บันทึกข้อความ

ส่วนงาน สำนักบริหารเทคโนโลยีสารสนเทศ โทร. 0 2218 3314 โทรสาร 0 2218 3338

ที่ อว 64.2.11/0441 **วันที่** 23 สิงหาคม 2565

เรื่อง แจ้งเตือนกรณีพบภัยคุกคามจาก Botnet ชื่อ RapperBot

เรียน คณบดี/ผู้อำนวยการสถาบัน/ศูนย์/สำนัก/วิทยาลัย และหน่วยงานอื่นๆ

ด้วยสำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย ได้รับการแจ้งเตือนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.สกมช.) เกี่ยวกับภัยคุกคามจาก Botnet ชื่อ RapperBot กำหนดเป้าหมายการโจมตีที่ระบบปฏิบัติการ Linux Servers ด้วยการ SSH Brute-Forcing Attack ซึ่งเป็นรูปแบบการโจมตีด้วยการเข้าควบคุมเครื่องผ่านการคาดเดา username และ password ทั้งนี้หากทางหน่วยงานของท่านมีการใช้งานระบบปฏิบัติการดังกล่าว ควรตรวจสอบข้อมูลที่เกี่ยวข้อง และปฏิบัติตามคำแนะนำเพื่อลดความเสี่ยงที่จะถูกโจมตี ดังรายละเอียดตามเอกสารแนบ

และหากทางหน่วยงานประสงค์จะทราบข้อมูลเพิ่มเติม หรือ ความช่วยเหลือใดๆ กรุณาติดต่อหน่วยประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ สำนักบริหารเทคโนโลยีสารสนเทศ โทร 83413 หรืออีเมล csirt@chula.ac.th

จึงเรียนมาเพื่อโปรดพิจารณา

(นายรุ่งโรจน์ กิตติถาวรกุล)
ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ

เรียน รองคณบดีฝ่ายนวัตกรรมการศึกษาและสารสนเทศ
เพื่อโปรดพิจารณา

(นางสุชิรา ปัญญาสันติกุล)
ผู้อำนวยการฝ่ายบริหาร
๒๓ สิงหาคม ๒๕๖๕

เรียน หัวหน้าภาควิชา/หน่วยงาน
เพื่อโปรดทราบ

(รองศาสตราจารย์ นายแพทย์วันล่า กุลวิชิต)
รองคณบดีฝ่ายนวัตกรรมการศึกษาและสารสนเทศ
24 สิงหาคม 2565

ประชาสัมพันธ์ในภาควิชา

(รศ.ดร.นพ.วิโรจน์ ศรีอุฬารพงศ์)
หัวหน้าภาควิชาอายุรศาสตร์
26 สิงหาคม 2565

TLP:CLEAR

เอกสารการแจ้งเตือนกรณีพบภัยคุกคามจาก Botnet ชื่อ RapperBot

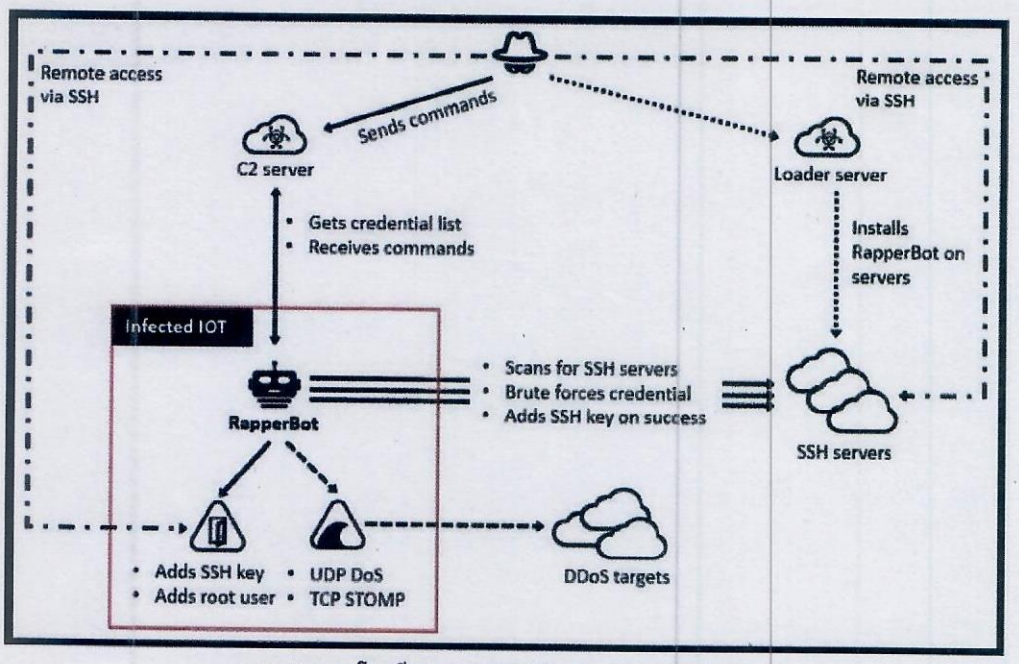
ตามกระดาษเขียนข่าวที่ สกมช 0820/599 ลงวันที่ 15 สิงหาคม 2565

แจ้งเตือนกรณีกรณีพบภัยคุกคามจาก Botnet ชื่อ RapperBot กำหนดเป้าหมายการโจมตีที่ระบบปฏิบัติการ Linux Servers ด้วยการ SSH Brute-Forcing Attack

