แนวทางการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ในเขตพื้นที่พุทธสถาน กรณีศึกษาเมสแก๊ง

A Guideline for Ransomware Detection and Prevention at the Buddhist Places : A case study of Maze Gang

คริชณะ ฉิมมณี*
Krishna Chimmanee
มณีสุข โชติรุ่งรัตน์
Maneesook Chotrungrat
วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต, ประเทศไทย
College of Digital Innovation Technology, Rangsit University, Thailand
Email: sanon.s@rsu.ac.th

Received: April 8, 2021
Revised: December 3, 2021
Accepted: December 12, 2021

บทคัดย่อ

เนื่องจากจากการแพร่ระบาดของโรคโควิด ๑๙ ทำให้ตลอดปี ค.ศ. ๒๐๒๐ เป็นช่วงที่การทำงานจากที่บ้าน (Work from home) ได้เข้ามามีบทบาทสำคัญต่อองค์กร ธุรกิจและหน่วยงานทั่วโลก ทำให้ภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ที่เกิดจากการใช้งานอินเทอร์เน็ตเพิ่มมากยิ่งขึ้น โดยเฉพาะภัยจากมัลแวร์เรียกค่าไถ่ จากการสำรวจในปี พ.ศ. ๒๕๖๓ พบว่า มีการโจมตีทางไซเบอร์ด้วยมัลแวร์ประเภทนี้ในเขตพื้นที่พุทธสถาน ดังนั้น งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อศึกษาแนวทางการป้องกันความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่จากการทบทวนวรรณกรรมที่เกี่ยวข้องจากบทความวิจัยต่างประเทศ และใช้กรณีศึกษาจริงจากการโจมตีทางไซเบอร์จากเมสแก๊ง นอกจากนี้ได้รวบรวมผลการวิเคราะห์ต่าง ๆ มาใช้เป็นแนวทางป้องกันการโจมตีจากเมสแก๊ง

จากผลการศึกษาขั้นตอนการโจมตีของเมสแก๊งพบว่า มีพฤติกรรมหลายอย่างที่สามารถนำมาสร้างแนวทางในการป้องกันได้ เช่น การแอบฝังตัวอยู่ในระบบโครงข่ายเป็นเวลานานก่อนที่จะลงมือนำข้อมูลที่สำคัญออกมาจากเครือข่ายของเป้าหมายและดำเนินการเข้ารหัสไฟล์ข้อมูล แต่ถ้ามีมาตรการในการเฝ้าระวังระบบเครือข่ายที่ดีเพียงพอ ก็อาจจะสามารถตรวจพบและระงับภัยคุกคามไซเบอร์ที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่ได้ เป็นต้น ดังนั้น บทความฉบับนี้จึงได้เสนอแนวทางการป้องกันการโจมตีจากมัลแวร์เรียกค่าไถ่เมสแก๊งบนพื้นฐานกรอบแนวคิดของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติกระทรวงพาณิชย์สหรัฐฯ ได้แก่ (๑) การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (๒) การปกป้องดูแลทรัพย์สิน

* รศ.ดร.คริชณะ ฉิมมณี Assoc.Prof.Dr.Krishna Chimmanee

สารสนเทศ (๓) ความสามารถในการตรวจพบเหตุภัยคุกคามไซเบอร์ (๔) การรับมือภัยคุกคาม (๕) การกู้คืนข้อมูลหลังเกิดเหตุภัยคุกคามไซเบอร์

คำสำคัญ: มัลแวร์เรียกค่าไถ่; เมสแก๊ง; ความมั่นคงปลอดภัยไซเบอร์

Abstract

Due to the spread of COVID 19, throughout the year 2020, working from home has played an important part in the organization, businesses and agencies around the world. This makes the various types of cyber threats posed by the use of the internet even more, especially the threat of ransomware. A survey in 2020 showed that cyberattacks with this type of malware were found in Buddhist areas. Thus, this research aimed to study how to protect cyber assets against ransomware by reviewing relevant literature from foreign research articles as well as the real case studies of the cyber attack from Maze gang. In addition, this research is to study the prevention and detection of ransomware from the research articles in order to introduce a guideline to prevent ransomware from happening in the future.

From the study of Maze gang's attack pattern, they employed generally the same attack techniques that can be used to create a preventative approach, such as trying to maintain their foothold and hiding in the network for a long time before taking the sensitive information out of the target's network and encrypting the data file. However, if we have effective monitoring systems, the suspicious cyber threat will be detected and prevented from incurring. Therefore, this article presents the guideline for the prevention from Maze ransomware based on the concept of the National Institute of Standards and Technology of the United States Department of Commerce, which are: (1) Establishing cybersecurity measurement (2) Safeguarding information assets (3) Cyber threat detection capability (4) threat response (5) Post-disaster data recovery after the cyber incident.

Keywords: Ransomware; Maze gang; Cyber security.

บทนำ

ในปี พ.ศ. ๒๕๖๓ จากรายงานของแบล็คฟ็อก[๑] ซึ่งเป็นบริษัทชั้นนำในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านมัลแวร์เรียกค่าไถ่พบว่า มีการจ่ายเงินเนื่องจากมัลแวร์เรียกค่าไถ่สูงถึง ๓๔ ล้าน

[๑] BLACKFOG, **The State of Ransomware in 2021.** [Online], Available: https://www.blackfog.com/category/ransomware/ [1 March 2021].

ดอลลาร์ นอกจากนี้มีการคาดการณ์ว่า มีอาชญากรรมไซเบอร์เกิดขึ้นกับองค์กรต่าง ๆ ทุก ๑๑ วินาที และคาดว่ามีมูลค่าความเสียหายจากการโจมตีเหล่านี้สูงถึงประมาณ ๒๐ พันล้านดอลลาร์ภายในปี พ.ศ. ๒๕๖๔ ซึ่งหนึ่งในสามของสาเหตุการถูกโจมตีเกิดจากผู้ใช้งานภายในองค์กรเอง โดยเพิ่มขึ้นร้อยละ ๘ จาก พ.ศ. ๒๕๖๔ เนื่องจากสถานการณ์โควิดส่งผลให้บุคลากรต้องทำงานที่บ้านและใช้การเข้าถึงเครือข่ายจากระยะไกลมากขึ้น จากเหตุการณ์ที่เกิดขึ้นในปีที่ผ่านมาทำให้องค์กรได้เรียนรู้ว่า การทำงานจากระยะไกลเป็นช่องโหว่ที่สำคัญของการโจมตีทางไซเบอร์ ปกติในอดีตที่ผ่านมา มัลแวร์เรียกค่าไถ่จะเน้นการเข้ารหัสไฟล์ข้อมูล แต่จากรายงานของแซก วิดเทคเกอร์[๒] พบว่า เมสแก๊งได้ใช้วิธีการนำข้อมูลออกมาจากองค์กร ก่อนจะทำการเข้ารหัสข้อมูล และข่มขู่ที่จะนำข้อมูลสำคัญมาเปิดเผยแพร่ในเว็บไซต์สาธารณะ เพื่อสามารถใช้เป็นเงื่อนไขในการเรียกค่าไถ่ให้ได้มากที่สุด และในเดือนมิถุนายน พ.ศ. ๒๕๖๓ รองผู้ว่าการสารสนเทศและสื่อสาร การไฟฟ้าส่วนภูมิภาค (กฟภ.) ยอมรับว่าโดนมัลแวร์เรียกค่าไถ่จากเมสแก๊งโจมตี และส่งผลให้แอพพลิเคชั่นพีอีเอสมาร์ทพลัสไม่สามารถใช้งานได้ ในลำดับถัดมาข้อมูลของ กฟภ. ที่ถูกขโมยออกไปโดยเมสแก๊งได้ถูกนำไปเผยแพร่ในเว็บสาธารณะ เนื่องจาก กฟภ. ตัดสินใจที่จะไม่จ่ายค่าไถ่[๓] จากบทเรียนที่ผ่านมาทำให้องค์กรตระหนักว่า การสูญเงินจากมัลแวร์เรียกค่าไถ่มีมูลค่าที่สูงกว่า การซื้ออุปกรณ์รักษาความมั่นคงปลอดภัยไซเบอร์และการฝึกอบรมพนักงานให้ตระหนักรู้ถึงภัยคุมคามไซเบอร์

