คู่มือการใช้งานโปรแกรม
ESET Endpoint Antivirus

สำหรับผู้ใช้งานทั่วไป

สารบัญ

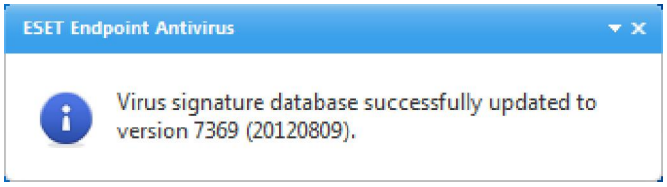
หน้าที่

<u>การใช้งานโปรแกรม ESET Endpoint Antivirus</u>

1. เมื่อทำการติดตั้งโปรแกรม ESET Endpoint Antivirus เสร็จเรียบร้อยสมบูรณ์แล้ว จะมีหน้าต่างโลโก้ของโปรแกรมแสดงขึ้นมาตรงกลางหน้าจอคอมพิวเตอร์ ดังรูปที่ (1)

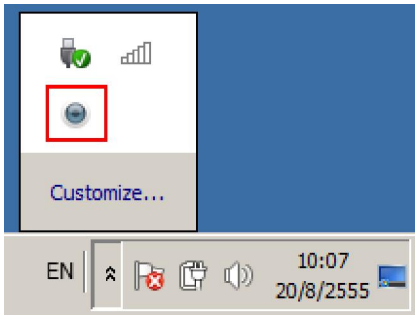
รูปที่ (1)

2. ในกรณีที่เครื่องมีการเชื่อมต่ออินเทอร์เน็ต โปรแกรมจะทำการอัพเดทไฟล์ฐานข้อมูลไวรัสโดยอัตโนมัติ และจะแสดงข้อความหลังจากการอัพเดทฐานข้อมูลไวรัสเสร็จสิ้น (สังเกตุว่าวงเล็บที่ด้านหลังจะเป็นวันที่ออกฐานข้อมูลไวรัสที่อัพเดทล่าสุด) ดังรูปที่ (2)



รูปที่ (2)

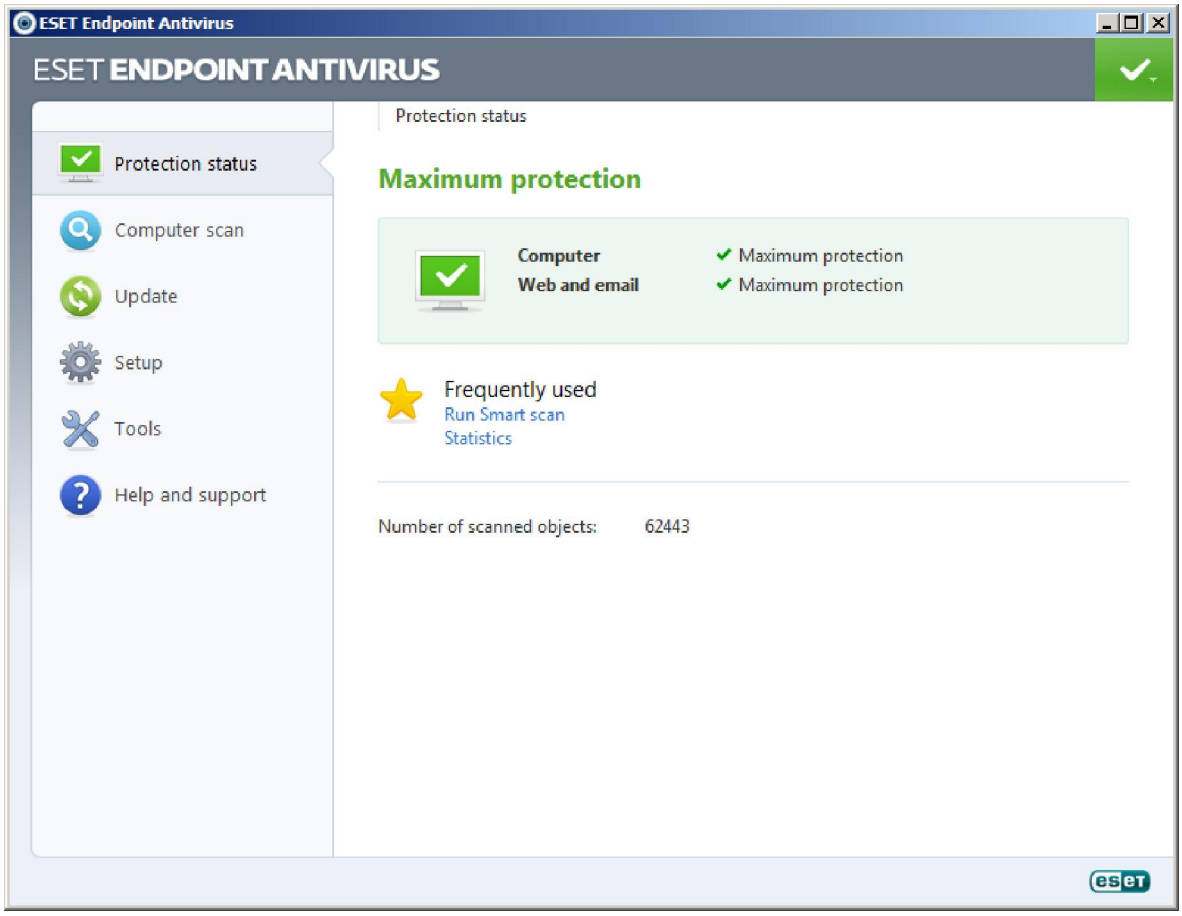
3. เมื่อโปรแกรมรันขึ้นมาแล้ว จะมีไอคอนของโปรแกรมปรากฏที่ซิสเท็มส์เทรย์ ทางมุมขวาล่างของจอภาพ สามารถดับเบิลคลิกที่ไอคอนเพื่อเรียกหน้าต่างโปรแกรม ESET Endpoint Antivirus ขึ้นมาทำงาน ดังรูปที่ (3)



