แฮกเกอร์ก็ชอบวันหยุด

เผยแพร่เมื่อวันที่ 10 เมษายน 2566

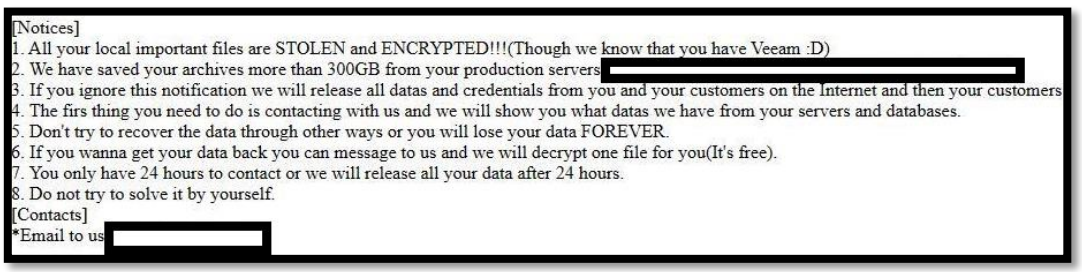
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

เมื่อถึงวันหยุดยาวต่อเนื่องหลายวัน มักเป็นช่วงเวลาที่สร้างรอยยิ้มให้กับคนทำงาน เพราะจะได้พักผ่อนและวางภาระหน้าที่จากการงานลง มีเวลาให้กับตัวเองและครอบครัวมากขึ้น หรือไปเที่ยวในสถานที่ต่าง ๆ

แต่รู้หรือไม่ว่า นอกจาก “พวกเรา” ที่ตั้งตารอวันหยุดอย่างมีความสุขกันแล้ว **“มิจฉาชีพ” ก็ชอบวันหยุดเช่นกัน** เห็นได้จากข่าวอยู่บ่อย ๆ ว่า ในช่วงวันหยุดยาวที่เราหลายคนพักผ่อน มิจฉาชีพจะออกทำงาน เช่น โจรกรรมทรัพย์สิน สำนักงานตำรวจแห่งชาติจึงมีโครงการ “ฝากบ้านไว้กับตำรวจ” เพื่อเฝ้าระวัง ป้องกันการเกิดเหตุ และสร้างความมั่นใจให้กับประชาชน

ในช่วงวันหยุดยาวแบบนี้ก็เป็นเวลาทองของ **“แฮกเกอร์”** เช่นเดียวกัน จากข้อมูลของ Cybersecurity and Infrastructure Security Agency (CISA) และ Federal Bureau of Investigation (FBI) ระบุตรงกันว่า ในอดีตแฮกเกอร์มักจะโจมตีในช่วงวันหยุดสุดสัปดาห์ คือ วันศุกร์และวันเสาร์ **แต่ในปัจจุบันแฮกเกอร์จะเลือกโจมตีในช่วงวันหยุดยาวของเหยื่อในแต่ละประเทศ** เช่น โจมตีเหยื่อในประเทศจีน ช่วงเทศกาลตรุษจีน โจมตีเหยื่อในประเทศญี่ปุ่น ช่วงเทศกาลโอบง เป็นต้น **ส่วนในประเทศไทยอาจได้รับผลกระทบเช่นกัน ในช่วงเทศกาลสงกรานต์**

ในปัจจุบันการโจมตีทางไซเบอร์ที่มักพบบ่อย ๆ คือ Ransomware ที่สามารถโจรกรรมข้อมูลสำคัญจากระบบคอมพิวเตอร์ของเหยื่อเพื่อเรียกค่าไถ่ ในระยะหลังมีการเรียกค่าไถ่เป็นสกุลเงินดิจิทัลเพื่อให้ติดตามได้ยากยิ่งขึ้น ทำให้ Ransomware มีจำนวนและความถี่เพิ่มขึ้นอย่างมากในแต่ละปี ในอดีต Ransomware ทำการโจมตีเพียงการแค่เข้ารหัสไฟล์ในเครื่องของเหยื่อเท่านั้น ถ้าเหยื่อไม่จ่ายเงินค่าไถ่ก็จะไม่สามารถใช้ไฟล์ได้ **แต่ปัจจุบัน Ransomware มีการเข้ารหัสไฟล์ในเครื่องของเหยื่อ รวมถึงโจรกรรมไฟล์โดยนำออกจากระบบของเหยื่อ ซึ่งในไฟล์อาจจะมีข้อมูลสำคัญรวมอยู่ด้วย** เช่น ข้อมูลของลูกค้า เอกสารลับขององค์กร เป็นต้น ถ้าเหยื่อไม่จ่ายเงินค่าไถ่ก็จะถูกข่มขู่ว่าจะเผยแพร่ข้อมูลสำคัญที่โจรกรรมมานั้นลงสู่อินเตอร์เน็ต ให้เป็นข้อมูลที่ใครก็เข้าถึงได้ ซึ่งนั่นเป็นสิ่งที่น่ากลัวอย่างมาก (ดังรูป)