จากการรายงานของเพอเพิลเซก[๔] (Purplesec) พบว่าองค์กรการศึกษาเป็นเป้าหมายที่ใหญ่ที่สุดของการโจมตีแรนซัมแวร์ในปี พ.ศ. ๒๕๖๒ โดยสูงถึงร้อยละหกสิบเอ็ด ส่งผลให้การเรียนการสอนของสถาบันการศึกษาประมาณ ๑,๒๓๓ แห่งต้องหยุดชะงัก เมื่อวันที่ ๒๖ กุมภาพันธ์ พ.ศ. ๒๕๖๓ โรงเรียนสปาตันเบิร์ก (Spartanburg Country School District) ได้ตกเป็นเหยื่อของการโจมตีมัลแวร์เรียกค่าไถ่ โดยส่งผลให้การเชื่อมต่ออินเทอร์เน็ตและการเข้าถึงเครือข่ายถูกปิดเป็นเวลาสามวัน แม้จะพบว่าไม่มีข้อมูลรั่วไหล แต่ก็ทำให้การเข้าถึงออนไลน์ถูกระงับทั้งหมด ซึ่งปัจจุบันนี้ในเขตพุทธสถานพระภิกษุสงฆ์ได้ใช้อินเทอร์เน็ตในการเผยแพร่พุทธศาสนาอย่างแพร่หลายโดยเฉพาะสื่อสังคมออนไลน์[๕] ทำให้ในเขตพุทธสถานที่มีบริการอินเทอร์เน็ตมีโอกาสเสี่ยงต่อภัยคุกคามทางไซเบอร์ โดยเฉพาะเขตพุทธสถานที่เป็นสถาบันการศึกษา เช่น มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย ซึ่งมีพระภิกษุ สามเณรและคฤหัสถ์เข้าศึกษา

---

[๒] Whittaker, Z., **Maze, a notorious ransomware group, says it's shutting down.** [Online], Available: https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/ [3 November 2020].

[๓] I-SECURE, **"กลุ่ม Maze Ransomware ปล่อยข้อมูลชุดสมบูรณ์ 100% ของการไฟฟ้าส่วนภูมิภาคแล้ว"**, [ออนไลน์]. แหล่งที่มา: https://www.i-secure.co.th/2020/07/กลุ่ม-maze-ransomware-ปล่อยข้อมูลชุดส/ [๒๒ กรกฎาคม, ๒๔๖๓].

[๔] Firch, J., PurpleSec LLC, **10 Cyber Security Trends You Can't Ignore In 2021**. [Online], Available: https://purplesec.us/cyber-security-trends-2021/ [31 December 2020].

[๕] พระมหาเอก เมธิกญาโณ เจตสลัน, "พฤติกรรมการใช้สื่อสังคมออนไลน์ ของพระนิสิตระดับปริญญาตรี มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย อำเภอวังน้อย จังหวัดพระนครศรีอยุธยา", **วารสารมหาจุฬาวิชาการ**, ปีที่ ๗ ฉบับที่ ๒ (๒๗ สิงหาคม ๒๕๖๓) : หน้า ๑๗๙-๑๙๐.

ต่อระดับปริญญาตรี โท เอก ดังนั้นจึงมีความจำเป็นที่จะต้องศึกษาแนวทางรักษาความมั่นคงปลอดภัยในเขตพุทธสถาน

งานวิจัยฉบับนี้ได้ทบทวนวรรณกรรมจากต่างประเทศที่เกี่ยวข้องกับมัลแวร์เรียกค่าไถ่จากเมสแก๊ง ซึ่งเป็นข้อมูลทุติยภูมิ และได้แบ่งออกเป็น ๕ ขั้นตอน ได้แก่ วิธีการเจาะระบบเครือข่าย (Initial Access) การโจรกรรมข้อมูลเพื่อยกระดับสิทธิ (Credential Theft) การขยายการโจมตีไปยังเน็ตเวิร์คที่เกี่ยวข้อง (Lateral Movement) การแอบฝังตัวในระบบเครือข่าย (Persistence) การติดตั้งมัลแวร์เรียกค่าไถ่ (Payload) พร้อมทั้งได้ศึกษาการโจมตีจากสถานการณ์จริงของเมสแก๊ง เพื่อนำมาวิเคราะห์ขั้นตอนเชิงลึก และนำแนวทางการป้องกันตามสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology – NIST) มาประยุกต์ใช้ เพื่อสร้างหาแนวทางการป้องกันการโจมตีมัลแวร์เรียกค่าไถ่จากเมสแก๊ง

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาหาแนวทางการรักษาความมั่นคงปลอดภัยจากเมสแก๊งในเขตพื้นที่พุทธสถาน

ทบทวนวรรณกรรม

การทบทวนบทความวิจัยต่างประเทศของไอทริปเปิลอี (IEEE: The Institute of Electrical and Electronics Engineers) มีดังนี้

ใน ค.ศ. ๒๐๑๗ ได้มีบทความวิจัยกล่าวถึง วิธีการโจมตีของมัลแวร์เรียกค่าไถ่จำนวน ๗ สายพันธุ์ พร้อมทั้งได้ยกตัวอย่างกรณีศึกษาที่ประเทศอินเดีย และได้แนะนำวิธีการแก้ไขมัลแวร์เรียกค่าไถ่ในกรณีที่เครื่องคอมพิวเจอร์ได้ติดมัลแวร์แล้ว รวมถึงได้แนะนำขั้นตอนการป้องกันการโจมตี[๖]

ในปี ค.ศ. ๒๐๑๘ ได้มีบทความวิจัยกล่าวถึง ลักษณะการโจมตีของมัลแวร์เรียกค่าไถ่ในอดีต และคาดการณ์การขยายตัวของมัลแวร์เรียกค่าไถ่ในอนาคต โดยได้แบ่งออกเป็น ๓ ขั้นตอน ดังนี้ วิธีการโจมตี วิธีการป้องกัน และแนวโน้มการพัฒนามัลแวร์เรียกค่าไถ่ในอนาคต[๗]

ในปี ค.ศ. ๒๐๑๙ ได้มีบทความวิจัยกล่าวถึง วิธีที่ใช้รับมือมัลแวร์เรียกค่าไถ่ที่เกี่ยวข้องกับอินเตอร์เน็ตของสรรพสิ่ง (IOT) และสรุปผลสิ่งที่ได้เรียนรู้จากการถูกโจมตี ข้อควรระวัง และวิธีการแก้ปัญหาที่เป็นไปได้[๘]

---

[๖] Saxena, S. & Soni, H.K.,"Strategies for Ransomware Removal and Prevention". **IEEE 4th International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB-18),** (2017) : 1-4.

