือนสิงหาคม ทาง ACSC ของ ASD ได้นำเอเจนต์ตรวจสอบที่ติดกับโฮสต์ (host-based agent) ไปลงในอุปกรณ์โฮสต์บนเครือข่ายขององค์กรที่มีหลักฐานว่าได้รับผลกระทบจากการถูกบุกรุก

หลักฐานบางอย่างที่อาจเป็นประโยชน์ต่อความพยายามในการสืบสวนยังไม่สามารถเข้าถึงได้ เนื่องจากการตั้งค่าระบบบันทึกหรือล็อกข้อมูล (Logging) หรือการออกแบบเครือข่าย แม้ว่าจะขาดหลักฐาน ความพร้อมขององค์กรในการให้ข้อมูลทั้งหมดที่มีอยู่ ช่วยให้ทีมตอบสนองเหตุการณ์ภายใต้ ACSC ของ ASD สามารถดำเนินการวิเคราะห์อย่างครอบคลุม และสร้างความเข้าใจเกี่ยวกับกิจกรรมของกลุ่ม APT40 ที่อาจเกิดขึ้นบนเครือข่ายได้

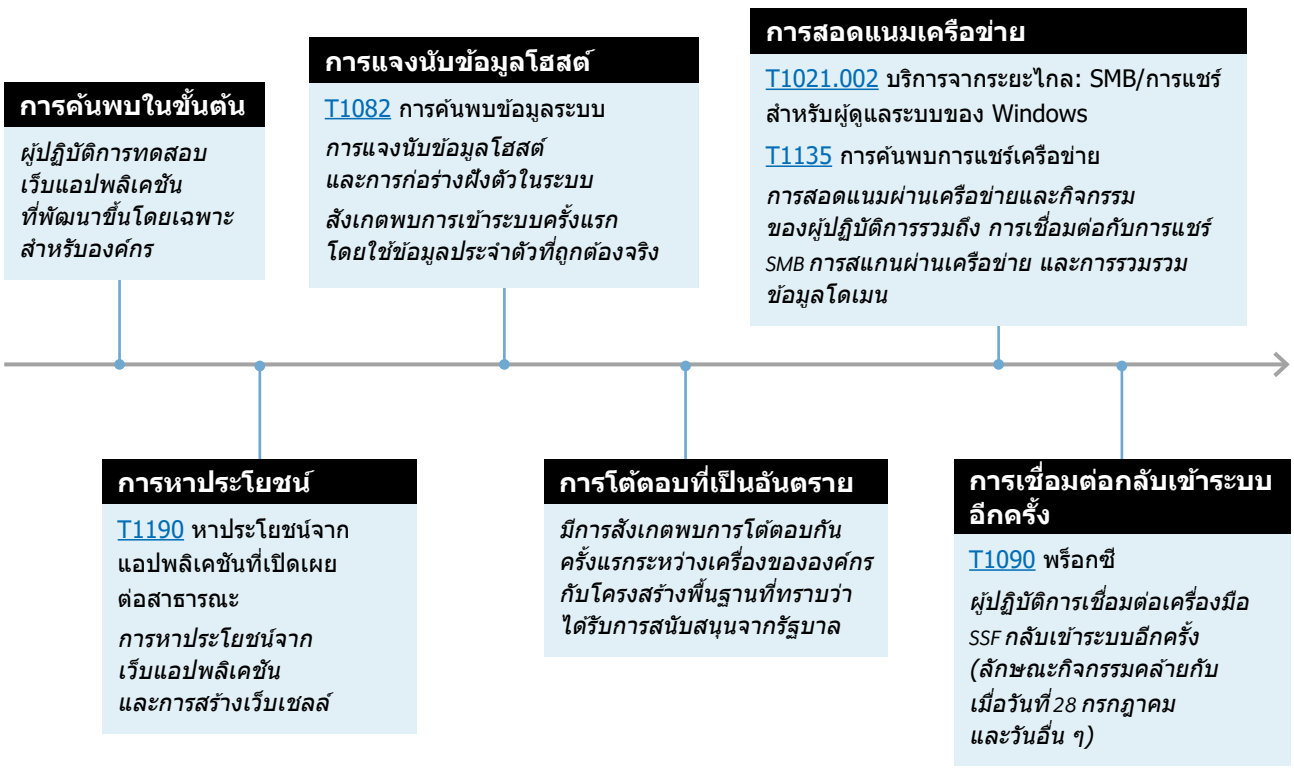
ในเดือนกันยายน หลังจากปรึกษากับ ACSC ของ ASD แล้ว องค์กรได้ตัดสินใจขึ้นบัญชีปฏิเสธ (Denylist) ที่อยู่ IP ที่ระบุไว้ในการแจ้งเตือนขั้นต้น ในเดือนตุลาคม องค์กรได้เริ่มดำเนินการแก้ไขปัญหา

รายละเอียด

ตั้งแต่เดือนกรกฎาคมเป็นต้นมา กลุ่มผู้ปฏิบัติการสามารถทดสอบและหาประโยชน์จากเว็บแอปพลิเคชันที่พัฒนาขึ้นเป็นเฉพาะ (T1190) ซึ่งทำงานอยู่บน `<webapp>2-ext` ที่ทำให้กลุ่มผู้ปฏิบัติการสามารถมีที่มั่นในเขตปลอดภัย (Demilitarised zone - DMZ) ของเครือข่ายได้ โดยกลุ่มผู้ปฏิบัติการใช้ประโยชน์ที่มั่นนี้ในการรวบรวมข้อมูลทั้งจากในเครือข่ายและโดเมนที่มองเห็นได้ทั้งหมด ข้อมูลประจำตัวที่ถูกบุกรุก (T1078.002) ถูกนำไปใช้เพื่อขอข้อมูลจาก Active Directory (T1018) และลักลอบนำข้อมูลออกโดยการเชื่อมต่อกับการแชร์ไฟล์ (T1039) จากหลายเครื่องภายในเขต DMZ ผู้ปฏิบัติการยังได้ดำเนินการโจมตีแบบ Kerberoasting เพื่อดึงข้อมูลประจำตัวเครือข่ายที่ถูกต้องจากเซิร์ฟเวอร์ (T1558.003) อย่างไรก็ตาม ไม่พบว่ากลุ่มผู้ปฏิบัติการสามารถขยายการเข้าถึงเพิ่มเติมไปยังจุดอื่น ๆ ภายในเขต DMZ หรือเครือข่ายภายใน

ภาพลำดับเหตุการณ์

ลำดับเหตุการณ์ข้างล่างนี้ แสดงภาพรวมโดยคร่าว ๆ ของช่วงเหตุการณ์สำคัญ ๆ ของผู้ไม่ประสงค์ดีที่สังเกตพบในเครือข่ายขององค์กร



ลำดับเหตุการณ์โดยละเอียด

กรกฎาคม กลุ่มผู้ปฏิบัติการได้เชื่อมต่อในขั้นต้นกับหน้าแรกของเว็บแอปพลิเคชันที่พัฒนาขึ้นโดยเฉพาะ (T1190) สำหรับองค์กร (ต่อไปนี้เรียกกวา 'เว็บแอปพลิเคชัน' or '*webapp*') ผ่านการเชื่อมต่อแบบ Transport layer security (TLS)(T1102). ไม่สังเกตพบกิจกรรมที่สำคัญอย่างอื่นเพิ่มเติม

กรกฎาคม กลุ่มผู้ปฏิบัติการเริ่มรวบรวมข้อมูลจากเว็บไซต์ของเว็บแอปพลิเคชันเพื่อค้นหาจุดสิ้นสุด (Endpoints) [2] สำหรับการสืบสวนเพิ่มเติม

กรกฎาคม กลุ่มผู้ปฏิบัติการมุ่งเป้าไปที่ความพยายามในการหาประโยชน์จากจุดสิ้นสุดเฉพาะจุด

กรกฎาคม กลุ่มผู้ปฏิบัติการสามารถส่งคำสั่งแบบ POST ไปยังเว็บเซิร์ฟเวอร์ได้สำเร็จ โดยน่าจะผ่านเว็บเชลล์ที่ฝังไว้ในหน้าอื่น ที่อยู่ IP ตัวที่สอง ซึ่งน่าจะใช้โดยกลุ่มผู้ปฏิบัติการกลุ่มเดียวกัน ก็เริ่มส่งคำสั่งแบบ POST ไปยัง URL เดียวกันด้วย กลุ่มผู้ปฏิบัติการสร้างและทดสอบเว็บเชลล์หลายรายการที่เป็นไปได้

ไม่ทราบวิธีการหาประโยชน์ที่แน่ชัด แต่มีความชัดเจนว่าจุดสิ้นสุดเฉพาะจุดนั้นถูกกำหนดเป้าหมายเพื่อสร้างไฟล์บน `<webapp>2-ext`

ACSC ของ ASD เชื่อว่าการเชื่อมต่อด้วยที่อยู่ IP สองรายการนั้นเป็นส่วนหนึ่งของการบุกรุกเดียวกัน เนื่องจากมีความสนใจร่วมกันและการเชื่อมต่อในช่วงเริ่มต้นที่เกิดขึ้นห่างกันเพียงไม่กี่นาทีเท่านั้น

กรกฎาคม กลุ่มผู้ปฏิบัติการยังคงดำเนินการแจงนับข้อมูลโฮสต์ โดยมองหาโอกาสในการยกระดับสิทธิพิเศษ และติดตั้งเว็บเชลล์ตัวอื่นเพิ่มเติม กลุ่มผู้ปฏิบัติการเข้าสู่ระบบเว็บแอปพลิเคชันโดยใช้ข้อมูลประจำตัวที่ถูกบุกรุกสำหรับ `<firstname.surname>@<organisation domain>`

กิจกรรมของกลุ่มผู้ปฏิบัติการดูเหมือนจะไม่สามารถยกระดับสิทธิพิเศษบน `<webapp>2-ext` ได้สำเร็จ แทนที่จะยกระดับสิทธิพิเศษ กลุ่มผู้ปฏิบัติการได้เปลี่ยนไปดำเนินกิจกรรมที่เน้นเครือข่ายแทน