[Notices]
1. All your local important files are STOLEN and ENCRYPTED!!!(Though we know that you have Veeam :D)
2. We have saved your archives more than 300GB from your production servers [redacted]
3. If you ignore this notification we will release all datas and credentials from you and your customers on the Internet and then your customers
4. The firs thing you need to do is contacting with us and we will show you what datas we have from your servers and databases.
5. Don't try to recover the data through other ways or you will lose your data FOREVER.
6. If you wanna get your data back you can message to us and we will decrypt one file for you(It's free).
7. You only have 24 hours to contact or we will release all your data after 24 hours.
8. Do not try to solve it by yourself.
[Contacts]
*Email to us [redacted]

ข้อความที่ผู้ไม่ประสงค์ดี ทิ้งไว้ให้เหยื่อ หลังจากถูก Ransomware โจมตี

จากการสังเกตของผู้เชี่ยวชาญ พบว่า Ransomware ส่วนใหญ่จะมีการบุกรุกเข้ามาในระบบล่วงหน้าและฝังตัวในระบบเป็นเวลานาน (เฉลี่ย 72.5 วัน) เพื่อรอเวลาในช่วงหยุดยาวก่อนที่จะลงมือ ด้วยการเข้ารหัสไฟล์หรือดำเนินการโจรกรรมข้อมูลออกไป จากเหตุการณ์ที่เกิดขึ้นหลายครั้ง มักเริ่มต้นจากการโจมตีผ่าน Phishing Email หรือ Website (ที่มีช่องโหว่) โดยการใช้เทคนิค SQL Injection เพื่อให้ได้ webshell/cmdshell และจากนั้นใช้ Remote Desktop Protocol (RDP) เพื่อส่งและรันโปรแกรม Ransomware ในเครื่องของเหยื่อเพื่อโจรกรรมข้อมูลนำออกนอกระบบและทำการเข้ารหัสไฟล์ในเครื่องของเหยื่อต่อไป

จะเห็นได้ว่า “ภัยคุกคามทางไซเบอร์” เกิดขึ้นได้ทุกวัน ไม่เว้นวันหยุดราชการ ไม่ว่าจะเป็นบุคคลหรือองค์กรย่อมมีโอกาสถูกโจมตีได้ทุกเวลาเช่นกัน ดังนั้น เพื่อลดโอกาสการโจมตีจากผู้ไม่ประสงค์ดี หรือ “แฮกเกอร์” ในการสร้างความเสียหายแก่ระบบงานต่าง ๆ ก่อนวันหยุด วันเสาร์-อาทิตย์ หรือหยุดยาวในช่วงเทศกาล และเพื่อให้วันหยุดพักผ่อนดำเนินไปอย่างราบรื่น **จึงควรเตรียมความพร้อมในการป้องกัน และลดความเสี่ยงจากภัยไซเบอร์ โดยมีข้อแนะนำในเบื้องต้น ดังนี้**

(1) **สำรองข้อมูลที่สำคัญทั้งหมด** โดยแยกเก็บชุดข้อมูลสำรองไว้ และทดสอบการกู้คืนเพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลที่สำรองไว้มาใช้กอบกู้ระบบงาน หรือแก้ไขสถานการณ์และดำเนินธุรกิจต่อไปได้เมื่อจำเป็น

(2) **เปลี่ยนรหัสผ่านบัญชีที่เข้าถึงระบบสำคัญ และเปิดใช้ MFA** (Multi-Factor Authentication) รวมถึงทบทวนสิทธิ์ ข้อมูลผู้ใช้งานในระบบ โดยเฉพาะ User ที่มีสิทธิ์สูงในระบบ (High Privilege) เช่น Root หรือ Administrator เป็นต้น รวมทั้ง Test User หรือ Dummy User ที่เคยถูกสร้างขึ้นเพื่อใช้งานเฉพาะ เมื่อไม่ได้ใช้งานแล้วควรปิดการใช้งาน หรือลบ User ที่ไม่ได้ใช้งานออกจากระบบ