[๗] Garg, D., Thakral A., Nalwa T., & Choudhury T., "A past examination and future expectation: Ransomware". **IEEE International Conference on Advances in Computing & Communication Engineering,** (2018) : 243-247.

[๘] Zahra, S.R. & Chishti, M.A., "RansomWare_and Internet of Things: A New Security Nightmare". **IEEE International Conference on Cloud Computing, Data Science & Engineering,** (2019) : 551-555.

ในปี ค.ศ. ๒๐๒๐ ได้มีบทความวิจัยกล่าวถึง รายละเอียดวิวัฒนาการของมัลแวร์เรียกค่าไถ่โดยเริ่มจากปี ค.ศ. ๑๙๘๙ ซึ่งสายพันธุ์แรกที่ถูกค้นพบเรียกว่า AIDS Trojan โดยได้โจมตีองค์การอนามัยโลก ตั้งแต่ช่วงปี ค.ศ. ๒๐๑๕ ถึง ๒๐๑๙ มีมัลแวร์เรียกค่าไถ่ที่สำคัญ เช่น Locker (2015), Petya (2016), WannaCry (2017), Artemis (2017), Bad Rabbit (2017), GandCrab (2018), Dharma (2019), LockerGoga (2019) และ SamSam (2019)

นอกจากนี้ บทความดังกล่าวยังได้ให้เหตุผลในการพิจารณาตัดสินใจว่าควรจะจ่ายค่าไถ่หรือไม่ วิธีการหลีกเลี่ยงปัญหาของมัลแวร์เรียกค่าไถ่ และวิธีการแก้ไขมัลแวร์เรียกค่าไถ่ในกรณีที่เครื่องคอมพิวเตอร์ได้ติดมัลแวร์แล้ว พร้อมทั้งแสดงสถิติข้อมูลการติดมัลแวร์เรียกค่าไถ่ในช่วงปี ค.ศ. ๒๐๑๗ ถึง ค.ศ. ๒๐๑๘ โดยในปี ค.ศ. ๒๐๑๗ ประเทศไทยถูกจัดอันดับเป็นเป้าหมายการโจมตีสูงที่สุด[๙] บทความวิจัยในลำดับถัดมาได้กล่าวถึง ขั้นตอนการทำงานของมัลแวร์เรียกค่าไถ่ District ซึ่งใช้ไฟล์ District.exe และเรียกใช้ไฟล์ดีแอลแอล (DLL) หลายไฟล์ เช่น ADVAPI32.dll นอกจากนี้ทรัพยากรของระบบปฏิบัติการวินโดวส์ยังถูกเรียกใช้งานจากมัลแวร์เป็นอย่างมาก เช่น ไฟล์ csrss.exe, svchost.exe, tasking.exe, services.exe และ TrustedInstaller.exe เป็นต้น[๑๐]

บทความวิจัยในลำดับถัดมาได้อธิบายถึงการทำงานของมัลแวร์เรียกค่าไถ่โดยแบ่งออกเป็น ๕ ขั้นตอน ได้แก่

๑) ช่องทางการแพร่ระบาดมัลแวร์เรียกค่าไถ่ (Infection) โดยแฝงมากับอีเมล์ และมัลแวร์ลิงค์

๒) การสื่อสารติดต่อระหว่างเซิร์ฟเวอร์ของแฮกเกอร์และคอมพิวเตอร์ที่ติดมัลแวร์ (Contact C&C servers)

๓) การเข้ารหัสกุญแจ (Encryption Key Management) หลังจากได้กุญแจเข้ารหัสมาจากเซิร์ฟเวอร์ของแฮกเกอร์ ก็จะทำการเข้ารหัสกุญแจนี้อีกครั้งที่เครื่องเป้าหมาย

๔) การเข้ารหัสไฟล์ข้อมูล (Data encryption) แฮกเกอร์จะทำการเข้ารหัสไฟล์ข้อมูลและลบไฟล์เหล่านั้นทิ้ง

๕) การข่มขู่เรียกค่าไถ่ (Extortion) แฮกเกอร์จะเรียกร้องค่าไถ่ กำหนดเงื่อนไขเวลาการจ่ายค่าไถ่ และวิธีการจ่ายค่าไถ่[๑๑]

---

[๙] Chesti, I.A., Humayun M., Sama, N.U., & Jhanjhi, NZ., "Evolution, Mitigation, and Prevention of Ransomware". **IEEE International Conference on Computer and Information Sciences,** (2020).

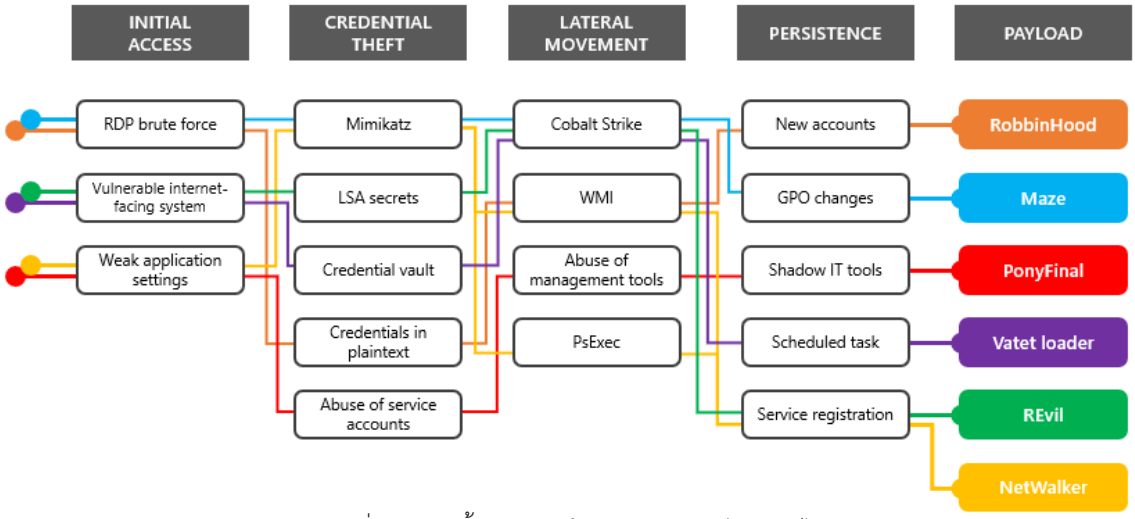
[๑๐] Andes, N., & Wei, M., "District Ransomware: Static and Dynamic Analysis". **IEEE 8th International Symposium on Digital Forensics and Security (ISDFS),** (2020).

[๑๑] Berrueta, E., Morato, D., Magaña, E., & Izal M., "Open Repository for the Evaluation of Ransomware Detection Tools". **IEEE Access,** 2020 (8) : 65658 – 65669.