กรกฎาคม ผู้ปฏิบัติการทดสอบข้อมูลประจำตัวที่ถูกบุกรุกสำหรับบัญชีบริการ (Service account)[3] ซึ่งน่าจะพบในไฟล์ปฏิบัติการไบนารี (Binary) ที่สามารถเข้าถึงได้ภายในองค์กรโดยถูกฝังโค้ดไว้โดยตรง (Hardcoded)

กรกฎาคม กลุ่มผู้ปฏิบัติการได้ติดตั้งเครื่องมือโอเพนซอร์ส Secure Socket Funnelling ซึ่งถูกใช้ในการเชื่อมต่อออกไปยังโครงสร้างพื้นฐานที่เป็นอันตราย การเชื่อมต่อนี้ถูกใช้เป็นช่องทางในการส่งข้อมูลที่ไหลเวียนจากเครื่องโจมตีของผู้ปฏิบัติการเข้าสู่เครือข่ายภายในขององค์กร โดยชื่อของเครื่องเหล่านี้ปรากฏอยู่ในบันทึกเหตุการณ์ (Event logs) ขณะที่พวกเขาพยายามใช้ข้อมูลประจำตัวสำหรับบัญชีบริการ

สิงหาคม พบว่ากลุ่มผู้ปฏิบัติการดำเนินกิจกรรมในวงจำกัด รวมถึงไม่สามารถเชื่อมต่อโดยใช้บัญชีบริการได้สำเร็จ

สิงหาคม กลุ่มผู้ปฏิบัติการทำการรวบรวมข้อมูลเครือข่ายและระบบ Active Directory อย่างมีนัยสำคัญ บัญชีที่ถูกบุกรุกอีกบัญชีหนึ่งจะถูกนำมาใช้ในภายหลังเพื่อเชื่อมต่อการแชร์[4] บนเครื่อง Windows ภายในเขต DMZ ซึ่งจะสามารถลักลอบนำข้อมูลออกจากระบบได้สำเร็จ

ดูเหมือนว่าจะเป็นการใช้ข้อมูลประจำตัวที่ขโมยโดยฉวยโอกาสบนเครื่องที่สามารถเชื่อมต่อการแชร์ได้ภายในเขต DMZ ไฟร์วอลล์ปิดกั้นไม่ให้ผู้ปฏิบัติการดำเนินกิจกรรมลักษณะเดียวกันในการโจมตีเครือข่ายภายใน

สิงหาคม - กันยายน เครื่องมือ SSF สร้างการเชื่อมต่อกลับไปยังที่อยู่ IP ที่เป็นอันตรายอีกครั้ง ไม่สังเกตเห็นว่ากลุ่มผู้ปฏิบัติการดำเนินกิจกรรมเพิ่มเติมใด ๆ จนกระทั่งการเข้าถึงของพวกเขาจะถูกปิดกั้น

กันยายน องค์กรปิดกั้นที่อยู่ IP ที่เป็นอันตรายโดยการขึ้นบัญชีปฏิเสธบนไฟร์วอลล์ขององค์กร

2 ในบริบทนี้ จุดสิ้นสุด (Endpoint) หมายถึงฟังก์ชันหนึ่งของเว็บแอปพลิเคชัน

3 บัญชีบริการไม่ผูกติดกับผู้ใช้รายบุคคล แต่ผูกกับบริการต่าง ๆ แทน ในโดเมนองค์กรของ Microsoft จะมีบัญชีผู้ใช้ประเภทต่าง ๆ หลายประเภทด้วยกัน

4 การเชื่อมต่อกับการแชร์ (Mounting shares) คือกระบวนการที่ทำให้ไฟล์ในโครงสร้างระบบไฟล์สามารถเข้าถึงได้โดยผู้ใช้หรือกลุ่มผู้ใช้

กลยุทธ์และเทคนิคของผู้ปฏิบัติการ

กรอบงาน MITRE ATT&CK เป็นเอกสารที่บันทึกการรวบรวมกลยุทธ์และเทคนิคที่ผู้ปฏิบัติการที่เป็นภัยคุกคามใช้ในโลกไซเบอร์ กรอบงานนี้สร้างขึ้นโดย MITRE Corporation ซึ่งเป็นองค์กรไม่แสวงหาผลกำไรของสหรัฐอเมริกา และทำหน้าที่เป็นภาษากลางระดับสากลที่ใช้สื่อสารเกี่ยวกับพฤติกรรมของผู้ปฏิบัติการที่เป็นภัยคุกคาม

ACSC ของ ASD ประเมินว่าเทคนิคและกลยุทธ์ต่อไปนี้มีความเกี่ยวข้องกับกิจกรรมที่เป็นอันตรายของผู้ปฏิบัติการรายนี้

การสอดแนม

T1594 – ค้นหาเว็บไซต์ที่ผู้เสียหายเป็นเจ้าของ

ผู้ปฏิบัติการรวบรวมข้อมูลจากเว็บไซต์ของเว็บแอปพลิเคชันที่พัฒนาขึ้นโดยเฉพาะเพื่อหาโอกาสในการเข้าถึงเครือข่าย

การเข้าถึงในขั้นต้น

T1190 – หาประโยชน์จากแอปพลิเคชันที่เปิดเผยต่อสาธารณะ (เกี่ยวกับการใช้ประโยชน์จากเว็บแอปพลิเคชันที่พัฒนาขึ้นโดยเฉพาะ)

T1078.002 – บัญชีที่ถูกต้อง: บัญชีโดเมน (เกี่ยวกับการเข้าสู่ระบบด้วยข้อมูลประจำตัวที่ถูกบุกรุก)

การหาประโยชน์จากเว็บแอปพลิเคชันที่พัฒนาขึ้นโดยเฉพาะ ซึ่งเปิดเผยบนอินเทอร์เน็ตเป็นจุดเริ่มต้นในการเข้าถึงระบบของผู้ปฏิบัติการ ต่อมา ผู้ปฏิบัติการสามารถใช้ข้อมูลประจำตัวที่พวกเขาบุกรุกได้แล้วเพื่อขยายการเข้าถึงเครือข่ายมากยิ่งขึ้น

การดำเนินการ

T1059 – ตัวแปลคำสั่งและสคริปต์ (เกี่ยวกับการดำเนินการสั่งการผ่านเว็บเชลล์)

T1072 – เครื่องมือสำหรับการติดตั้งซอฟต์แวร์ (เกี่ยวกับผู้ปฏิบัติการที่ใช้เครื่องมือโอเพนซอร์ส Secure Socket Funnelling (SSF) เพื่อเชื่อมต่อกับที่อยู่ IP)

การฝังตัวในระบบ

T1505.003 – ส่วนประกอบซอฟแวร์ของเซิร์ฟเวอร์: เว็บเชลล์ (เกี่ยวกับการใช้เว็บเชลล์และ SSF เพื่อสร้างการเข้าถึง)

การเข้าถึงข้อมูลประจำตัว

T1552.001 – ข้อมูลประจำตัวจากคลังจัดเก็บรหัสผ่าน (เกี่ยวกับไฟล์รหัสผ่านที่เกี่ยวข้องกับระบบจัดการอาคาร หรือ Building management system - BMS)

T1558.003 – ขโมยหรือปลอมตั๋ว Kerberos: Kerberoasting (เกี่ยวกับการโจมตีเพื่อให้ได้ข้อมูลประจำตัวของเครือข่าย)

การแทรกซึมต่อภายในเครือข่าย

T1021.002 – บริการจากระยะไกล: การแชร์ผ่าน SMB (เกี่ยวกับกรณีที่ผู้ปฏิบัติการเชื่อมต่อกับการแชร์ SMB จากอุปกรณ์หลายเครื่อง)

การรวบรวมข้อมูล

T1213 – ข้อมูลจากแหล่งเก็บข้อมูล (เกี่ยวกับคู่มือ/เอกสารที่พบบนเซิร์ฟเวอร์ BMS)

การลักลอบนำข้อมูลออก

T1041 – การลักลอบนำข้อมูลออกผ่านช่องทาง C2 (เกี่ยวกับการลักลอบนำข้อมูลออกของผู้ปฏิบัติการจาก Active Directory และการเชื่อมต่อกับการแชร์)

กรณีศึกษาที่ 2

รายงานฉบับนี้ได้รับการปกปิดข้อมูลที่ระบุตัวตนไว้ เพื่อให้สามารถเผยแพร่อย่างกว้างขวางได้ ต่อไปนี้จะเรียกองค์กรที่ได้รับผลกระทบว่า 'องค์กร' รายละเอียดบางส่วนได้ถูกลบออกเพื่อปกป้องตัวตนของผู้เสียหายและวิธีการรับมือเหตุการณ์ภายใต้ ACSC ของ ASD

บทสรุปสำหรับผู้บริหาร

รายงานฉบับนี้ให้รายละเอียดการสืบสวนภายใต้ ACSC ของ ASD เกี่ยวกับเหตุการณ์ที่เครือข่ายขององค์กรแห่งหนึ่งถูกบุกรุกระบบจนสำเร็จ ระหว่างเดือนเมษายน ปี 2022 รายงานการสืบสวนฉบับนี้จัดทำขึ้นเพื่อมอบให้กับองค์กรดังกล่าว โดยสรุปกิจกรรมที่เป็นอันตรายซึ่งสังเกตพบ และให้กรอบคำแนะนำการแก้ไขปัญหา ผลการตรวจสอบบ่งชี้ว่าการบุกรุกระบบครั้งนี้ดำเนินการโดยกลุ่ม APT40

