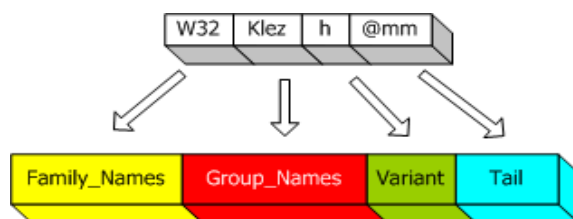


เรื่อง : ชื่อไวรัสบอกอะไรได้บ้าง

เคยสงสัยกันบ้างไหมว่าชื่อของไวรัสที่เห็นทั่วไปนั้นมีความหมายว่าอย่างไร ทำไมบริษัทที่พัฒนาโปรแกรมป้องกันไวรัสจึงตั้งชื่อแตกต่างกันไป ทั้งๆ ที่ไวรัสที่ค้นพบนั้นเป็นตัวเดียวกัน อย่างไรก็ตามแม้ว่าชื่อจะเขียนไม่เหมือนกันทุกตัวอักษร แต่ความหมายที่แปลได้จากชื่อนั้นเขาบอกว่าเหมือนกัน ตัวอย่างเช่น W32.Klez.h@mm, W32/Klez.h@MM, WORM_KLEZ.H I-Worm.Klez.h เป็นต้น บทความนี้จะอธิบายถึงส่วนต่างๆ ของชื่อไวรัส เพื่อให้ผู้อ่านสามารถจำแนกแยกแยะประเภทของไวรัสจากชื่อของไวรัส ความสามารถเด่นๆ ตลอดจนวิธีการแพร่กระจายตัวของไวรัสได้ ส่วนประกอบของชื่อไวสนั้นแบ่งได้เป็นส่วนๆ ดังนี้



รูปที่ 1 แสดงส่วนประกอบต่างๆ ของชื่อไวรัส

1. ส่วนแรกแสดงชื่อตระกูลของไวรัส (Family_Names) ส่วนใหญ่จะตั้งตามชนิดของปัญหาที่ไวรัสก่อขึ้น หรือภาษาที่ใช้ในการพัฒนา เช่น เป็นม้าโทรจัน ถูกพัฒนาด้วย Visual Basic scripts หรือเป็นไวรัสที่รบกวนระบบปฏิบัติการวินโดวส์ 32 บิต เป็นต้น ซึ่งชื่อของตระกูลของไวรัสที่ค้นพบในปัจจุบัน

Family_Names	ความหมาย
WM	ไวรัสที่เป็นมาโครของโปรแกรม Word
W97M	ไวรัสที่เป็นมาโครของโปรแกรม Word 97
XM	ไวรัสที่เป็นมาโครของโปรแกรม Excel
X97M	ไวรัสที่เป็นมาโครของโปรแกรม Excel 97
W32/Win32	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ 32 บิต
WNT	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ NT 32 บิต
I-Worm/Worm	หนอนอินเทอร์เน็ต
Trojan/Troj	ม้าโทรจัน
VBS	ไวรัสที่ถูกพัฒนาด้วย Visual Basic Script
PWSTEAL	ม้าโทรจันที่มีความสามารถในการขโมยรหัสผ่าน
Java	ไวรัสที่ถูกพัฒนาด้วยภาษาจาวา
Linux	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์
Palm	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการ Palm OS
Backdoor	เปิดช่องให้ผู้บุกรุกเข้าถึงเครื่องได้
HILLW	บ่งบอกว่าไวรัสถูกคอมไพล์ด้วยภาษาระดับสูง

ตารางที่ 1 แสดงรายชื่อตระกูลของไวรัส

2. ส่วนชื่อของไวรัส (Group_Name) เป็นชื่อดั้งเดิมที่ผู้เขียนไวรัสเป็นคนตั้ง โดยปกติจะถูกแทรกไว้ในโค้ดของไวรัส และในส่วนนี้เองจะเอามาเรียกชื่อไวรัสเปรียบเสมือนเรียกชื่อเล่น ตัวอย่างเช่น ชื่อของไวรัสคือ W32.Klez.h@mm และจะถูกเรียกว่า Klez.h เพื่อให้สั้นและกระชับขึ้นนั่นเอง

3. ส่วนของ Variant รายละเอียดส่วนนี้จะบอกว่าสายพันธุ์ของไวรัสชนิดนั้นๆ มีการปรับปรุงสายพันธุ์จนมีความสามารถต่างจากสายพันธุ์เดิมที่มีอยู่อย่างไร ลักษณะของ Variant มี 2 ลักษณะคือ

3.1 Major_Variants จะตามหลังส่วนชื่อของไวรัส เพื่อบ่งบอกว่ามีความแตกต่างกันอย่างชัดเจน เช่น หนองชื่อ VBS.LoveLetter.A (A เป็น Major_Variant) แตกต่างจาก BS.LoveLetter อย่างชัดเจน

3.2 Minor_Variants ใช้บ่งบอกในกรณีที่แตกต่างกันเล็กน้อย ในบางครั้ง Minor_Variant เป็นตัวเลขที่บอกขนาดไฟล์ของไวรัส ตัวอย่างเช่น W32.Funlove.4099 หนองชนิดนี้มีขนาดไฟล์เท่ากับ 4099 KB. นั่นเอง

4. ส่วนท้าย (Tail) เป็นส่วนที่จะบอกว่าวิธีการแพร่กระจาย ประกอบด้วย

4.1 @M หรือ @m บอกให้รู้ว่าไวรัสหรือหนองชนิดนี้เป็น "mailer" ที่จะส่งตัวเองผ่านทางอี-เมลล์เมื่อผู้ใช้ส่งอี-เมลล์เท่านั้น

4.2 @MM หรือ @mm บอกให้รู้ว่าไวรัสหรือหนองชนิดนี้เป็น "mass-mailer" ที่จะส่งตัวเองผ่านทุกอี-เมลล์แอดเดรสที่อยู่ในเมลล์บอกซ์

ตัวอย่าง W32.HILLW.Lovgate.C@mm แสดงว่า

- อยู่ในตระกูลที่มีผลต่อระบบปฏิบัติการวินโดวส์ 32 บิต และถูกคอมไพล์ด้วยภาษาระดับสูง
- ชื่อของไวรัสคือ Lovgate
- ที่มี variant คือ C
- มีความสามารถในการแพร่กระจายผ่านทางอี-เมลล์โดยส่งไปยังทุกอี-เมลล์แอดเดรสที่อยู่ในเมลล์บอกซ์

จากส่วนประกอบของชื่อไวรัสที่ได้อธิบายไว้ข้างต้นนั้น จะเห็นได้ว่าชื่อของไวรัสนั้นสามารถบอกถึงประเภทของไวรัส ชื่อดั้งเดิมของไวรัสที่ผู้เขียนไวรัสเป็นคนตั้ง สายพันธุ์ต่างๆ ของไวรัสที่ถูกพัฒนาต่อไป และวิธีการแพร่กระจายตัวของไวรัสเองด้วย

วินัย ปุริเกษม

นักวิชาการคอมพิวเตอร์

มหาวิทยาลัยบูรพา วิทยาเขตจันทบุรี