นอกจากนี้การทบทวนบทความจากต่างประเทศของไมโครซอฟต์[๑๒] แก๊งมัลแวร์เรียกค่าไถ่ที่สำคัญในช่วงปี ค.ศ. ๒๐๑๙ ถึง ๒๐๒๐ ได้แก่ PonyFinal (2020), Maze (2019), REvil (2019) และ NetWalker (2019)

วิเคราะห์ขั้นตอนการโจมตีทางไซเบอร์จากมัลแวร์เรียกค่าไถ่ของเมสแก๊ง

วิธีการโจมตีของแมสแก๊งจะเป็นลักษณะของมัลแวร์เรียกค่าไถ่แบบใช้คนสั่งการ (Human-operated ransomware) ตามที่ไมโครซอฟท์ได้ให้คำนิยามไว้นั้นจะต่างจากมัลแวร์เรียกค่าไถ่แบบแพร่กระจายอัตโนมัติ (Auto-spreading ransomware) โดยรูปแบบจะใกล้เคียงกับการโจมตีประเภทเอพีที (APT : Advanced Persistent Threat) ซึ่งผู้โจมตีจะใช้เวลาหลายเดือนในการเข้ามารวบรวมข้อมูลของระบบก่อน จากนั้นค่อยขยายไปยังเครื่องอื่น ๆ ในเครือข่าย สร้างช่องทางเชื่อมต่อทิ้งไว้ แล้วสุดท้ายค่อยดำเนินการติดตั้งมัลแวร์เรียกค่าไถ่ ทั้งนี้ นอกจากผู้โจมตีจะเจาะระบบเข้ามาเพื่อแพร่กระจายมัลแวร์แล้วอาจมีการโจมตีอย่างอื่นเพิ่มเติมด้วย เช่น ขโมยข้อมูลบัญชีรายชื่อและรหัสผ่าน (Credentials) รวมถึงข้อมูลที่สำคัญ (Sensitive data) โดยเมสแก๊งจะเข้ามาฝังตัวในระบบเครือข่ายและรอคอยจังหวะที่เหมาะสมในการลงมือเพื่อให้มั่นใจว่าจะได้ผลประโยชน์ตอบแทนจากการเรียนค่าไถ่สูงสุด[๑๓] ไมโครซอฟท์ได้นิยามขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่ออกเป็น ๕ ขั้นตอน ดังแสดงในภาพที่ ๑



ภาพที่ ๑ แสดงขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่

[๑๒] Microsoft 365 Defender Threat Intelligence Team, Microsoft., **Ransomware groups continue to target healthcare, critical services; here's how to reduce risk**. [Online], Available: https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/ [28 April 2020].

[๑๓] JERZEWSKI, M., Tripwire, **Ransomware Characteristics and Attack Chains – What you Need to Know about Recent Campaigns**. [Online], Available: https://www.tripwire.com/state-of-security/featured/ransomware-characteristics-attack-chains-recent-campaigns/ [7 July 2020].

๑. วิธีการเจาะระบบเครือข่าย (Initial Access)

จากภาพที่ ๑ โมโครซอฟท์ได้แบ่งออกเป็น ๓ วิธีการหลัก แฮกเกอร์จะลองทุกวิธีที่มีความเป็นไปได้ทั้งหมดจนกว่าจะพบช่องโหว่ เมสแก๊งนิยมใช้การเจาะระบบผ่านโปรโตคอลอาร์ดีพีและการบรูตฟอร์ซ (RDP brute force) เพราะว่าการเจาะระบบผ่านจุดอ่อนของโปรโตคอลอาร์ดีพี (RDP : Remote Desktop Protocol) ซึ่งไม่ได้ใช้เอ็มเอฟเอ (MFA : Multi-Factor Authentication) ทำให้สามารถใช้วิธีบรูตฟอร์ซ (Brute-forcing) ในเดารหัสผ่านได้

๒. การโจรกรรมข้อมูลเพื่อยกระดับสิทธิ (Credential Theft)

หลังจากที่แฮกเกอร์ได้เข้าถึงระบบด้วยการสวมรอยและยกระดับสิทธิ์ แฮกเกอร์จะพยายามที่ดัมพ์ (Dump) ข้อมูลบัญชีรายชื่อและรหัสผ่าน (Credential) ออกมาให้ได้มากที่สุด เทคนิคการดัมพ์ข้อมูลนี้ (Credential Dumping) จะช่วยให้แฮกเกอร์ได้ข้อมูลบัญชีรายชื่อและรหัสผ่านจากระบบปฏิบัติการและซอฟต์แวร์ ข้อมูลเหล่านี้จะช่วยให้แฮกเกอร์สามารถเข้าถึงระบบด้วยสิทธิในระดับสูงได้ เช่น บัญชีโดเมนที่มีสิทธิพิเศษ (Privileged domain account) หรือ ข้อมูลบัญชีรายชื่อและรหัสผ่านในการเข้าเครือข่ายคอมพิวเตอร์อื่น[๑๔] โดยไมโครซอฟท์ระบุว่า เมสแก๊งนิยมใช้เครื่องมือมิมิแคทซ (Mimikatz) ซึ่งเป็นโอเพนซอร์ส (Open source) ซอฟต์แวร์ สำหรับดัมพ์ข้อมูลบัญชีรายชื่อและรหัสผ่าน (Credential Dumping) มันสามารถดึงข้อมูลรหัสผ่านที่ถูกทำการแฮชไว้ (Hashed password) จากหน่วยความจำของโปรเซส lsass.exe นอกจากนี้เครื่องคอมพิวเตอร์ที่รันมิมิแคทซสามารถจะเข้าไปดัมพ์ข้อมูลบัญชีรายชื่อและรหัสผ่านในเอดี (AD : Active Directory) เซิร์ฟเวอร์จากระยะไกลได้ ดังนั้น แฮกเกอร์จึงสามารถขโมยบัญชีรายชื่อและรหัสผ่านของคอมพิวเตอร์ในระบบเครือข่ายได้

๓. การขยายการโจมตีไปยังเน็ตเวิร์คที่เกี่ยวข้อง (Lateral Movement)

ไมโครซอฟท์ได้แบ่งออกเป็น ๔ วิธีการหลัก ดังภาพที่ ๑ และได้ระบุว่าเมสแก๊งนิยมใช้โคบอลต์สไตรค์ ซึ่งเป็นเครื่องมือที่ใช้ในการเจาะระบบ โดยสามารถใช้เพื่อทำสเปียร์ฟิชชิ่ง และการเข้าถึงระบบเครือข่ายโดยการสวมสิทธิ์ รวมถึงมีความสามารถเป็นมัลแวร์ต่าง ๆ ที่ใช้ในการโจมตีระบบ[๑๕] โคบอลต์สไตรค์ประกอบไปด้วยเครื่องมือการทำสเปียร์ฟิชชิ่ง โดยเพียงแค่ใส่ข้อมูลของเป้าหมาย เช่น อีเมล์แอดเดรส จากนั้น ก็จะสร้างฟิชชิ่งยูอาร์เอล (Phishing URLs) ที่น่าเชื่อถือ พร้อมทั้งดำเนินการส่งอีเมล์ไปยังเป้าหมาย และเมื่อบุคคลเป้าหมายทำการกดลิงค์ ก็จะทำการแจ้งแฮกเกอร์ให้ทราบ นอกจากนี้สามารถใช้โคบอลต์สไตรค์ ในการขยายการโจมตีไปยังเน็ตเวิร์คที่เกี่ยวข้อง (Lateral Movement) เช่น การเข้าไปควบคุมเครือข่ายเหล่านั้นโดยไม่ต้องใช้มัลแวร์ การรันคำสั่งจากระยะไกล

---

[๑๔] Süleyman Özarslan, Picus Labs, MITRE ATT&CK T1003 Credential Dumping. [Online], Available https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1003-credential-dumping [1 July 2020].

[๑๕] Cynet, Cobalt Strike: White Hat Hacker Powerhouse in the Wrong Hands. [Online], Available https://www.cynet.com/network-attacks/cobalt-strike-white-hat-hacker-powerhouse-in-the-wrong-hands/ [27 July 2020].