ในเดือนพฤษภาคม ปี 2022 ทาง ACSC ของ ASD ได้แจ้งเตือนองค์กรแห่งหนึ่งเกี่ยวกับกิจกรรมที่ต้องสงสัยว่าเป็นอันตราย ซึ่งส่งผลกระทบต่อเครือข่ายขององค์กรตั้งแต่เดือนเมษายน ปี 2022 ต่อมาองค์กรดังกล่าวได้แจ้งให้ ACSC ของ ASD ทราบว่าได้ค้นพบซอฟต์แวร์ที่เป็นอันตรายบนเซิร์ฟเวอร์ที่เชื่อมต่อกับอินเทอร์เน็ต ซึ่งให้บริการพอร์ทัลเข้าสู่ระบบสำหรับโซลูชันการเข้าถึงระบบจากระยะไกลขององค์กร เซิร์ฟเวอร์นี้ใช้ผลิตภัณฑ์การจัดการการเข้าสู่ระบบและยืนยันข้อมูลประจำตัวจากระยะไกล และรายงานฉบับนี้จะเรียกว่า "อุปกรณ์ที่ถูกบุกรุก" รายงานฉบับนี้ให้รายละเอียดผลการสืบสวนและคำแนะนำในการแก้ไขปัญหาที่พัฒนาขึ้นสำหรับองค์กร เพื่อตอบสนองต่อการสืบสวนที่ดำเนินการโดย ACSC ของ ASD

หลักฐานบ่งชี้ว่าเครือข่ายบางส่วนขององค์กรได้ถูกบุกรุกโดย (กลุ่ม) ผู้ไม่ประสงค์ดีทางไซเบอร์ ผ่านทางพอร์ทัลเข้าสู่ระบบจากระยะไกลขององค์กร ตั้งแต่ช่วงอย่างน้อยเดือนเมษายน ปี 2022 เซิร์ฟเวอร์เครื่องนี้อาจถูกบุกรุกโดยผู้ปฏิบัติการหลายกลุ่ม และมีแนวโน้มว่าจะได้รับผลกระทบจากช่องโหว่การดำเนินการหรือรันโค้ดจากระยะไกล (Remote Code Execution - RCE) ซึ่งมีการเผยแพร่อย่างกว้างขวางในช่วงเวลาใกล้เคียงกับเหตุการณ์ดังกล่าว

กิจกรรมหลักของผู้ปฏิบัติการที่ ACSC ของ ASD สังเกตพบได้แก่

- การแจงนับข้อมูลโฮสต์ (Host enumeration) ซึ่งช่วยให้ผู้ปฏิบัติการสามารถสร้างแผนที่เครือข่ายของตนเองได้
- การหาประโยชน์จากแอปพลิเคชันที่เชื่อมต่อกับอินเทอร์เน็ต และการใช้เว็บเชลล์ ซึ่งช่วยให้ผู้ปฏิบัติการมีที่มั่นเข้าถึงเครือข่ายในขั้นต้น และสามารถดำเนินการสั่งการได้
- การใช้ประโยชน์จากช่องโหว่ของซอฟต์แวร์เพื่อยกระดับสิทธิพิเศษการเข้าถึง และ
- การรวบรวมข้อมูลประจำตัวเพื่อใช้ในการแทรกซึมต่อภายในเครือข่าย

ACSC ของ ASD พบว่ามีผู้ไม่ประสงค์ดีได้ลักลอบนำชื่อผู้ใช้และรหัสผ่านที่ไม่ซ้ำกันจำนวนหลายร้อยคู่ออกจากอุปกรณ์ที่ถูกบุกรุกในเดือนเมษายน ปี 2022 รวมถึงรหัสยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) จำนวนหนึ่ง และหลักฐานทางเทคนิคที่เกี่ยวข้องกับการเชื่อมต่อจากระยะไกล เมื่อองค์กรได้ตรวจสอบแล้ว พบว่ารหัสผ่านดังกล่าวเป็นของถูกต้องจริง ACSC ของ ASD ประเมินว่าผู้ปฏิบัติการอาจรวบรวมหลักฐานทางเทคนิคเหล่านี้ไว้เพื่อแย่งชิงหรือสร้างเซสชันการเข้าสู่ระบบจากระยะไกลในฐานะของผู้ใช้ที่ถูกต้องจริง และเข้าถึงเครือข่ายภายในขององค์กรโดยใช้บัญชีผู้ใช้ที่ถูกต้องจริง

ผลการสืบสวน

สรุปผลการสืบสวน

ACSC ของ ASD ระบุว่า ผู้ปฏิบัติการได้บุกรุกเข้าระบบอุปกรณ์หนึ่งหรือหลายเครื่องที่ใช้สำหรับให้บริการเซสชันเข้าสู่ระบบจากระยะไกลสำหรับพนักงานขององค์กร และได้ใช้ช่องทางที่บุกรุกได้นี้พยายามดำเนินกิจกรรมอื่นอีกเพิ่มเติม อุปกรณ์เหล่านี้ประกอบด้วยโฮสต์สามเครื่องที่ทำงานแบบโหลดบาลานซ์ โดยตรวจพบหลักฐานการถูกบุกรุกเป็นครั้งแรกในโฮสต์เหล่านี้ องค์กรได้ปิดระบบโฮสต์สองเครื่องจากสามเครื่องที่ทำงานแบบโหลดบาลานซ์ไม่นานหลังจากเกิดการบุกรุกในครั้งแรก ด้วยเหตุนี้ กิจกรรมทั้งหมดที่เกิดขึ้นหลังจากนั้นจึงเกิดขึ้นบนโฮสต์เพียงเครื่องเดียว ส่วนเซิร์ฟเวอร์อื่น ๆ ที่เชื่อมโยงกับอุปกรณ์ที่ถูกบุกรุกก็ทำงานแบบโหลดบาลานซ์ในลักษณะเดียวกันด้วย เพื่อความชัดเจนในการอ่านรายงานนี้ อุปกรณ์ทั้งหมดที่ถูกบุกรุกส่วนใหญ่จะอ้างถึงในรายงานนี้ว่าเป็น ‘อุปกรณ์เครื่องเดียว’

เชื่อว่าผู้ปฏิบัติการได้ใช้ช่องโหว่ที่เปิดเผยต่อสาธารณะในการติดตั้งเว็บเชลล์ลงในอุปกรณ์ที่ถูกบุกรุกตั้งแต่เดือนเมษายน ปี 2022 เป็นต้นมา ประเมินว่าผู้ปฏิบัติการที่เป็นภัยคุกคามจากกลุ่มดังกล่าวสามารถยกระดับสิทธิพิเศษการเข้าถึงบนอุปกรณ์ที่ถูกบุกรุกได้สำเร็จ ACSC ของ ASD ไม่สามารถระบุขอบเขตของกิจกรรมได้ทั้งหมดเนื่องจากขาดล็อกข้อมูล (log) ที่บันทึกเหตุการณ์ อย่างไรก็ตาม หลักฐานบนอุปกรณ์ชี้ให้เห็นว่าผู้ปฏิบัติการได้ดำเนินการดังต่อไปนี้

- การรวบรวมชื่อผู้ใช้และรหัสผ่านที่เป็นของจริงหลายร้อยคู่ และ
- การรวบรวมหลักฐานทางเทคนิคที่อาจช่วยให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงเซสชันโครงสร้างพื้นฐานเดสก์ท็อปเสมือน (Virtual desktop infrastructure - VDI) ในฐานะผู้ใช้ที่ถูกต้องจริงได้

ACSC ของ ASD ประเมินว่าผู้ปฏิบัติการน่าจะพยายามขยายผลการบุกรุกเครือข่ายขององค์กรต่อไป หลักฐานทางเทคนิคที่ถูกลักลอบนำออกไปโดยผู้ปฏิบัติการ อาจช่วยให้พวกเขาสามารถแย่งชิงหรือเริ่มต้นเซสชันเดสก์ท็อปเสมือนในฐานะผู้ใช้ที่ถูกต้องจริงได้ ซึ่งอาจเป็นผู้ใช้ที่พวกเขาเลือกเอง รวมถึงเป็นผู้ดูแลระบบด้วย ผู้ปฏิบัติการอาจใช้ช่องทางการเข้าถึงนี้ในการบุกรุกบริการขององค์กรเพิ่มเติม เพื่อให้สามารถฝังตัวในระบบและบรรลุเป้าหมายอื่น ๆ ได้

ส่วนอุปกรณ์อื่น ๆ ขององค์กรภายในสภาพแวดล้อมที่บริหารจัดการโดยผู้ให้บริการโฮสติ้ง ไม่พบหลักฐานการถูกบุกรุก

การเข้าถึง

โฮสต์ที่มีอุปกรณ์ถูกบุกรุกให้บริการการยืนยันตัวตนผ่าน Active Directory และเว็บเซิร์ฟเวอร์สำหรับผู้ใช้ที่เชื่อมต่อกับเซสชัน VDI (T1021.001)

ตำแหน่ง	ชื่อโฮสต์ของอุปกรณ์ที่ถูกบุกรุก (โหลดบาลานซ์)
Datacentre 1	HOST1, HOST2, HOST3

โครงสร้างพื้นฐานของอุปกรณ์ยังรวมถึงโฮสต์เกตเวย์สำหรับการเข้าถึงที่ให้บริการช่องทางการเชื่อมต่อไปยัง VDI สำหรับผู้ใช้ เมื่อผู้ใช้มีโทเคนการยืนยันตัวตนที่สร้างขึ้นและดาวน์โหลดมาจากอุปกรณ์นั้นแล้ว

ไม่พบหลักฐานการถูกบุกรุกของโฮสต์เหล่านี้แต่อย่างใด อย่างไรก็ตาม ล็อกข้อมูลของโฮสต์เกตเวย์สำหรับการเข้าถึงแสดงหลักฐานการโต้ตอบที่สำคัญกับที่อยู่ IP ที่ทราบว่าเป็นอันตราย มีแนวโน้มว่ากิจกรรมนี้สะท้อนถึงสิ่งที่เกิดขึ้นบนโฮสต์นี้ หรือเป็นการเชื่อมต่อเครือข่ายกับโครงสร้างพื้นฐานของผู้ปฏิบัติการที่เป็นภัยคุกคามที่เข้ามาถึงโฮสต์นี้ ลักษณะของกิจกรรมนี้ไม่สามารถระบุได้จากหลักฐานที่มีอยู่ แต่บ่งชี้ให้เห็นว่ากลุ่มดังกล่าวพยายามแทรกซึมต่อภายในเครือข่ายขององค์กร (TA0008)