(3) **อัปเดต Anti-Malware และสแกนทั้งระบบ** เพื่อกำจัด Malware ที่อาจฝังตัวอยู่ในระบบ

(4) **อัปเดตโปรแกรม** รวมถึงระบบปฏิบัติการให้เป็นปัจจุบัน เพื่อลดช่องโหว่ในระบบ

(5) **ทบทวนการตั้งค่าการเปิดรีโมทคอมพิวเตอร์จากระยะไกล** (Remote Access) ให้สิทธิ์เฉพาะผู้ที่จำเป็นในการใช้งานเท่านั้น เพื่อลดโอกาสที่ผู้ไม่ประสงค์ดี โดยอาจจะใช้เป็นช่องทางในการสั่ง Run Command ที่ฝังตัวอยู่ในระบบงาน

(6) **ทบทวนตรวจสอบการตั้งค่า Firewall** เพื่อทำการปิดกั้นการเชื่อมต่อที่ไม่ได้ใช้งาน

(7) **ติดตามข่าวสาร Cybersecurity จากแหล่งข้อมูลที่น่าเชื่อถือ** รวมถึงทบทวนและซักซ้อมแผนรับมือตาม Incident Response Handbook ขององค์กร กรณีเกิดเหตุภัยคุกคามทางไซเบอร์

(8) **ตรวจสอบ Website ที่อยู่ในการดูแล/ที่เชื่อมโยงกับระบบงานภายในของบริษัท** เพื่อไม่ให้ถูกใช้เป็นช่องทางในการเข้าถึงระบบงานภายในองค์กรได้ รวมถึงมีการเฝ้าระวังเหตุการณ์ไม่พึงประสงค์ โดยการ Monitor Network Traffic หรือ Log Files ที่ต้องสงสัย

ก.ล.ต. หวังว่าคำแนะนำเบื้องต้นทั้ง 8 ข้อนี้ จะช่วยลดโอกาสที่ “แฮกเกอร์” จะใช้ช่วงวันหยุดยาวเข้ามาสร้างความเสียหายและเดือดร้อนกับผู้ประกอบธุรกิจและผู้ใช้บริการในภาคตลาดทุนได้


กลต
8 ข้อควรทำ ก่อนวันหยุดยาว
เพื่อป้องกันภัยคุกคามทางไซเบอร์ เพราะ "แฮกเกอร์" ก็ชอบวันหยุด
1
สำรองข้อมูลที่สำคัญทั้งหมด
โดยมีการแยกเก็บ
ชุดข้อมูลสำรองไว้
2
เปลี่ยนรหัสผ่านบัญชีที่เข้าถึง
ระบบสำคัญและเปิดใช้ MFA
(Multi-Factor
Authentication)
3
อัปเดต Anti-Malware
และ สแกนทั้งระบบ
เพื่อกำจัด Malware
ที่อาจฝังตัวอยู่ในระบบ
4
อัปเดตโปรแกรม
และระบบปฏิบัติการ
ให้เป็นปัจจุบัน
เพื่อลดช่องโหว่ในระบบ
5
ตรวจสอบการตั้งค่ารีโมท
คอมพิวเตอร์จากระยะไกล
(Remote Access)
6
ตรวจสอบการตั้งค่า Firewall
เพื่อทำการปิดกั้น
การเชื่อมต่อที่ไม่ได้ใช้งาน
7
ติดตามข่าวสาร Cybersecurity จากแหล่งข้อมูลที่น่าเชื่อถือ
รวมถึงทบทวนและซักซ้อมแผนรับมือ
กรณีเกิดเหตุภัยคุกคามทางไซเบอร์
8
ตรวจสอบ Website ที่เชื่อมโยงกับระบบงานภายในของบริษัท
รวมถึงมีการเฝ้าระวังเหตุการณ์ไม่พึงประสงค์
โดยการ Monitor Network Traffic หรือ Log Files ที่ต้องสงสัย
www.sec.or.th สำนักงาน กลต. ThaiSEC_News 1207