๔. การแอบฝังตัวในระบบเครือข่าย (Persistence)

จากหลักฐานดิจิทัลที่ได้มาจากการทำแผนตอบสนองภัยคุกคามไซเบอร์โดยทีมดาร์ท (DART : Microsoft Detection and Response Team) ของไมโครซอฟท์รายงานว่า แฮกเกอร์ได้ค่อย ๆ แทรกซึมเข้ามาในระบบเครือข่ายเป้าหมายตั้งแต่ช่วงต้นปี ค.ศ. ๒๐๒๐ แล้ว และได้ใช้วิธีแบบคนสั่งการ (human-operated) โดยแฮกเกอร์ก็ต้องพยายามสรรหาวิธีการใหม่ ๆ ในการแอบฝังตัวเองให้อยู่ในระบบเครือข่ายของเป้าหมายให้ได้นานที่สุดเป็นเวลาหลายเดือน โดยที่เหยื่อไม่รู้ตัว และพยายามรวบรวมการบันทึกข้อมูลบัญชีรายชื่อและรหัสของผู้ใช้ในระบบให้ได้มากที่สุด รวมถึงอาจจะมีการสร้างบัญชีที่มีสิทธิ์พิเศษขึ้นใหม่ในเครือข่ายอีกด้วย นอกจากนี้ยังพยายามที่จะเพิ่มแบ็คดอร์ (Backdoors) ต่าง ๆ ในในกรณีที่มัลแวร์ได้ถูกตรวจพบและลบออกไป แฮกเกอร์ก็สามารถที่จะเข้าควบคุมเครือข่ายได้อีกครั้งโดยผ่านแบ็คดอร์ที่แอบเปิดช่องทางไว้ ทำให้สามารถโจมตีเครือข่ายได้อีกเป็นครั้งที่สอง การแฝงตัวในเครือข่ายเป็นเวลานาน จะช่วยทำให้สามารถรวบรวมข้อมูลที่สำคัญได้มากและขยายวงการโจมตีออกไปอย่างกว้างขวาง เพื่อให้ได้รับประโยชน์จากการเรียกค่าไถ่ให้ได้มากที่สุด เมสแก๊งจะเริ่มเปิดเผยตัวตนโดยใช้มัลแวร์เรียกค่าไถ่ในขั้นตอนสุดท้าย (payload) ดังนั้น ผู้ดูแลระบบเครือข่ายจึงควรหมั่นตรวจสอบหาเหตุการณ์ความผิดปกติที่อาจจะเกิดขึ้น เช่น การตั้งค่านโยบายเพื่อควบคุมการทำงานของเครื่องคอมพิวเตอร์และผู้ใช้งานในจีพีโอ (GPO : Group Policy Object) หรือ กำหนดความมั่นคงปลอดภัยในเครือข่าย การติดตั้งและการอัพเดทซอร์ฟแวร์ การรันสคริปต์ เป็นต้น

กระบวนการฝังตัวของเมสแก๊งในเครือข่ายนอกจากจะใช้การเปลี่ยนแปลงจีพีโอเพื่อทำให้นโยบายความมั่งคงปลอดภัยเกิดความหละหลวมแล้ว แมสแก๊งยังได้ใช้วิธีการ Schedule Task อีกด้วย โดยจะพยายามหลีกเลี่ยงการติดตั้งไฟล์มัลแวร์ต่าง ๆ (Fileless) แต่จะพยายามใช้ฟีเจอร์ของ Schedule Task ในการทำหน้าตั้งเวลา การทำงานต่าง ๆ ร่วมกับการใช้คำสั่ง PowerShell จากระยะไกล

๕. เปย์โหลด (Payload)

ขั้นตอนสุดท้ายของการโจมตีจะเป็นการสั่งติดตั้งมัลแวร์เรียกค่าไถ่ ซึ่งหลายครั้งเป็นการสั่งดาวน์โหลดมัลแวร์มาติดตั้งโดยใช้คำสั่ง PowerShell ซึ่งเกี่ยวข้องกับซีทูซี (C2C: Command-and-control) เพื่อสื่อสารกับไอพีแอดแดรสของแฮกเกอร์ รวมถึงใช้ในการนำข้อมูลส่งออกนอกระบบเครือข่าย ซึ่งอาจจะใช้วิธีส่งผ่านโปรโตคอลอาร์ดีพี เอชทีทีพี (HTTP) เอฟทีพี (FTP) หลังจากแฮกเกอร์ได้นำข้อมูลที่สำคัญของเป้าหมายออกมาเป็นที่น่าพอใจแล้ว ก็จะดำเนินการเข้ารหัสไฟล์ข้อมูลโดยใช้ขั้นตอนวิธีอาร์เอสเอ (RSA Algorithm) และก็จะทิ้งข้อความเรียกค่าไถ่ไว้เพื่อให้ดำเนินการจ่ายค่าไถ่กับแมสแก๊งได้[๑๖]

[๑๖] ShieldX Networks, **Try Not to Be A'Maze'd.** [Online], Available: https://www.shieldx.com/wp-content/uploads/2020/05/ShieldX-Maze-Ransomware-Blog.pdf [18 November 2020].

กรณีศึกษาจากเหตุการณ์ที่เกิดขึ้นจริง

กรณีศึกษาเมสแก๊ง : วิเคราะห์พฤติกรรมการโจมตีของเมสแก๊งโดยใช้มัลแวร์เรียกค่าไถ่แบบใช้คนสั่งการ (human-operated ransomware)[๑๗] องค์กรขนาดใหญ่แห่งหนึ่งในประเทศสหรัฐอเมริกาได้เริ่มถูกโจมตีในวันเสาร์ที่ ๔ กรกฎาคม ๒๕๖๓ เนื่องจากแฮกเกอร์คาดว่า พนักงานไม่น่าจะทำงานในวันดังกล่าว เพราะเป็นวันชาติของประเทศสหรัฐอเมริกา

๑. วิธีการเจาะระบบเครือข่าย (Initial Access)

เมสแก๊งใช้วิธีการเจาะระบบผ่านโปรโตคอลอาร์ดีพี (RDP: Remote Desktop Protocol) โดยทั่วไปแฮกเกอร์จะสามารถเจาะระบบผ่านโปรโตคอลอาร์ดีพีซึ่งใช้หมายเลขพอร์ตปริยาย รวมถึงตั้งค่าบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ง่าย ด้วยวิธีบรูตฟอร์ซ (Brute-forcing) นอกจากนี้ แม็คอาฟี่ยังพบว่าข้อมูลบัญชีรายชื่อและรหัสผ่านของผู้ใช้งานโปรโตคอลอาร์ดีพีได้ถูกขายในตลาดใต้ดิน (Underground markets) เป็นจำนวนมากในราคาที่ค่อนข้างต่ำ[๑๘]

๒. การโจรกรรมข้อมูลเพื่อยกระดับสิทธิ์ (Credential Theft)

หลังจากที่แฮกเกอร์ได้เจาะระบบผ่านโปรโตคอลอาร์ดีพีแล้ว จะทำการอัพโหลดและติดตั้งไฟล์มัลแวร์ (Beacon payload) ที่ตั้งชื่อเหมือนกับไฟล์ netplwiz.exe และไฟล์ปลอมนี้มีประกาศนียบัตรที่ถูกขโมยมา ทำให้สามารถติดตั้งลงในเครื่องคอมพิวเตอร์เป้าหมายได้

๓. การขยายการโจมตีไปยังเน็ตเวิร์คที่เกี่ยวข้อง (Lateral Movement)

โดยส่วนใหญ่ เมสแก๊งจะใช้เครื่องมือ Cobalt Strike's Beacon ในการขยายวงการโจมตีไปยังเน็ตเวิร์คอื่นภายในองค์กร อย่างไรก็ตาม เมสแก๊งก็อาจใช้วิธีการอาร์ดีพีร่วมด้วยเพื่อเชื่อมต่อไปยังเน็ตเวิร์คอื่น รวมถึงเครื่องมืออื่น เช่น Ngrok เพื่อสร้างการเชื่อมต่อไปยังคอมพิวเตอร์เป้าหมาย และ tscon ในการขโมยเซสชันอาร์ดีพี (Hijack an RDP session) จากนั้นจะทำการติดตั้งไฟล์มัลแวร์ (Beacon payload) โดยวิธีดังกล่าวนี้จะทำให้เมสแก๊งสามารถเข้าถึงคอมพิวเตอร์แม่ข่ายที่ให้บริการในองค์กรได้เป็นจำนวนมาก[๑๙]

---

[๑๗] SENTINELLABS, **Case Study: Catching a Human-Operated Maze Ransomware Attack In Action**. [Online], Available: https://labs.sentinelone.com/case-study-catching-a-human-operated-maze-ransomware-attack-in-action/ [13 August 2020].

