แจ้งเตือน : การโจมตีจากกลุ่ม จากกรณีความขัดแย้งระหว่างประเทศ

ผลกระทบทางธุรกิจ
- ☐ Financial damage
- ☒ Reputation damage
- ☐ Non-compliance
- ☐ Privacy violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : WHITE

ผู้รับสามารถส่งต่อได้เฉพาะภายในหน่วยงานของผู้รับข้อมูลโดยยึดหลัก need-to-know basis

แจ้งเตือนการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศรัสเซียและยูเครนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช. สกมช.)

วันที่แจ้งเตือน 3 มีนาคม 2565

ตามที่มีรายงานการแจ้งเตือนการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศรัสเซียและยูเครนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช. สกมช.) เมื่อวันที่ 1 มีนาคม 2565 และ ก.ล.ต. ได้ติดตามความคืบหน้าของสถานการณ์อย่างใกล้ชิด โดยพบว่าเริ่มมีการพัฒนาของสถานการณ์ทั้งที่เกิดจากการเรียกร้องจากนานาชาติให้แต่ละประเทศแสดงจุดยืน และถ้อยแถลงในเวทีสากลซึ่งอาจมีโอกาสทำให้ความขัดแย้งขยายตัวมายังประเทศที่ไม่เกี่ยวข้องได้ และเริ่มมีการตรวจพบการใช้งานเครื่องมือที่ผู้ไม่หวังดีหรือช่องโหว่ที่ใช้ในการโจมตี และกิจกรรมในลักษณะเดียวกันอย่างกว้างขวางขึ้น

ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจจะเกิดต่อบริษัทในตลาดทุน จึงขอให้ผู้ประกอบธุรกิจเพิ่มระดับการเฝ้าระวังการโจมตีจากเครื่องมือหรือช่องโหว่ข้างต้นอย่างเข้มงวด และดำเนินการตามคำแนะนำของ ศปช. สกมช. โดยมีรายละเอียดดังนี้

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.สกมช.)
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210 โทรศัพท์ 0-2142-6885 อีเมล์ ncert@ncsa.or.th

TLP : WHITE

แจ้งหน่วยงานป้องกัน ติดตาม เฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ จากกรณีความขัดแย้งในต่างประเทศ

จากกรณีความขัดแย้งระหว่าง “รัสเซีย กับ ยูเครน” ทำให้มีการปฏิบัติการโจมตีทางทหารและการโจมตีทางไซเบอร์เกิดขึ้น โดยมีเหตุการณ์การโจมตีทางไซเบอร์ในระหว่างวันที่ 22 -25 กุมภาพันธ์ 2565 ดังนี้[1]

1. เกิดเหตุการณ์การโจมตีทางไซเบอร์ ในรูปแบบ DDoS (Distributed-denial-of-service) คือการก่อกวนเว็บไซต์ของหน่วยงานสำคัญระดับประเทศ เช่น กระทรวงการต่างประเทศ กระทรวงสาธารณสุข และภาคธนาคาร โดยทำการเข้าถึงหลายเว็บไซต์พร้อม ๆ กัน ทำให้ไม่สามารถเข้าใช้งานได้ ส่งผลให้ระบบเครือข่ายอินเทอร์เน็ตล่ม

2. มีการตรวจพบมัลแวร์ชื่อ Hermetic Wiper ซึ่งมีลักษณะการทำงานที่เน้นการล้างข้อมูลของเป้าหมายบนระบบเครือข่ายภายในประเทศยูเครน ซึ่งบริษัทด้านความปลอดภัยไซเบอร์[2] เปิดเผยว่ามัลแวร์นี้จะสร้างความเสียหายให้กับ Master Boot Record (MBR) ทำให้คอมพิวเตอร์ที่ติดมัลแวร์ไม่สามารถทำงานได้

3. มีการตรวจพบมัลแวร์ชื่อ Cyclops Blink[3] จากกรณีการปลอมแปลงเว็บไซต์หน่วยงานรัฐบาลของประเทศยูเครน ซึ่งในเว็บไซต์ปลอมนี้ทำแคมเปญชื่อว่า ‘Support the President’ หลอกให้ผู้ใช้งานหลงเชื่อทำการคลิกลิงก์ที่เป็นอันตราย จากนั้นมัลแวร์จะถูกดาวน์โหลดไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งานและรวบรวมข้อมูลในอุปกรณ์คอมพิวเตอร์ ซึ่งส่งกระทบต่อระบบเครือข่ายคอมพิวเตอร์ของประเทศยูเครนในขณะนี้