โฮสต์ภายในระบบเครือข่าย

ACSC ของ ASD ได้ทำการสืบสวนตามข้อมูลที่มีอยู่จำกัดจากส่วนเครือข่ายภายในขององค์กร กิจกรรมที่เป็นอันตรายที่พยายามดำเนินการหรือดำเนินการสำเร็จซึ่งทราบว่ามีผลกระทบต่อส่วนเครือข่ายภายในขององค์กร ได้แก่ การที่ผู้ปฏิบัติการเข้าถึงหลักฐานทางเทคนิคที่เกี่ยวข้องกับ VDI การดึงข้อมูลจากเซิร์ฟเวอร์ SQL ภายใน (T1505.001) และการสังเกตพบปริมาณการรับส่งข้อมูลที่ไม่สามารถอธิบายได้จากที่อยู่ IP ที่ทราบว่าเป็นอันตรายผ่านอุปกรณ์เกตเวย์สำหรับการเข้าถึง (TA0011)

โดยใช้การเข้าถึงอุปกรณ์ที่ถูกบุกรุก กลุ่มดังกล่าวได้รวบรวมชื่อผู้ใช้จริง รหัสผ่าน (T1003) และค่ารหัสโทเคนยืนยันตัวตนแบบหลายปัจจัย (MFA token) (T1111) กลุ่มดังกล่าวยังได้รวบรวมโทเคนเว็บ JSON (JSON Web Tokens - JWTs) (T1528) ซึ่งเป็นหลักฐานทางเทคนิคสำหรับการยืนยันตัวตนที่ใช้สร้างเซสชันการเข้าสู่ระบบเดสก์ท็อปเสมือน ผู้ปฏิบัติการอาจสามารถใช้ข้อมูลเหล่านี้ในการสร้างหรือแย่งชิงเซสชันเดสก์ท็อปเสมือนได้ (T1563.002) และเข้าถึงส่วนเครือข่ายภายในขององค์กรในฐานะผู้ใช้ที่ถูกต้องจริง (T1078)

ผู้ปฏิบัติการยังใช้การเข้าถึงอุปกรณ์ที่ถูกบุกรุกเพื่อดึงข้อมูลจากเซิร์ฟเวอร์ SQL (T1505.001) ซึ่งตั้งอยู่ในเครือข่ายภายในขององค์กร เป็นไปได้ว่าผู้ปฏิบัติการสามารถเข้าถึงข้อมูลนี้ได้

หลักฐานที่มีจากอุปกรณ์เกตเวย์สำหรับการเข้าถึงเผยให้เห็นว่ามีปริมาณการรับส่งข้อมูลในเครือข่ายผ่านหรือไปยังอุปกรณ์นี้จากที่อยู่ IP ที่ทราบว่าเป็นอันตรายตามที่อธิบายไว้ข้างต้น สิ่งนี้อาจบ่งชี้ว่าผู้ไม่ประสงค์ดีทางไซเบอร์ได้ส่งผลกระทบหรือใช้ประโยชน์จากอุปกรณ์นี้โดยมีแนวโน้มที่จะเคลื่อนที่เข้าสู่เครือข่ายภายใน

ลำดับเหตุการณ์การสืบสวน

รายการด้านล่างนี้แสดงลำดับเหตุการณ์ของกิจกรรมสำคัญที่ค้นพบในระหว่างการสืบสวน

เวลา	เหตุการณ์
เมษายน ปี 2022	ที่อยู่ IP ที่ทราบว่าเป็นอันตรายมีการโต้ตอบกับโฮสต์เกตเวย์สำหรับการเข้าถึงชื่อ HOST7 ไม่สามารถระบุลักษณะของการโต้ตอบได้
เมษายน ปี 2022	โฮสต์ทั้งหมด ได้แก่ HOST1, HOST2 และ HOST3 ถูกบุกรุกโดยผู้ไม่ประสงค์ดีรายหนึ่งหรือหลายราย และมีการวางเว็บเชลล์ไว้บนโฮสต์เหล่านั้น มีการสร้างหรือแก้ไขไฟล์บันทึกข้อมูลบน HOST2 ไฟล์นี้มีข้อมูลประจำตัว ซึ่งมีความเป็นไปได้ว่าถูกผู้ไม่ประสงค์ดียึดไป ไฟล์ /etc/security/opasswd และ /etc/shadow ถูกแก้ไขบน HOST1 และ HOST3 ซึ่งบ่งชี้ว่ามีการเปลี่ยนแปลงรหัสผ่านแล้ว หลักฐานที่มีอยู่บน HOST1 ชี้ให้เห็นว่ารหัสผ่านของผู้ใช้ 'sshuser' ถูกเปลี่ยนแปลงแล้ว
เมษายน ปี 2022	HOST2 ถูกปิดระบบการใช้งานโดยองค์กร เว็บเชลล์เพิ่มเติม (T1505.003) ถูกสร้างขึ้นบน HOST1 และ HOST3 HOST1 ประสบกับความพยายามโจมตีแบบ SSH brute force จาก HOST3 ไฟล์บันทึกข้อมูลถูกแก้ไข (T1070) บน HOST3 ไฟล์นี้มีข้อมูลประจำตัว (T1078) ซึ่งมีความเป็นไปได้ว่าถูกผู้ไม่ประสงค์ดียึดไป มีการยึดข้อมูล JWTs (T1528) ไปและบันทึกออกเป็นไฟล์บน HOST3 HOST3 ถูกปิดระบบการใช้งานโดยองค์กร กิจกรรมทั้งหมดหลังจากเวลานี้เกิดขึ้นบน HOST1
เมษายน ปี 2022	เว็บเชลล์เพิ่มเติมถูกสร้างขึ้นบน HOST1 (T1505.003) มีการยึดข้อมูล JWTs ไปและบันทึกออกเป็นไฟล์บน HOST1
เมษายน ปี 2022	เว็บเชลล์เพิ่มเติมถูกสร้างขึ้นบน HOST1 (T1505.003) ที่อยู่ IP ที่ทราบว่าเป็นอันตรายมีการโต้ตอบกับโฮสต์ (TA0011) ที่อยู่ IP ที่ทราบว่าเป็นอันตรายมีการโต้ตอบกับโฮสต์เกตเวย์สำหรับการเข้าถึงชื่อ HOST7
พฤษภาคม ปี 2022	ที่อยู่ IP ที่ทราบว่าเป็นอันตรายมีการโต้ตอบกับโฮสต์เกตเวย์สำหรับการเข้าถึงชื่อ HOST7 (TA0011) เหตุการณ์การยืนยันตัวตนของผู้ใช้มีความเชื่อมโยงกับที่อยู่ IP ที่ทราบว่าเป็นอันตรายในล็อกข้อมูลบน HOST1 เว็บเชลล์เพิ่มเติมถูกสร้างขึ้นบนโฮสต์นี้ (T1505.003)
พฤษภาคม ปี 2022	สคริปต์บน HOST1 ถูกแก้ไขโดยผู้ปฏิบัติการ (T1543) สคริปต์นี้มีฟังก์ชันที่สามารถดึงข้อมูลจากเซิร์ฟเวอร์ SQL ภายในองค์กรได้
พฤษภาคม ปี 2022	ไฟล์บันทึกข้อมูลเพิ่มเติมบน HOST1 ถูกแก้ไขครั้งล่าสุด (T1070) ไฟล์นี้มีข้อมูลคู่ชื่อผู้ใช้และรหัสผ่านของเครือข่ายองค์กร ซึ่งเชื่อว่าเป็นข้อมูลที่ถูกต้องจริง (T1078)
พฤษภาคม ปี 2022	ไฟล์บันทึกข้อมูลเพิ่มเติมถูกแก้ไขครั้งล่าสุด (T1070) ไฟล์นี้มี JWTs ที่รวบรวมมาจาก HOST1
พฤษภาคม ปี 2022	เว็บเชลล์เพิ่มเติมถูกสร้างขึ้นบน HOST1 (T1505.003) ในวันที่นี้ องค์กรรายงานไปยัง ACSC ของ ASD ว่ามีการค้นพบเว็บเชลล์ที่มีวันที่สร้างในเดือนเมษายน 2022
พฤษภาคม ปี 2022	มีการสร้างสคริปต์จำนวนหนึ่งบน HOST1 รวมถึงไฟล์หนึ่งที่ชื่อว่า Log4jHotPatch.jar
พฤษภาคม ปี 2022	คำสั่ง iptables-save ถูกใช้เพื่อเพิ่มพอร์ตที่เปิดสองพอร์ตไปยังโฮสต์เกตเวย์สำหรับการเข้าถึง พอร์ตที่ถูกเพิ่มคือ 9998 และ 9999 (T1572)

กลยุทธ์และเทคนิคของผู้ปฏิบัติการ

ด้านล่างนี้เป็นการเน้นกลยุทธ์และเทคนิคหลายประการที่ระบุได้ระหว่างการสืบสวน

การเข้าถึงในขั้นต้น

T1190 แสวงหาประโยชน์จากแอปพลิเคชันที่เปิดเผยสู่สาธารณะ

กลุ่มดังกล่าวมีแนวโน้มที่จะหาประโยชน์จากการดำเนินการหรือรันโค้ดจากระยะไกล (RCE) การยกระดับสิทธิพิเศษ และการเลี่ยงการยืนยันตัวตน ในผลิตภัณฑ์การจัดการการเข้าสู่ระบบและยืนยันข้อมูลประจำตัวจากระยะไกลเพื่อเข้าสู่เครือข่ายในขั้นต้น

วิธีการเข้าถึงในขั้นต้นนี้ถือว่าเป็นไปได้มากที่สุดเนื่องจากเหตุผลดังต่อไปนี้

- เซิร์ฟเวอร์มีช่องโหว่ต่อ CVEs เหล่านี้ในเวลาขณะนั้น
- มีความพยายามที่จะหาประโยชน์จากช่องโหว่เหล่านี้จากโครงสร้างพื้นฐานของผู้ปฏิบัติการที่ทราบ และ
- กิจกรรมที่เป็นอันตรายภายในระบบที่ทราบเป็นครั้งแรก เกิดขึ้นไม่นานหลังจากที่มีความพยายามใช้ช่องโหว่เหล่านี้

การดำเนินการ

T1059.004 ตัวแปลคำสั่งและสคริปต์: ยูนิกซ์เชลล์ (Unix Shell)