[๑๘] Whitney, L., TechRepublic, **How to combat cyberattacks that exploit Microsoft's Remote Desktop Protocol**. [Online], Available: https://www.techrepublic.com/article/how-to-combat-cyber-attacks-that-exploit-microsofts-remote-desktop-protocol/ [7 May 2020].

[๑๙] Kennelly, J., Goody, K., & Shilko, J., FIREEYE, **Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents.** [Online], Available: https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html [7 May 2020].

๔. การแอบฝังตัวในระบบเครือข่าย (Persistence)

โดยปกติเครื่องคอมพิวเตอร์ที่ใช้บริการจากโซลาร์วินดส์ (SolarWinds) จะใช้โปรแกรม RabbitMQ ในการสื่อสารซึ่งใช้ไฟล์ Erlang runtime service (erlsrv.exe) ในการรัน แฮกเกอร์จะอาศัยขบวนการทำงานของไฟล์ erlsrv.exe ในการแฝงตัวเองไว้ในระบบ จากนั้นทำการรีสตาร์ท (Restart) โปรแกรม RabbitsMQ โดยใช้คำสั่งหยุดการทำงานและเริ่มต้นโปรแกรม RabbitsMQ โดยปกติไฟล์ไลบรารี version.dll จะถูกเรียกใช้งานจากแฟ้มข้อมูล System 32 แต่ถ้ามีไฟล์ version.dll อยู่ในแฟ้มข้อมูลเดียวกันกับไฟล์ erlsrv.exe มันจะเรียกใช้ไฟล์ version.dll ที่อยู่ในแฟ้มข้อมูลเดียวกันแทน และไฟล์ไลบรารี acluapi.dll ก็จะถูกเรียกใช้ไปด้วย ซึ่งทั้ง ๒ ไฟล์ไลบรารีนี้เป็นมัลแวร์ที่แฮกเกอร์นำมาใส่ไว้ หลังจากนั้นโปรแกรม Cobalt Strike's Beacon ซึ่งแฝงมากับไฟล์ netplwiz.exe ก็จะสามารถสื่อสารกับ erlsrv.exe ได้ และมีผลทำให้การฝังตัวเป็นไปอย่างสมบูรณ์ ในอีกกรณีหนึ่งแฮกเกอร์ใช้วิธีในทำนองเดียวกันในการแฝงตัวเข้ากับการทำงานปกติของระบบปฏิบัติการ โดยแฮกเกอร์นำไฟล์มัลแวร์ไลบรารีมาใส่ไว้ และไฟล์นี้ถูกเรียกใช้โดยไฟล์ jusched.exe เมื่อโปรแกรม Java Updater เริ่มต้นทำงาน หลังจากแฮกเกอร์ได้ดำเนินการแอบฝังตัวในระบบได้อย่างสมบูรณ์ แฮกเกอร์จะทำการลาดตระเวนค้นหาข้อมูลต่าง ๆ และดำเนินการอัพโหลดโปรแกรมยูทิลิตี้ ngrok ไปยัง C:\Windows\dwm.exe ของคอมพิวเตอร์เป้าหมายอื่น ๆ เพื่อสร้างการเชื่อมไปเป้าหมายต่าง ๆ ในระบบเครือข่าย[๒๒]

๕. เปย์โหลด (Payload)

ปกติไฟล์ mshta.exe ถูกเรียกใช้โดยระบบปฏิบัติการวินโดวส์เพื่อรันไฟล์นามสกุล HTA แต่แฮกเกอร์ได้พัฒนาไฟล์มัลแวร์นามสกุล HTA (HTA Payload) ซึ่งใช้ไฟล์ mshta.exe ในการรัน โดยผู้เชี่ยวชาญจากเซนทินอล (SENTINEL) คาดการณ์ว่าแฮกเกอร์ได้ใช้แนวทางของไฟล์มัลแวร์นามสกุลเอชทีเอ (HTA) ในการทำงานจากระยะไกลบนเครื่องเป้าหมายได้ ก่อนที่จะใช้เครื่องมือ Cobalt Strike Beacon ไฟล์มัลแวร์นามสกุลเอชทีเอน่าจะถูกเขียนขึ้นเองโดยเมสแก๊ง และมีการเข้ารหัสในส่วนของคำสั่งให้มีความซับซ้อน จากข้อมูลที่ได้กล่าวมาสรุปได้ว่า เมสแก๊งมีความสามารถในการคิดค้นพัฒนาวิธีการโจมตี การเข้ายึดครองคอมพิวเตอร์เป้าหมายได้อย่างรวดเร็ว และยากต่อการตรวจจับ

แนวทางป้องกันมัลแวร์เรียกค่าไถ่จากเมสแก๊งตามแนวทางปฏิบัติของ NIST

ในบทนี้จะนำเสนอแนวทางการป้องกันมัลแวร์เรียกค่าไถ่จากเมสแก๊ง โดยแบ่งออกเป็น ๕ ขั้นตอน ตามหลักการของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) เพื่อปรับใช้ในเขตพื้นที่พุทธสถาน ดังนี้

๑. การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify) คือ วิเคราะห์ว่ามีระบบงาน ทรัพย์สิน หรือข้อมูลใดบ้างที่มีความเสี่ยงและอาจส่งผลกระทบต่อการทำงานหากเกิดสถานการณ์การโจมตี มีการจัดลำดับความสำคัญในการดูแลรักษาระบบเครือข่าย เพื่อใช้กำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์

๑. การตรวจสอบรายการที่เกี่ยวข้องกับด้านไอทีทั้งหมด

๑.๑. การตรวจสอบรายการอุปกรณ์ไอทีทั้งหมดภายในองค์กร เพื่อตรวจสอบการอัพเดทแพตช (Patch) และการบำรุงรักษา เพื่อปิดช่องโหว่ (Vulnerability)

๑.๒. การตรวจสอบบัญชีรายชื่อที่ไม่ได้ใช้งาน เช่น พนักงานลาออกไปแล้ว เป็นต้น

๒. การกำหนดมาตรการสำหรับผู้ใช้งาน

๒.๑. พิจารณาก่อนคลิกทุกครั้ง ห้ามดาวน์โหลดไฟล์ทุกชนิดจากเว็บไซต์ที่ไม่น่าเชื่อถือมาติดตั้งลงในคอมพิวเตอร์ขององค์กร ไม่เปิดไฟล์แนบในอีเมลจากบุคคลที่ไม่รู้จัก หรือไม่น่าเชื่อถือ เพื่อป้องการดาวน์โหลดมัลแวร์ ไม่คลิกลิงก์ในอีเมลที่ไม่น่าเชื่อถือ เพื่อป้องกันอีเมล์ฟิชชิ่ง ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่างพอปอัพ (pop-up) เพื่อป้องการดาวน์โหลดมัลแวร์