จากเหตุการณ์ดังกล่าวที่เกิดขึ้น สกมช. ได้รวบรวมข้อมูลที่คาดว่าเป็นช่องโหว่ที่ใช้ในการโจมตีเพื่อเข้าถึงบัญชีและเครือข่ายที่มีความปลอดภัยต่ำ โดยแบ่งประเภทตามช่องโหว่[4] ดังนี้

- เครือข่ายเทคโนโลยีสาธารณะ (IT)

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol

จ่าสิบเอก	(สิทธิศักดิ์ มินทบุญ)	ผู้แจ้งเตือน	พันตำรวจเอก (ณัทกฤช พรหมจันทร์) ผู้รับรองข้อมูล
ร้อยตรี	(พีรพัฒน์ สุขเกิด)	ผู้ตรวจสอบ	ผู้อนุมัติการแจ้งเตือน นาวาอากาศเอก (อมร ชมเชย) รอง ลธ.สกมช.(๔)/ผอ.ศปช.

- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare (note: this was a zero-day at time.)
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

- เครือข่ายเทคโนโลยีปฏิบัติการ (OT)/ระบบควบคุมอุตสาหกรรม (ICS)

- ICS Advisory ICS Focused Malware – Havex
- ICS Alert Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
- ICS Alert Cyber-Attack Against Ukrainian Critical Infrastructure Technical Alert CrashOverride Malware
- CISA MAR HatMan: Safety System Targeted Malware (Update B)

ทั้งนี้ หน่วยงานควรเตรียมแผนสำรองการรับมือเหตุการณ์ให้สามารถทำงานได้อย่างต่อเนื่อง หากระบบเกิดการ Offline หรือระบบหยุดชะงัก ทำการตรวจสอบการปิดช่องโหว่ที่อาจได้รับการโจมตี เพิ่มความระวังและติดตามข่าวสารและรายงานจาก สกมช. เพื่อรับการแจ้งเตือนได้ทันท่วงที อย่างไรก็ตาม เพื่อเป็นการป้องกันการโจมตีทางไซเบอร์ที่อาจจะเกิดขึ้น หน่วยงานควรตรวจสอบระบบสารสนเทศภายในองค์กรให้มีความมั่นคงปลอดภัยเพื่อป้องกันตนเองจากภัยคุกคามที่อาจจะเกิดขึ้น โดยสามารถดำเนินการได้ทันทีดังนี้

1. ดำเนินการตรวจสอบและปิดช่องโหว่จากข้อมูลที่คาดว่าเป็นช่องโหว่ที่ใช้ในการโจมตีดังกล่าว
2. สำรองข้อมูลอย่างน้อย 3 ชุด โดยต้องมีการ Backup แบบ Offline และควรให้สำเนาข้อมูลอยู่ในอุปกรณ์จัดเก็บข้อมูล หรือ cloud ที่แยกออกจากระบบงาน และไม่สามารถเข้าถึงได้จากระบบงานปกติ
3. ตรวจสอบระบบการเข้าถึงเครือข่ายจากระยะไกล เช่น Remote Desktop Protocol, Virtual Private Network ว่ามีการเข้าถึงที่ผิดปกติหรือไม่ และควรหมั่นตรวจสอบสิทธิ์ การเข้าถึงระบบอย่างสม่ำเสมอ
4. ควรใช้การยืนยันตัวตนแบบ Two-factor Authentication เป็นอย่างน้อย และตั้งรหัสผ่านให้ซับซ้อนคาดเดาได้ยาก
5. หมั่น Patch คอมพิวเตอร์ ระบบปฏิบัติการ อุปกรณ์ต่าง ๆ รวมถึง Applications ให้ทันสมัยอยู่เสมอ โดยเฉพาะช่องโหว่ที่มีการแจ้งเตือนล่าสุด หรือช่องโหว่ประเภท 0-day ต่าง ๆ เช่น log4j, SolarWinds Supply Chain, Exchange Server และ Win32 Elevation Vulnerability เป็นต้น
6. ติดตั้งโปรแกรมป้องกันมัลแวร์ และอัปเดตให้ทันสมัยอยู่เสมอ

7. ตรวจสอบระบบของพนักงานที่มีการ Work from home โดยเฉพาะระบบที่ System Admin ใช้งาน

8. เพิ่ม Indicators of Compromise (IOCs) ลงในอุปกรณ์รักษาความมั่นคงปลอดภัยของระบบเพื่อเป็นการป้องกันการโจมตีอีกทาง

<u>อ้างอิง</u>

1. https://www.helpnetsecurity.com/2022/02/24/cyber-attacks-ukraine/?utm_source=dlvr.it&utm_medium=linkedin&fbclid=IwAR3N5eiNlpTuOjLRPEDy3O1JoQET8_AE-2bwUcaycXSFW3yurdJTIJJhLXc
2. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
3. https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
4. https://www.cisa.gov/uscert/ncas/alerts/aa22-011a