กลุ่มดังกล่าวที่หาประโยชน์จากช่องโหว่ข้างต้นได้สำเร็จอาจสามารถรันคำสั่งในยูนิกซ์เชลล์ที่มีอยู่บนอุปกรณ์ที่ได้รับผลกระทบได้ ไม่สามารถให้รายละเอียดคำสั่งทั้งหมดที่ผู้ปฏิบัติการรันได้ เนื่องจากอุปกรณ์ไม่ได้บันทึกข้อมูลเหล่านั้นไว้

การฝังตัวในระบบ

T1505.003 ส่วนประกอบซอฟแวร์ของเซิร์ฟเวอร์: เว็บเชลล์

ผู้ปฏิบัติการได้ติดตั้งเว็บเชลล์หลายรายการบนอุปกรณ์ที่ได้รับผลกระทบ เป็นไปได้ว่ามีผู้ปฏิบัติการหลายกลุ่มที่ติดตั้งเว็บเชลล์บนอุปกรณ์ที่ได้รับผลกระทบ แต่มีเพียงจำนวนน้อยกว่าที่ดำเนินกิจกรรมโดยใช้เว็บเชลล์เหล่านั้น เว็บเชลล์จะเปิดโอกาสให้ผู้ปฏิบัติการสามารถดำเนินการหรือรันคำสั่งใดก็ได้บนอุปกรณ์ที่ถูกบุกรุก

การยกระดับสิทธิพิเศษ

T1068 หาประโยชน์จากการยกระดับสิทธิพิเศษ

หลักฐานที่มีอยู่ไม่สามารถอธิบายระดับสิทธิพิเศษที่ผู้ปฏิบัติการได้รับได้ อย่างไรก็ตาม โดยการใช้เว็บเชลล์ กลุ่มผู้ปฏิบัติการน่าจะได้รับระดับสิทธิพิเศษที่เทียบเท่ากับเซิร์ฟเวอร์เว็บบนอุปกรณ์ที่ถูกบุกรุก ช่องโหว่ที่เชื่อว่ามีอยู่บนอุปกรณ์ที่ถูกบุกรุกนั้น อาจเปิดโอกาสให้กลุ่มผู้ปฏิบัติการสามารถได้รับสิทธิพิเศษระดับรูทได้

การเข้าถึงข้อมูลประจำตัว

T1056.003 การยึดข้อมูลนำเข้า: การยึดเว็บพอร์ทัล

หลักฐานบนอุปกรณ์ที่ถูกบุกรุกแสดงให้เห็นว่าผู้ปฏิบัติการได้ยึดคู่ชื่อผู้ใช้และรหัสผ่านหลายร้อยคู่ไป ในรูปแบบข้อความที่ชัดเจน ซึ่งเชื่อว่าเป็นข้อมูลที่ถูกต้องจริง มีความเป็นไปได้ว่าข้อมูลเหล่านี้ถูกยึดไปโดยใช้การแก้ไขบางอย่างในกระบวนการยืนยันตัวตนที่แท้จริง ซึ่งส่งออกเป็นข้อมูลประจำตัวไปยังไฟล์

T1111 การดักจับข้อมูลการยืนยันตัวตนแบบหลายปัจจัย

ผู้ปฏิบัติการยังได้ยึดค่าของโทเคน MFA ที่สอดคล้องกับการเข้าสู่ระบบที่ถูกต้องจริงไป ข้อมูลเหล่านี้น่าจะถูกยึดไปโดยการดัดแปลงกระบวนการยืนยันตัวจริงที่แท้จริงเพื่อส่งออกค่าดังกล่าวไปยังไฟล์ ไม่พบหลักฐานการถูกบุกรุกของ ‘เซิร์ฟเวอร์ลับ’ (Secret server) ที่เก็บค่าที่ไม่ซ้ำกันซึ่งใช้ทำหน้าที่ในการรักษาความปลอดภัยของโทเคน MFA

T1040 การดักจับข้อมูลเครือข่าย

เชื่อว่าผู้ปฏิบัติการได้ยึด JWT ไปโดยการดักจับปริมาณการรับส่งข้อมูล HTTP บนอุปกรณ์ที่ถูกบุกรุก มีหลักฐานว่าโปรแกรมยูทิลิตี้ tcpdump ถูกใช้งานบนอุปกรณ์ที่ถูกบุกรุก ซึ่งอาจเป็นวิธีที่ผู้ปฏิบัติการใช้ในการยึด JWT เหล่านี้

T1539 ขโมยคุกกี้เซสชันของเว็บ

ตามที่ได้อธิบายไว้ข้างต้น ผู้ปฏิบัติการได้ยึด JWTs ซึ่งมีลักษณะคล้ายกับคุกกี้เซสชันของเว็บ ข้อมูลเหล่านี้อาจถูกนำกลับมาใช้ซ้ำโดยผู้ปฏิบัติการเพื่อสร้างการเข้าถึงเพิ่มเติม

การค้นพบ

T1046 การค้นพบบริการเครือข่าย

มีหลักฐานว่าเครื่องมือสแกนเครือข่าย nmap ถูกใช้งานบนอุปกรณ์ที่ถูกบุกรุกเพื่อสแกนอุปกรณ์อื่น ๆ ในส่วนเครือข่ายเดียวกัน ผู้ปฏิบัติการมีแนวโน้มที่จะใช้เครื่องมือนี้ในการค้นหาบริการเครือข่ายอื่น ๆ ที่สามารถเข้าถึงได้ ซึ่งอาจนำไปสู่โอกาสการแทรกซึมต่อภายในเครือข่าย

การรวบรวมข้อมูล

หลักฐานที่มีอยู่ไม่เปิดเผยว่าผู้ปฏิบัติการรวบรวมข้อมูลอย่างไร หรือมีข้อมูลที่รวบรวมจากอุปกรณ์ที่ถูกบุกรุกหรือจากระบบอื่น ๆ อย่างไร อย่างไรก็ตาม มีแนวโน้มว่าผู้ปฏิบัติการสามารถเข้าถึงไฟล์ทั้งหมดบนอุปกรณ์ที่ถูกบุกรุกได้ รวมถึงข้อมูลประจำตัว (T1003) ค่าของโทเคน MFA (T1111) และ JWTs ซึ่งยึดมาได้ดังที่อธิบายไว้ข้างต้นด้วย

ระบบสั่งการและควบคุม

T1071.001 โปรโตคอลชั้นแอปพลิเคชัน: โปรโตคอลเว็บ

ผู้ปฏิบัติการใช้เว็บเชลล์สำหรับระบบสั่งการและควบคุม คำสั่งเว็บเชลล์น่าจะถูกส่งผ่านทาง HTTPS โดยใช้เว็บเซิร์ฟเวอร์ที่มีอยู่บนอุปกรณ์ (T1572)

T1001.003 การปกปิดข้อมูล: การแอบอ้างโปรโตคอล

ผู้ปฏิบัติการใช้เครื่องมือที่ถูกบุกรุกเป็นจุดเริ่มต้นในการโจมตีที่ออกแบบมาเพื่อให้แฝงตัวเข้ากับปริมาณการรับส่งข้อมูลที่ถูกต้องจริง

คำแนะนำด้านการตรวจจับและบรรเทาปัญหา

ACSC ของ ASD ขอแนะนำอย่างยิ่งให้ดำเนินการตามมาตรการควบคุม Essential Eight ของ ASD อีกทั้ง กลยุทธ์ที่เกี่ยวข้องในการบรรเทาปัญหาเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (Strategies to Mitigate Cyber Security Incidents) ที่เกี่ยวข้อง ด้านล่างนี้เป็นคำแนะนำสำหรับการดำเนินการด้านความปลอดภัยเครือข่ายที่ควรนำไปใช้เพื่อการตรวจจับและป้องกันการบุกรุกโดยกลุ่ม APT40 ตามด้วยการบรรเทาปัญหาเฉพาะสำหรับกลยุทธ์ เทคนิค และขั้นตอนปฏิบัติ (TTP) ที่สำคัญ 4 รายการ ซึ่งสรุปไว้ในตารางที่ 1

การตรวจจับ

ไฟล์บางรายการที่ระบุไว้ข้างต้นถูกวางไว้ในตำแหน่งต่าง ๆ เช่น C:\Users\Public* และ C:\Windows\Temp* ตำแหน่งเหล่านี้อาจเป็นจุดที่สะดวกในการเขียนข้อมูล เนื่องจากโดยทั่วไปแล้ว ผู้ใช้ทั่วโลกจะสามารถเขียนได้ นั่นคือ บัญชีผู้ใช้ทั้งหมดที่ลงทะเบียนใน Windows จะสามารถเข้าถึงไดเรกทอรีเหล่านี้และไดเรกทอรีย่อยของตนได้ บ่อยครั้ง ผู้ใช้คนไหนก็สามารถเข้าถึงไฟล์เหล่านี้ได้ในภายหลัง ซึ่งเปิดโอกาสให้เกิดการแทรกซึมต่อภายในเครือข่าย การหลบเลี่ยงการตรวจจับ การดำเนินการด้วยสิทธิพิเศษต่ำ และการเตรียมการลักลอบนำข้อมูลออกจากระบบ

กฎของ Sigma ต่อไปนี้ใช้ตรวจจับการดำเนินการจากตำแหน่งที่น่าสงสัย ซึ่งถือเป็นสัญญาณของกิจกรรมที่ผิดปกติ ในทุกกรณี จำเป็นต้องมีการสืบสวนเพิ่มเติมเพื่อยืนยันกิจกรรมที่เป็นอันตรายและเพื่อระบุแหล่งที่มา

หัวข้อ: การดำเนินการที่ทั่วโลกสามารถเขียนได้ - Temp

รหัส (ID): d2fa2d71-fbd0-4778-9449-e13ca7d7505c

คำอธิบาย ตรวจจับการดำเนินกระบวนการจาก C:\Windows\Temp

ความเป็นมา

กฎนี้จะตรวจจับเฉพาะการดำเนินการจาก C:\Windows\Temp* โดยโฟลเดอร์ Temp มักถูกใช้งานโดยแอปพลิเคชันที่ไม่เป็นอันตรายมากกว่า และจึงเป็นตัวบ่งชี้ความเป็นอันตรายที่มีความน่าเชื่อถือต่ำกว่าการดำเนินการจากไดเรกทอรีย่อยอื่นที่ทั่วโลกสามารถเขียนได้ใน C:\Windows