๒.๒. กำหนดบทลงโทษกับผู้ฝ่าฝืนนโยบาย เช่น การส่งจดหมายแจ้งเตือน

๒.๓. ห้ามใช้อุปกรณ์แฟลชไดร์ฟ (Flash drive) หรืออุปกรณ์ส่วนตัวเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายภายในองค์กร หากมีความจำเป็นต้องขออนุญาตจากผู้ดูแลระบบ

๒.๔. ใช้รหัสผ่านที่แข็งแรง ไม่ซ้ำกัน

๒.๕. ไม่ใช้บัญชีรายชื่อและรหัสผ่านร่วมกัน

๒. การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect) คือ การวางมาตรฐานควบคุมเพื่อปกป้องดูแลระบบขององค์กร การพัฒนาและดำเนินการป้องกันความปลอดภัยทางไซเบอร์อย่างเหมาะสม ได้แก่ การควบคุมการเข้าถึง การรับรู้และการฝึกอบรม ความปลอดภัยของข้อมูล การคุ้มครองข้อมูล กระบวนการและขั้นตอน ซ่อมบำรุง และเทคโนโลยีการป้องกัน

๑. แยกส่วนระบบเครือข่าย (Network segregation) เพื่อลดผลกระทบจากการแพร่กระจายมัลแวร์ผ่านเครือข่าย

๒. การกำหนดสิทธิการเข้าถึงเครือข่าย ตามหน้าที่รับผิดชอบ (Authentication, Authorization)

๓. การควบคุมการเข้าถึงจากระยะไกล (Remote Access)

๓.๑ การเปลี่ยนหมายเลขพอร์ตปริยาย 3389 ของโปรโตคอลอาร์ดีพี

๓.๒ ใช้การพิสูจน์ตัวตนหลายขั้นตอนแบบเอ็มเอฟเอ

๓.๓ จำกัดบัญชีหมายเลขไอพีแอดเดรสที่สามารถใช้การเชื่อมต่อจากระยะไกล รวมถึงการเชื่อมต่อจากวีพีเอ็น (VPN: Virtual Private Network)

๔. การฝึกอบรมพนักงานทางด้านการรักษาความมั่นคงปลอดภัย เช่น

๔.๑ การจำลองสถานการณ์การโจมตีทางไซเบอร์ (Cyber Drill)

๔.๒ ความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Management)

๔.๓ แผนตอบสนองภัยคุกคามไซเบอร์ (Incident Management Plan)

๔.๔ แผนกอบกู้สถานการณ์ภัยพิบัติ (Business Continuity Plan)

๕. เทคโนโลยีการป้องกัน เช่น Security Information and Event Management (SIEM), Firewall, IPS/IDS, Email Security, Antivirus, Endpoint Detection Software

๓. ความสามารถในการตรวจพบเหตุภัยคุกคามไซเบอร์ (Detect) คือ การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับเหตุภัยคุกคามไซเบอร์

๑. ความผิดปกติและเหตุการณ์ (anomalies and events) คือ การจัดเก็บบันทึกกิจกรรม (log) เช่น จากอุปกรณ์ไฟร์วอลล์ (Firewall) จากอุปกรณ์ไอพีเอส (IPS : Intrusion Protection System) จากเอดี (AD)

๒. การเฝ้าระวังความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security continuous monitoring) และกระบวนการตรวจจับ (detection processes)

๒.๑ อุปกรณ์ในการเฝ้าระวัง เช่น ไอพีเอส ดับเบิลยูไอดีเอส (WIDS), เซียม (SIEM: Security Information and Event Management) และอีดีอาร์ (EDR :Endpoint Detection and Response)

๒.๒ นักวิเคราะห์ด้านความปลอดภัย (Security Analyst), ทีมเซิรต์ (Cert :Cyber emergency response team) และซ็อก (SOC : security operation center)

๔. การรับมือภัยคุกคาม (Respond) คือ การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

๑. การวางแผนการตอบโต้ (response planning)

๑.๑ กำหนดบทบาทหน้าที่ของคนแต่ละคนในองค์กรไว้ล่วงหน้าเมื่อถูกโจมตี

๑.๒ ตัดการเชื่อมต่อทางเครือข่าย สำหรับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เพื่อป้องกันการกระจายของมัลแวร์ไปยังระบบสารสนเทศอื่น

๑.๓ เปลี่ยนรหัสผ่านที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงรหัสผ่านของอุปกรณ์เครือข่ายและระบบทั้งหมด และหลังจากที่ได้กำจัดมัลแวร์ต่าง ๆ ออกจากระบบหมดแล้ว ต้องดำเนินการเปลี่ยนรหัสผ่านใหม่ทั้งหมดอีกครั้งที่ใช้งานผ่านระบบควบคุมบัญชีผู้ใช้งานทั้งหมด[๒๐]

๒. การสื่อสาร (Communications)

๒.๑ แจ้งเหตุไปยังหน่วยงานภายในต่าง ๆ ที่เกี่ยวข้อง และผู้ใช้บริการระบบภายในให้ทราบ

๒.๒ แจ้งเหตุไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและไทยเซิร์ต

๓. การวิเคราะห์ (Analysis) คือ การตรวจสอบสายพันธุ์ของมัลแวร์เรียกค่าไถ่ โดยอาศัยข้อมูลที่ปรากฏในเครื่องคอมพิวเตอร์ ที่ติดมัลแวร์ เช่น นามสกุลของไฟล์ที่เปลี่ยนไป ข้อความที่ปรากฏบนหน้าจอในการเรียกค่าไถ่ เพื่อประเมินวิธีการแก้ไขปัญหา เช่น การกู้คืนข้อมูล เป็นต้น

---

[๒๐] Singh, A., **Ransomware: How to Prevent or Recover from an Attack.** [Online]. Available: https://www.backblaze.com/blog/complete-guide-ransomware/ [13 October 2020].

๔. การลดผลกระทบ (Mitigation) คือ แผนชี้แจงต่อสาธารณะชน องค์กรใหญ่ ๆ ที่มีชื่อเสียง หากตกเป็นข่าวด้านความปลอดภัยในการดูแลข้อมูลขึ้นมา จะส่งผลต่อความเชื่อใจของลูกค้าที่มีกับองค์กร ดังนั้น การแถลงการณ์ต่อสื่อ การติดต่อกับผู้ดูแลกฎหมาย สิ่งเหล่านี้ควรวางแผนไว้ก่อน เพื่อให้รับมือกับสถานการณ์ที่เกิดขึ้นได้อย่างรวดเร็วที่สุด

๕. การปรับปรุงการตอบโต้ (Improvements) คือ ปรับแผนการตอบโต้ให้มีประสิทธิภาพมากขึ้นจากเหตุการณ์จริงที่เกิดขึ้น หรืออ้างอิงจากกรณีศึกษาที่ทันสมัย

๕. การกู้คืนข้อมูลและระบบหลังเหตุภัยคุกคามไซเบอร์ (Recovery) คือ การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