1. ได้ปรากฏข่าวสารผ่านแหล่งข่าวเปิด กรณีพบภัยคุกคามจาก Botnet ชื่อ RapperBot มีเป้าหมายการโจมตี คือระบบปฏิบัติการ Linux Servers ในรูปแบบ SSH Brute-Forcing Attack[1]

2. มีรูปแบบการโจมตีด้วยการเข้าควบคุมเครื่องผ่านการคาดเดา username และ password ที่โปรแกรม SSH (Secure Shell) เพื่อเข้าสู่ระบบโดยไม่ได้รับอนุญาต ทำการสุ่มรหัสผ่านของระบบจนกว่าจะเจอรหัสที่ถูกต้อง เพื่อเข้าถึงเครื่องปลายทางได้โดยไม่จำเป็นต้องไปใช้งานที่หน้าจอคอนโซลของเครื่อง

3. ผู้โจมตีใช้ไฟล์ /.ssh/authorized_keys เพื่อเข้าถึงระบบโดยใส่คีย์สาธารณะ SSH ซึ่งช่วยให้ผู้โจมตีสามารถเข้าสู่ระบบและรับรองความถูกต้องกับเซิร์ฟเวอร์โดยไม่ต้องระบุรหัสผ่าน



ภาพแสดงการโจมตีรูปแบบ SSH Brute-Forcing Attack

คำแนะนำเบื้องต้นและแนวทางในการรับมือเหตุการณ์ดังกล่าวสามารถทำได้ดังนี้[2]

1. ไม่ควรให้ root สามารถ login ได้จาก Remote login และตั้งรหัสผ่านที่มีความซับซ้อน โดยรหัสผ่านไม่ควรเป็นคำศัพท์ วันเดือนปีเกิด เลขที่อยู่ และควรมีความยาวอย่างน้อย 8 ตัวอักษร มีการใช้ตัวพิมพ์ใหญ่ เล็ก มีอักขระพิเศษ และตัวเลข ผสมอยู่ในรหัสผ่าน และเปลี่ยนรหัสผ่าน ทุกๆ 30 หรือ 90 วัน

2. ใช้ Key pair authentication แทนการใช้รหัสผ่าน

3. เปลี่ยน SSH port เป็นเลขอื่นที่ไม่ใช่ 22

4. ใช้โปรแกรมช่วยป้องกัน เช่น fail2ban

อ้างอิง

1. https://www.bleepingcomputer.com/news/security/new-linux-malware-brute-forces-ssh-servers to-breach-networks/
2. https://www.nipa.cloud/blog/brute-force-attack/

TLP:CLEAR

กระดาษเขียนข่าว

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ความเร่งด่วน-ผู้รับปฏิบัติ		ลำดับความเร่งด่วน-ผู้รับทราบ	วัน เวลา	คำแนะนำในการส่งข่าว
ด่วนที่สุด		ด่วนที่สุด	๑๕ สิงหาคม ๒๕๖๕	
จาก	ผู้อำนวยการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ			
ถึง	ผู้รับปฏิบัติ	ผู้ดูแลระบบ หรือผู้ที่เกี่ยวข้อง		ชั้นความลับ
	ผู้รับทราบ	หัวหน้าส่วนราชการ/หัวหน้าหน่วยงาน		ที่ของผู้ให้ข่าว ที่ สกมช ๐๘๒๐/๒๙๙

๑. เพื่อกรุณาทราบ

๒. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ติดตามสถานการณ์ข้อมูลสารเกี่ยวกับภัยคุกคามทางไซเบอร์ และได้ข่าวสารผ่านแหล่งข่าวเปิด กรณีพบภัยคุกคามจาก Botnet ชื่อ RapperBot มีเป้าหมายการโจมตีคือระบบปฏิบัติการ Linux Servers ในรูปแบบ SSH Brute-Forcing Attack มีรูปแบบการโจมตีด้วยการเข้าควบคุมเครื่องผ่านการคาดเดา username และ password ที่โปรแกรม SSH (Secure Shell) เพื่อเข้าสู่ระบบโดยไม่ได้รับอนุญาต ทำการสุ่มรหัสผ่านของระบบจนกว่าจะเจอรหัสที่ถูกต้อง เพื่อเข้าถึงเครื่องปลายทางได้โดยไม่จำเป็นต้องไปใช้งานที่หน้าจอคอนโซลของเครื่อง นั้น

๓. ในการนี้ ศปช. สกมช. ได้สรุปข้อมูลเกี่ยวกับเหตุการณ์และได้จัดทำคำแนะนำในการแก้ไขเบื้องต้น จึงขอให้ท่านใช้เป็นแนวทางในการป้องกันความเสียหายที่อาจเกิดขึ้นได้ ทั้งนี้ หากมีข้อสงสัยสามารถติดต่อสอบถามเพิ่มเติมได้ที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หมายเลขโทรศัพท์ ๐๒ ๑๑๔ ๓๕๓๑ หรือ E-mail : ncert@ncsa.or.th

<u>หมายหมายเหตุ</u> รายละเอียดเพิ่มเติมปรากฏตามเอกสารการแจ้งเตือน กรณีพบภัยคุกคามจาก Botnet ชื่อ RapperBot

หน้า ๑ ของ ๑ หน้า	อ้างถึงข่าว	ผู้เขียนข่าว	หน่วย	โทรศัพท์
	ชั้นความลับ [ ] กำหนด [/] ไม่กำหนด	พ.ต.อ. (ณัทกฤช พรหมจันทร์)	ศปช.	๐๒ ๑๑๔ ๓๕๓๑
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ		ผู้อนุมัติข่าว พล.อ.ต. (อมร ชมเชย) รอง ลธ.กมช.(๔)/ผอ.ศปช.		

TLP:CLEAR