การตัดแอปพลิเคชันที่ดำเนินการโดยผู้ใช้ SYSTEM หรือ NETWORK SERVICE ออก จะช่วยลดปริมาณกิจกรรมที่ไม่เป็นอันตรายที่กฎนี้เลือกได้เป็นอย่างมาก ซึ่งหมายความว่ากฎนี้อาจไม่สามารถตรวจจับการดำเนินการที่เป็นอันตรายในระดับสิทธิพิเศษสูงกว่าได้ อย่างไรก็ตาม ขอแนะนำให้ใช้กฎอื่นร่วมด้วยเพื่อระบุว่าผู้ใช้พยายามยกระดับสิทธิพิเศษไปเป็น SYSTEM หรือไม่

การสืบสวน

1. ตรวจสอบข้อมูลที่เกี่ยวข้องโดยตรงกับการดำเนินการไฟล์นี้ เช่น บริบทของผู้ใช้ ระดับความสมบูรณ์ของการดำเนินการ กิจกรรมที่ต่อเนื่องมาทันที และภาพที่ไฟล์โหลดขึ้น
2. สืบสวนกระบวนการตามบริบทที่เกี่ยวข้อง เครือข่าย ไฟล์ และข้อมูลสนับสนุนอื่น ๆ บนโฮสต์ เพื่อช่วยประเมินว่ากิจกรรมนั้นเป็นอันตรายหรือไม่
3. หากจำเป็น ให้พยายามรวบรวมสำเนาของไฟล์โดยนำไปวิเคราะห์ย้อนกลับ เพื่อพิจารณาว่าไฟล์นั้นถูกต้องจริงหรือไม่

เอกสารอ้างอิง

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ผู้แต่ง: ACSC ของ ASD

วันที่: 19 มิถุนายน 2024

สถานะ: ขั้นการทดลอง

แท็ก (Tag)

- tlp.green
- classification.au.official
- attack.execution

แหล่งล็อกข้อมูล

```
category: process_creation
product: windows
```

การตรวจจับ

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    User:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

condition: temp and not (common_temp_path or system_user or dismhost or known_parent)

ผลบวกปลอม

- มีการสังเกตพบว่าแอปพลิเคชันตรวจสอบรายชื่อที่อนุญาต (Allowlist auditing) กำลังดำเนินการรันไฟล์ปฏิบัติการจากโฟลเดอร์ชั่วคราว (Temp)
- โฟลเดอร์ชั่วคราว (Temp) จะมีแอปพลิเคชันติดตั้งและตัวเรียกใช้งานประเภทต่าง ๆ โดยมีความถูกต้องจริงอยู่เป็นจำนวนมาก ดังนั้น จึงควรพิจารณาว่าพฤติกรรมนี้เป็นเรื่องที่เกิดขึ้นบ่อยแค่ไหนในเครือข่ายที่มีการเฝ้าระวัง (และสามารถอยู่ในรายชื่อที่อนุญาตได้หรือไม่) ก่อนที่จะนำกฎนี้ไปใช้งาน

ระดับ: ต่ำ

หัวข้อ: การดำเนินการที่ทั่วโลกสามารถเขียนได้ - ไม่ใช่-ไดเรกทอรีย่อยของระบบ Temp

รหัส (ID): 5b187157-e892-4fc9-84fc-aa48aff9f997

คำอธิบาย ตรวจจับการดำเนินกระบวนการจากตำแหน่งที่ทั่วโลกสามารถเขียนได้ในไดเรกทอรีย่อยของตำแหน่งที่ติดตั้งระบบปฏิบัติการ Windows

ความเป็นมา

กฎนี้จะตรวจจับเฉพาะการดำเนินการจากไดเรกทอรีที่ทั่วโลกสามารถเขียนได้ภายในไดรฟ์ C:\ และโดยเฉพาะอย่างยิ่ง C:\Windows* ยกเว้น C:\Windows\Temp (ซึ่งมักถูกใช้งานโดยแอปพลิเคชันที่ไม่เป็นอันตรายมากกว่า และจึงเป็นตัวบ่งชี้ความเป็นอันตรายที่มีความน่าเชื่อถือต่ำกว่า)

โฟลเดอร์ AppData จะได้รับการยกเว้นหากรันไฟล์ด้วย SYSTEM เนื่องจากเป็นวิธีที่ไม่เป็นอันตรายของการเรียกใช้งานไฟล์แอปพลิเคชันชั่วคราวจำนวนมาก

หลังจากเสร็จสิ้นการสร้างข้อมูลพื้นฐานของเครือข่ายในขั้นต้นและระบุการดำเนินการที่ทราบว่าไม่เป็นอันตรายจากตำแหน่งเหล่านี้แล้ว กฎนี้ควรถูกเรียกใช้งานน้อยครั้งมาก

การสืบสวน

1. ตรวจสอบข้อมูลที่เกี่ยวข้องโดยตรงกับการดำเนินการไฟล์นี้ เช่น บริบทของผู้ใช้ ระดับความสมบูรณ์ของการดำเนินการ กิจกรรมที่ต่อเนื่องมาทันที และภาพที่ไฟล์โหลดขึ้น
2. สืบสวนกระบวนการตามบริบทที่เกี่ยวข้อง เครือข่าย ไฟล์ และข้อมูลสนับสนุนอื่น ๆ บนโฮสต์ เพื่อช่วยประเมินว่ากิจกรรมนั้นเป็นอันตรายหรือไม่
3. หากจำเป็น ให้พยายามรวบรวมสำเนาของไฟล์โดยนำไปวิเคราะห์ย้อนกลับ เพื่อพิจารณาว่าไฟล์นั้นถูกต้องจริงหรือไม่

เอกสารอ้างอิง

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ผู้แต่ง: ACSC ของ ASD

วันที่: 19 มิถุนายน 2024
สถานะ: ขั้นการทดลอง

แท็ก (Tag)

- tlp.green
- classification.au.official
- attack.execution

แหล่งล็อกข้อมูล

category: process_creation
product: windows

การตรวจจับ

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'

User: 'SYSTEM'

condition: writable_path and not appdata

ผลบวกปลอม

มีการสังเกตพบว่าแอปพลิเคชันตรวจสอบรายชื่อที่อนุญาต (Allowlist auditing) กำลังดำเนินการรันไฟล์ปฏิบัติการจากโฟลเดอร์เหล่านี้

เป็นไปได้ว่าสคริปต์และเครื่องมือสำหรับการจัดการระบบที่ใช้ในสภาพแวดล้อมที่เฝ้าระวัง อาจถูกจัดเก็บไว้ในไดเรกทอรีเหล่านี้บางแห่ง และควรพิจารณาเป็นกรณีไป

ระดับ: สูง

หัวข้อ: การดำเนินการที่ทั่วโลกสามารถเขียนได้ - ผู้ใช้

รหัส (ID): 6dda3843-182a-4214-9263-925a80b4c634

คำอธิบาย ตรวจจับการดำเนินกระบวนการจาก C:\Users\Public* และโฟลเดอร์อื่น ๆ ภายใต้ Users ที่ทั่วโลกสามารถเขียนได้

ความเป็นมา

โฟลเดอร์ AppData จะได้รับการยกเว้นหากรันไฟล์ด้วย SYSTEM เนื่องจากเป็นวิธีที่ไม่เป็นอันตรายของการเรียกใช้งานไฟล์แอปพลิเคชันชั่วคราวจำนวนมาก

การสืบสวน

1. ตรวจสอบข้อมูลที่เกี่ยวข้องโดยตรงกับการดำเนินการไฟล์นี้ เช่น บริบทของผู้ใช้ ระดับความสมบูรณ์ของการดำเนินการ กิจกรรมที่ต่อเนื่องมาทันที และภาพที่ไฟล์โหลดขึ้น
2. สืบสวนกระบวนการตามบริบทที่เกี่ยวข้อง เครือข่าย ไฟล์ และข้อมูลสนับสนุนอื่น ๆ บนโฮสต์ เพื่อช่วย
3. ประเมินว่ากิจกรรมนั้นเป็นอันตรายหรือไม่
4. หากจำเป็น ให้พยายามรวบรวมสำเนาของไฟล์โดยนำไปวิเคราะห์ย้อนกลับ เพื่อพิจารณาว่าไฟล์นั้นถูกต้องจริงหรือไม่

เอกสารอ้างอิง

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

ผู้แต่ง: ACSC ของ ASD

วันที่: 19 มิถุนายน 2024

สถานะ: ขั้นการทดลอง

แท็ก (Tag)

- tlp.green
- classification.au.official
- attack.execution

แหล่งล็อกข้อมูล

category: process_creation

product: windows

การตรวจจับ

```
users:
    Image|contains:
    - ':\\Users\\All Users\\'
    - ':\\Users\\Contacts\\'
    - ':\\Users\\Default\\'
    - ':\\Users\\Public\\'
    - ':\\Users\\Searches\\'
appdata:
    Image|contains: '\\AppData\\'
    User: 'SYSTEM'
condition: users and not appdata
```

ผลบวกปลอม

- เป็นไปได้ว่าสคริปต์และเครื่องมือสำหรับการจัดการระบบที่ใช้ในสภาพแวดล้อมที่เฝ้าระวังอาจถูกจัดเก็บไว้ในไดเรกทอรีสาธารณะหรือไดเรกทอรีย่อย และควรพิจารณาเป็นกรณีไป

ระดับ: กลาง

การบรรเทาปัญหา

การทำล็อกข้อมูล

ระหว่างการสืบสวนภายใต้ ACSC ของ ASD ปัญหาทั่วไปที่ทำให้ประสิทธิภาพและความรวดเร็วของการสืบสวนลดลง ก็คือการขาดล็อกข้อมูลที่มีรายละเอียดย้อนหลังและครอบคลุมในหลายด้าน เช่น ล็อกคำขอของเว็บเซิร์ฟเวอร์ ล็อกเหตุการณ์ของ Windows และล็อกพร็อกซีอินเทอร์เน็ต