๑. แผนการคืนสภาพ (Recovery planning) คือ การวางแผนล่วงหน้าในการรับมือมัลแวร์เรียกค่าไถ่ และทำการทดสอบด้วยแผนรับมือที่สามารถกู้คืนสถานการณ์เลวร้ายที่เกิดจากการถูกโจมตีทางไซเบอร์ ควรเป็นมาตรฐานสำคัญของแผนธุรกิจ ซึ่งแผนรับมือเมื่อถูกมัลแวร์เรียกค่าไถ่โจมตีเป็นสิ่งที่ขาดไปไม่ได้เลยในปัจจุบันนี้ โดยแผนที่วางต้องไม่ใช่แค่การป้องกัน หรือแค่การกู้คืนข้อมูลที่สำรองไว้

๒. การปรับปรุงการคืนสภาพ (improvements) คือ การปรับแผนการคืนสภาพให้มีประสิทธิภาพมากขึ้นจากเหตุการณ์จริงที่เกิดขึ้น หรือจากกรณีศึกษาที่ทันสมัย

๓. การสื่อสาร (communications)

๑.๑ การสื่อสารระหว่างหน่วยงานภายในองค์กร เพื่อให้ทราบความคืบหน้าและขั้นตอนของการกู้คืนระบบเป็นระยะ ๆ

๑.๒ ในกรณีที่ไม่สามารถให้บริการแก่ผู้รับบริการภายนอกได้ ต้องเตรียมเหตุผลเพื่อการประชาสัมพันธ์สำหรับเหตุการณ์ดังกล่าว โดยให้มีผลกระทบต่อองค์กรให้น้อยที่สุด

อภิปรายผลและข้อเสนอแนะ

บทความฉบับนี้ได้ใช้วิธีวิเคราะห์ขั้นตอนการโจมตีของมัลแวร์เรียกค่าไถ่เมสแก๊งจากกรอบไมโครซอฟท์ เนื่องจากกลุ่มเป้าหมายการโจมตีของมัลแวร์เรียกค่าไถ่ส่วนใหญ่เป็นผู้ใช้ระบบปฏิบัติการวินโดวส์ โดยสอดคล้องกับข้อมูลของบอริส[๒๑] ที่ระบุว่าร้อยละ ๙๓ ของมัลแวร์เรียกค่าไถ่เป็นไฟล์นามสกุล exe ซึ่งทำงานบนระบบปฏิบัติการวินโดวส์ สำหรับขั้นตอนการป้องกันควรนำ NISTIR 8374 (ฉบับร่าง) ที่อาจจะออกเป็นฉบับสมบูรณ์ในปี พ.ศ. ๒๕๖๕ มาประยุกต์ใช้เพิ่มเติมเพื่อต่อยอดแนวทางที่นำเสนอให้กลายเป็นเฟรมเวิร์ก (Framework) ที่สมบูรณ์สามารถนำมาปรับใช้ได้ในทุกองค์กร

---

[๒๑] Boris, T., **Windows Users Beware: 95% of Ransomware Attacks Target Microsoft's OS.** [Online]. Available: https://www.techtimes.com/articles/266728/20211015/windows-users-ransomware-attack-windows-ransomware-windows-microsoft-google-report.htm [15 October 2021].

บรรณานุกรม

พระมหาเอก เมธิกญาโณ เจตสลัน. “พฤติกรรมการใช้สื่อสังคมออนไลน์ ของพระนิสิตระดับปริญญาตรี มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย อำเภอวังน้อย จังหวัดพระนครศรีอยุธยา”. **วารสารมหาจุฬาวิชาการ**. ปีที่ ๗ ฉบับที่ ๒ (พฤษภาคม-สิงหาคม ๒๕๖๓) : ๑๗๙-๑๙๐.

Berrueta, E., Morato, D., Magaña, E., & Izal M., “Open Repository for the Evaluation of Ransomware Detection Tools”. **IEEE Access**, 2020 (8) : 65658 – 65669.

Garg, D., Thakral A., Nalwa T., & Choudhury T., “A past examination and future expectation: Ransomware”. **IEEE International Conference on Advances in Computing & Communication Engineering,** (2018) : 243-247.

Chesti, I.A., Humayun M., Sama, N.U., & Jhanjhi, NZ., “Evolution, Mitigation, and Prevention of Ransomware”. **2nd IEEE International Conference on Computer and Information Sciences (ICCIS),** (2020).

Andes, N., & Wei, M., “District Ransomware: Static and Dynamic Analysis”. **IEEE 8th International Symposium on Digital Forensics and Security (ISDFS),** (2020).

Saxena, S. & Soni, H.K.,“Strategies for Ransomware Removal and Prevention”. **IEEE 4th International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB-18),** (2017) : 1-4.

Zahra, S.R. & Chishti, M.A., “RansomWare and Internet of Things: A New Security Nightmare”. **IEEE International Conference on Cloud Computing, Data Science & Engineering,** (2019) : 551-555.

เว็บไซต์

BLACKFOG, **The State of Ransomware in 2021.** [Online], Available: https://www.blackfog.com/category/ransomware/ [1 March 2021].

Whittaker, Z., **Maze, a notorious ransomware group, says it’s shutting down.** [Online], Available: https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/ [3 November 2020].

I-SECURE, **“กลุ่ม Maze Ransomware ปล่อยข้อมูลชุดสมบูรณ์ 100% ของการไฟฟ้าส่วนภูมิภาคแล้ว”**, [ออนไลน์]. แหล่งที่มา : https://www.i-secure.co.th/2020/07/กลุ่ม-maze-ransomware-ปล่อยข้อมูลชุดส/ [๒๒ มิถุนายน ๒๕๖๓].

Firch, J., PurpleSec LLC, **10 Cyber Security Trends You Can’t Ignore In 2021.** [Online], Available: https://purplesec.us/cyber-security-trends-2021/ [31 December 2020].

Microsoft 365 Defender Threat Intelligence Team, Microsoft., **Ransomware groups**

continue to target healthcare, critical services; here's how to reduce risk. [Online], Available: https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/ [28 April 2020].

JERZEWSKI, M., Tripwire, **Ransomware Characteristics and Attack Chains – What you Need to Know about Recent Campaigns.** [Online], Available: https://www.tripwire.com/state-of-security/featured/ransomware-characteristics-attack-chains-recent-campaigns/ [7 July 2020].

Süleyman Özarslan, Picus Labs, **MITRE ATT&CK T1003 Credential Dumping.** [Online], Available https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1003-credential-dumping [1 July 2020].

Cynet, Cobalt Strike: **White Hat Hacker Powerhouse in the Wrong Hands.** [Online], Available: https://www.cynet.com/network-attacks/cobalt-strike-white-hat-hacker-powerhouse-in-the-wrong-hands/ [27 July 2020].

ShieldX Networks, **Try Not to Be A'Maze'd.** [Online], Available: https://www.shieldx.com/wpcontent/uploads/2020/05/ShieldX-Maze-Ransomware-Blog.pdf [18 November 2020].

SENTINELLABS, **Case Study: Catching a Human-Operated Maze Ransomware Attack In Action.** [Online], Available: https://labs.sentinelone.com/case-study-catching-a-human-operated-maze-ransomware-attack-in-action/ [13 August 2020].

Whitney, L., TechRepublic, **How to combat cyberattacks that exploit Microsoft's Remote Desktop Protocol.** [Online], Available: https://www.techrepublic.com/article/how-to-combat-cyberattacks-that-exploit-microsofts-remote-desktop-protocol/ [7 May 2020].

Kennelly, J., Goody, K., & Shilko, J., FIREEYE, **Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents.** [Online], Available: https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html [7 May 2020].

Singh, A., **Ransomware: How to Prevent or Recover from an Attack.** [Online]. Available: https://www.backblaze.com/blog/complete-guide-ransomware/ [13 October 2020].