ACSC ของ ASD แนะนำให้ทบทวนและนำแนวทางเกี่ยวกับการบันทึกและการส่งต่อเหตุการณ์ของ Windows รวมทั้งไฟล์การตั้งค่าและสคริปต์ที่อยู่ในคลังข้อมูลการบันทึกเหตุการณ์ของ Windows และแนวปฏิบัติสำหรับการเฝ้าระวังระบบตามคู่มือการรักษาความปลอดภัยข้อมูล (Information Security Manual) ออกใช้งานด้วย เพื่อให้ครอบคลุมถึงการรวมศูนย์และการเก็บรักษาล็อกข้อมูลในระยะเวลาที่เหมาะสม

การจัดการแพตช์

รีบอัปเดตแพตช์ให้อุปกรณ์และบริการที่เชื่อมต่อกับอินเทอร์เน็ตทั้งหมด รวมถึงเว็บเซิร์ฟเวอร์ เว็บแอปพลิเคชัน และเกตเวย์สำหรับการเข้าถึงจากระยะไกล พิจารณานำระบบการจัดการแพตช์แบบรวมศูนย์ออกใช้งาน เพื่อทำให้งานนี้เป็นไปโดยอัตโนมัติและเร่งกระบวนการให้รวดเร็วขึ้น ACSC ของ ASD แนะนำให้นำแนวปฏิบัติในการจัดการระบบของ ISM ออกใช้งาน โดยเฉพาะอย่างยิ่ง การควบคุมการติดตั้งแพตช์ระบบในกรณีที่เกี่ยวข้อง

การหาประโยชน์ส่วนใหญ่ที่ผู้ปฏิบัติการใช้เป็นช่องโหว่ที่เป็นที่รู้จักในสาธารณะและมีแพตช์หรือวิธีการบรรเทาปัญหาให้ใช้งานได้แล้ว องค์กรควรทำให้แน่ใจว่าได้ติดตั้งแพตช์ความปลอดภัยหรือใช้วิธีการบรรเทาปัญหากับโครงสร้างพื้นฐานที่เชื่อมต่อกับอินเทอร์เน็ตภายใน 48 ชั่วโมง และหากเป็นไปได้ ควรใช้ซอฟต์แวร์และระบบปฏิบัติการเวอร์ชันล่าสุดด้วย

การแบ่งส่วนเครือข่าย

การแบ่งส่วนเครือข่าย (Network segmentation) สามารถทำให้ผู้ไม่ประสงค์ดีเข้าถึงและได้รับข้อมูลสำคัญขององค์กรได้ยากขึ้นอย่างมีนัยสำคัญ แบ่งส่วนเครือข่ายเพื่อจำกัดหรือปิดกั้นการแทรกซึมต่อภายในเครือข่าย โดยการปฏิเสธการรับส่งข้อมูลระหว่างคอมพิวเตอร์ เว้นแต่จะมีความจำเป็น เซิร์ฟเวอร์ที่สำคัญ เช่น Active Directory และเซิร์ฟเวอร์สำหรับการยืนยันตัวตนอื่น ๆ ควรได้รับการจัดการจากเซิร์ฟเวอร์ตัวกลางที่มีจำนวนจำกัด หรือที่เรียกว่า 'Jump servers' เท่านั้น ควรมีการเฝ้าระวังเซิร์ฟเวอร์เหล่านี้อย่างใกล้ชิด มีการรักษาความปลอดภัยอย่างเข้มงวด และจำกัดเฉพาะผู้ใช้และอุปกรณ์ที่จะสามารถเชื่อมต่อกับเซิร์ฟเวอร์เหล่านี้ได้เท่านั้น

แม้จะมีกรณีที่พบว่าสามารถป้องกันการแทรกซึมต่อภายในเครือข่ายแล้วก็ตาม การแบ่งส่วนเครือข่ายเพิ่มเติมก็อาจช่วยจำกัดปริมาณข้อมูลที่กลุ่มผู้ปฏิบัติการสามารถเข้าถึงและดึงออกไปได้มากยิ่งขึ้น

วิธีบรรเทาปัญหาเพิ่มเติม

หน่วยงานผู้ร่วมจัดทำรายงานนี้ยังแนะนำวิธีการบรรเทาปัญหาต่อไปนี้เพื่อรับมือกับกลุ่ม APT40 และกลุ่มอื่น ๆ ที่ใช้กลยุทธ์ เทคนิค และขั้นตอนปฏิบัติ (TTP) ตามที่ระบุด้านล่างนี้

- ปิดการใช้งานบริการเครือข่าย พอร์ต และโปรโตคอลที่ไม่ได้ใช้งานหรือไม่จำเป็น
- ใช้ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน (Web application firewalls - WAF) ที่ปรับแต่งอย่างเหมาะสมเพื่อปกป้องเว็บเซิร์ฟเวอร์และแอปพลิเคชันต่าง ๆ
- บังคับใช้หลักการให้สิทธิพิเศษเท่าที่จำเป็น (Least privilege) เพื่อจำกัดการเข้าถึงเซิร์ฟเวอร์ การแชร์ไฟล์ และทรัพยากรอื่น ๆ
- ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) และบัญชีบริการที่มีการจัดการ (Managed Service Accounts) เพื่อทำให้เข้าถึงข้อมูลประจำตัวได้ยากขึ้นและไม่สามารถนำกลับมาใช้ใหม่ได้ง่าย ควรนำการยืนยันตัวตนแบบหลายปัจจัย (MFA) มาใช้กับบริการเข้าถึงจากระยะไกลที่สามารถเข้าถึงผ่านอินเทอร์เน็ตได้ทั้งหมด รวมถึง
  - อีเมลบนเว็บและระบบคลาวด์
  - แพลตฟอร์มการทำงานร่วมกัน
  - การเชื่อมต่อเครือข่ายส่วนตัวเสมือน (VPN)
  - บริการเดสก์ท็อปจากระยะไกล
- เปลี่ยนอุปกรณ์ที่หมดอายุการใช้งาน

ตารางที่ 1 กลยุทธ์/เทคนิคการบรรเทาปัญหา

กลยุทธ์ เทคนิค และขั้นตอนปฏิบัติ (TTP)	กลยุทธ์การบรรเทาปัญหา Essential Eight	การควบคุม ISM
การเข้าถึงในขั้นต้น T1190 การหาประโยชน์จากแอปพลิเคชันที่เปิดเผยต่อสาธารณะ	แอปพลิเคชันสำหรับติดตั้งแพตช์ ระบบปฏิบัติการแพตช์ การยืนยันตัวตนแบบหลายปัจจัย การควบคุมแอปพลิเคชัน	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
การดำเนินการ (Execution) T1059 ตัวแปลคำสั่งและสคริปต์	การควบคุมแอปพลิเคชัน จำกัดการใช้งานแมโครของ Microsoft Office จำกัดสิทธิพิเศษการดูแลระบบ	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
การฝังตัวในระบบ T1505.003 Server Software Component: เว็บเชลล์	การควบคุมแอปพลิเคชัน จำกัดสิทธิพิเศษการดูแลระบบ	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
การเข้าถึงในขั้นต้น / การยกระดับสิทธิพิเศษ / การฝังตัวในระบบ T1078 บัญชีที่ถูกต้อง	ระบบปฏิบัติการแพตช์ การยืนยันตัวตนแบบหลายปัจจัย จำกัดสิทธิพิเศษการดูแลระบบ การควบคุมแอปพลิเคชัน การเสริมความแข็งแกร่งให้กับแอปพลิเคชันของผู้ใช้	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

สำหรับคำแนะนำเพิ่มเติมเกี่ยวกับการตรวจจับและบรรเทาปัญหาทั่วไป กรุณาอ่านส่วน การตรวจจับและบรรเทาปัญหา (Mitigations and Detection) บนหน้าเว็บเทคนิค MITRE ATT&CK สำหรับแต่ละเทคนิคที่ระบุไว้ในบทสรุป MITRE ATT&CK ที่ท้ายเอกสารข้อแนะนำฉบับนี้

ข้อจำกัดความรับผิดชอบ

ข้อมูลในเอกสารนี้ได้รับการจัดหา “ตามสภาพที่เป็น” เพื่อวัตถุประสงค์ในการให้ข้อมูลเท่านั้น หน่วยงานผู้จัดทำไม่รับรองนิติบุคคลเชิงพาณิชย์ ผลิตภัณฑ์ บริษัท หรือบริการใด ๆ รวมถึงนิติบุคคล ผลิตภัณฑ์ หรือบริการที่เชื่อมโยงอยู่ในเอกสารนี้ การอ้างอิงถึงนิติบุคคลเชิงพาณิชย์ ผลิตภัณฑ์ กระบวนการ หรือบริการใด ๆ โดยการแสดงเครื่องหมายบริการ เครื่องหมายการค้า ผู้ผลิต หรืออื่น ๆ ไม่ได้ถือเป็นการรับรอง การแนะนำ หรือการสนับสนุนจากหน่วยงานผู้จัดทำ

เอกสารนี้ใช้เครื่องหมาย TLP:CLEAR กำกับ การเปิดเผยข้อมูลไม่มีข้อจำกัด แหล่งข้อมูลอาจใช้เครื่องหมาย TLP:CLEAR เมื่อข้อมูลมีความเสี่ยงที่จะถูกนำไปใช้งานในทางที่ผิดน้อยมากหรือไม่มีเลย ทั้งนี้ให้เป็นไปตามกฎและขั้นตอนที่เกี่ยวข้องสำหรับการเผยแพร่สู่สาธารณะ ขึ้นอยู่กับกฎลิขสิทธิ์มาตรฐาน ข้อมูลที่มีเครื่องหมาย TLP:CLEAR สามารถแจกจ่ายได้โดยไม่มีข้อจำกัด สำหรับข้อมูลเพิ่มเติมเกี่ยวกับมาตรฐานการจัดการและเผยแพร่ Traffic Light Protocol กรุณาดูที่ cisa.gov/tlp

MITRE ATT&CK – ประวัติกลยุทธ์ย้อนหลังที่น่าสนใจของ APT40

การสอดแนม (Reconnaissance) (TA0043)	
Search Victim-Owned Websites (T1594)	Gather Victim Identity Information: Credentials (T1589.001)
Active Scanning: Vulnerability Scanning (T1595.002)	Gather Victim Host Information (T1592)
Search Open Websites/Domains: Search Engines (T1593.002)	Gather Victim Network Information: Domain Properties (T1590.001)
Gather Victim Identity Information: Email Addresses (T1589.002)	

การพัฒนาทรัพยากร (Resource Development) (TA0042)	
Acquire Infrastructure: Domains (T1583.001)	Acquire Infrastructure (T1583)
Acquire Infrastructure: DNS Server (T1583.002)	Compromise Accounts (T1586)
Develop Capabilities: Code Signing Certificates (T1587.002)	Compromise Infrastructure (T1584)
Develop Capabilities: Digital Certificates (T1587.003)	Develop Capabilities: Malware (T1587.001)
Obtain Capabilities: Code Signing Certificates (T1588.003)	Establish Accounts: Cloud Accounts (T1585.003)
Compromise Infrastructure: Network Devices (T1584.008)	Obtain Capabilities: Digital Certificates (T1588.004)

การเข้าถึงในขั้นต้น (Initial Access) (TA0001)	
Valid Accounts (T1078)	Phishing (T1566)
Valid Accounts: Default Accounts (T1078.001)	Phishing: Spearphishing Attachment (T1566.001)
Valid Accounts: Domain Accounts (T1078.002)	Phishing: Spearphishing Link (T1566.002)
External Remote Services (T1133)	Exploit Public-Facing Application (T1190)
Drive-by Compromise (T1189)	

การดำเนินการ (Execution) (TA0002)	
Windows Management Instrumentation (T1047)	Command and Scripting Interpreter: Python (T1059.006)
Scheduled Task/Job: At (T1053.002)	Command and Scripting Interpreter: JavaScript (T1059.007)
Scheduled Task/Job: Scheduled Task (T1053.005)	Native API (T1106)
Command and Scripting Interpreter (T1059)	Inter-Process Communication (T1559)
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	System Services: Service Execution (T1569.002)
Command and Scripting Interpreter: PowerShell (T1059.001)	Exploitation for Client Execution (T1203)
Command and Scripting Interpreter: Visual Basic (T1059.005)	User Execution: Malicious File (T1204.002)
Command and Scripting Interpreter: Unix Shell (T1059.004)	Command and Scripting Interpreter: Apple Script (T1059.002)
Scheduled Task/Job: Cron (T1053.003)	Software Deployment Tools (T1072)

การฝังตัวในระบบ (Persistence) (TA0003)	
Valid Accounts (T1078)	Server Software Component: Web Shell (T1505.003)
Office Application Startup: Office Template Macros (T1137.001)	Create or Modify System Process: Windows Service (T1543.003)
Scheduled Task/Job: At (T1053.002)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Scheduled Task/Job: Scheduled Task (T1053.005)	Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
External Remote Services (T1133)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
Scheduled Task/Job: Cron (T1053.003)	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Account Manipulation (T1098)	Valid Accounts: Cloud Accounts (T1078.004)
Valid Accounts: Domain Accounts (T1078.002)	

การยกระดับสิทธิพิเศษ (Privilege Escalation) (TA0004)	
Scheduled Task/Job: At (T1053.002)	Create or Modify System Process: Windows Service (T1543.003)
Scheduled Task/Job: Scheduled Task (T1053.005)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Process Injection: Thread Execution Hijacking (T1055.003)	Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
Process Injection: Process Hollowing (T1055.012)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)

การยกระดับสิทธิพิเศษ (Privilege Escalation) (TA0004)	
Valid Accounts: Domain Accounts (T1078.002)	Exploitation for Privilege Escalation (T1068)
Access Token Manipulation: Token Impersonation/Theft (T1134.001)	Event Triggered Execution: Unix Shell Configuration Modification (T1546.004)
Process Injection: Dynamic-link Library Injection (T1055.001)	Valid Accounts: Domain Accounts (T1078.002)
Valid Accounts: Local Accounts (T1078.003)	

การหลบเลี่ยงการป้องกัน (Defence Evasion) (TA0005)	
Rootkit (T1014)	Indirect Command Execution (T1202)
Obfuscated Files or Information (T1027)	System Binary Proxy Execution: Mshta (T1218.005)
Obfuscated Files or Information: Software Packing (T1027.002)	System Binary Proxy Execution: Regsvr32 (T1218.010)
Obfuscated Files or Information: Steganography (T1027.003)	Subvert Trust Controls: Code Signing (T1553.002)
Obfuscated Files or Information: Compile After Delivery (T1027.004)	File and Directory Permissions Modifications: Linux and Mac File and Directory Permissions Modification (T1222.002)
Masquerading: Match Legitimate Name or Location (T1036.005)	Virtualisation/Sandbox Evasion: System Checks (T1497.001)
Process Injection: Thread Execution Hijacking (T1055.003)	Masquerading (T1036)
Reflective Code Loading (T1620)	Impair Defences: Disable or Modify System Firewall (T1562.004)
Process Injection: Process Hollowing (T1055.012)	Hide Artifacts: Hidden Files and Directories (T1564.001)
Indicator Removal: File Deletion (T1070.004)	Hide Artifacts: Hidden Window (T1564.003)
Indicator Removal: Timestomp (T1070.006)	Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
Indicator Removal: Clear Windows Event Logs (T1070.001)	Hijack Execution Flow: DLL Side-Loading (T1574.002)
Modify Registry (T1112)	Web Service (T1102)
Deobfuscate/Decode Files or Information (T1140)	Masquerading: Masquerade Task or Service (T1036.004)
Impair Defenses (T1562)	

การเข้าถึงข้อมูลประจำตัว (Credential Access) (TA0006)	
OS Credential Dumping: LSASS Memory (T1003.001)	Unsecured Credentials: Credentials in Files (T1552.001)
OS Credential Dumping: NTDS (T1003.003)	Brute Force: Password Guessing (T1110.001)
Network Sniffing (T1040)	Forced Authentication (T1187)

การเข้าถึงข้อมูลประจำตัว (Credential Access) (TA0006)	
Credentials from Password Stores: Keychain (T1555.001)	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)
Input Capture: Keylogging (T1056.001)	Multi-Factor Authentication Interception (T1111)
Steal Web Session Cookie (T1539)	Steal Application Access Token (T1528)
Exploitation for Credential Access (T1212)	Brute Force: Password Cracking (T1110.002)
Input Capture: Web Portal Capture (T1056.003)	OS Credential Dumping: DCSync (T1003.006)
Credentials from Password Stores (T1555)	Credentials from Password Stores: Credentials from Web Browsers (T1555.003)

การค้นพบ (Discovery) (TA0007)	
System Service Discovery (T1007)	System Information Discovery (T1082)
Application Window Discovery (T1010)	Account Discovery: Local Account (T1087.001)
Query Registry (T1012)	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
File and Directory Discovery (T1083)	System Time Discovery (T1124)
Network Service Discovery (T1046)	System Owner/User Discovery (T1033)
Remote System Discovery (T1018)	Domain Trust Discovery (T1482)
Account Discovery: Email Account (T1087.003)	Account Discovery: Domain Account (T1087.002)
System Network Connections Discovery (T1049)	Virtualisation/Sandbox Evasion: System Checks (T1497.001)
Process Discovery (T1057)	Software Discovery (T1518)
Permission Groups Discovery: Domain Groups (T1069.002)	Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
System Network Configuration Discovery: Internet Connection Discovery (T1016.001)	

การแทรกซึมต่อภายในเครือข่าย (Lateral Movement) (TA0008)	
Remote Services: Remote Desktop Protocol (T1021.001)	Remote Services (T1021)
Remote Services: SMB/Windows Admin Shares (T1021.002)	Use Alternate Authentication Material: Pass the Ticket (T1550.003)
Remote Services: Windows Remote Management (T1021.006)	Lateral Tool Transfer (T1570)

การรวบรวมข้อมูล (Collection) (TA0009)	
Data from Local System (T1005)	Archive Collected Data: Archive via Library (T1560.002)
Data from Network Shared Drive (T1039)	Email Collection: Remote Email Collection (T1114.002)

การรวบรวมข้อมูล (Collection) (TA0009)	
Input Capture: Keylogging (T1056.001)	Clipboard Data (T1115)
Automated Collection (T1119)	Data from Information Repositories (T1213)
Input Capture: Web Portal Capture (T1056.003)	Data Staged: Remote Data Staging (T1074.002)
Data Staged: Local Data Staging (T1074.001)	Archive Collected Data (T1560)
Email Collection (T1114)	

การลักลอบนำข้อมูลออก (Exfiltration) (TA0010)	
Exfiltration Over C2 Channel (T1041)	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002)
Exfiltration Over Alternative Protocol (T1048)	Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)

ระบบสั่งการและควบคุม (Command and Control) (TA0011)	
Data Obfuscation: Protocol Impersonation (T1001.003)	Web Service: Dead Drop Resolver (T1102.001)
Commonly Used Port (T1043)	Web Service: One-way Communication (T1102.003)
Application Layer Protocol: Web Protocols (T1071.001)	Ingress Tool Transfer (T1105)
Application Layer Protocol: File Transfer Protocols (T1071.002)	Proxy: Internal Proxy (T1090.001)
Proxy: External Proxy (T1090.002)	Non-Standard Port (T1571)
Proxy: Multi-hop Proxy (T1090.003)	Protocol Tunnelling (T1572)
Web Service: Bidirectional Communication (T1102.002)	Encrypted Channel (T1573)
Encrypted Channel: Asymmetric Cryptography (T1573.002)	Ingress Tool Transfer (T1105)
Proxy, Technique T1090 - Enterprise | MITRE ATT&CK®	

ผลกระทบ (Impact) (TA0040)	
Service Stop (T1489)	Disk Wipe (T1561)
System Shutdown/Reboot (T1529)	Resource Hijacking (T1496)

บันทึก

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