รูปที่ (3)

4. เมื่อเข้าสู่หน้าต่างหลักของโปรแกรมจะแสดงส่วนติดต่อผู้ใช้งาน ดังรูปที่ (4)

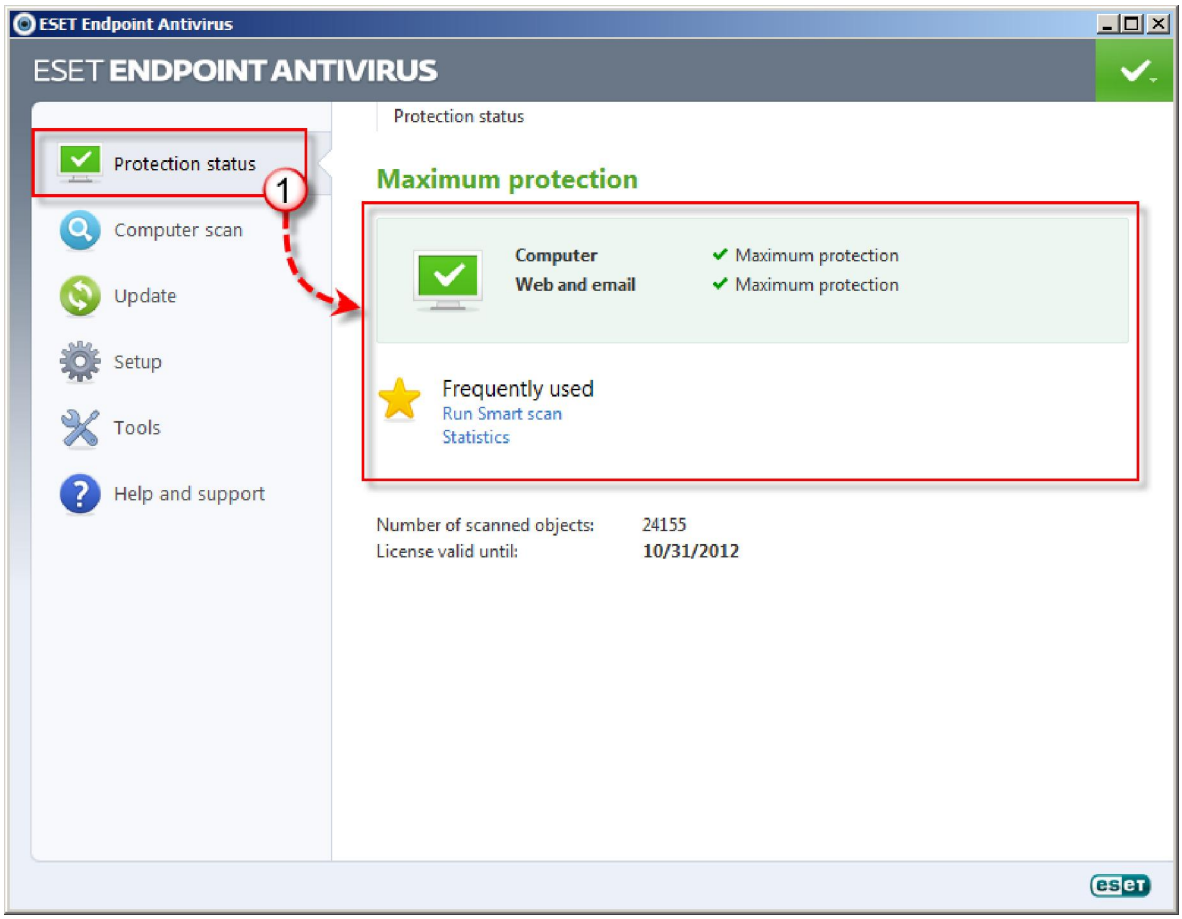
- Protection status แสดงข้อมูลเกี่ยวกับสถานะการป้องกันของ ESET Endpoint Antivirus
- Computer scan ตัวเลือกนี้จะช่วยให้สามารถกำหนดค่าและเปิดใช้การสแกนแบบสมาร์ท หรือ การสแกนที่กำหนดเอง
- Update แสดงข้อมูลเกี่ยวกับการอัพเดทฐานข้อมูลไวรัส
- Setup ปรับระดับความปลอดภัยสำหรับคอมพิวเตอร์, เว็บและอีเมล
- Tools การเข้าถึงไฟล์บันทึก, สถิติการป้องกัน, ติดตามการทำงาน, กระบวนการที่ทำงานอยู่, เครื่องมือวางกำหนดการ, กักเก็บไฟล์ไวรัส, ESET SysInspector (เครื่องมือช่วยตรวจสอบข้อมูลในเครื่อง) และ ESET SysRescue (สร้างซีดีกู้คืน)
- Help and support เรียกดูการเข้าถึงไฟล์วิธีใช้,ฐานความรู้ของ ESET และเข้าสู่เว็บไซต์ของ ESET


ESET Endpoint Antivirus
ESET ENDPOINT ANTIVIRUS
Protection status
Protection status
Computer scan
Update
Setup
Tools
Help and support
Maximum protection
Computer
Web and email
Maximum protection
Maximum protection
Frequently used
Run Smart scan
Statistics
Number of scanned objects: 62443
eset

รูปที่ (4)

การทำงานของ ESET Endpoint Antivirus

1. Protection status (สถานะการป้องกัน)
   เมนูนี้จะแจ้งให้ทราบเกี่ยวกับระดับความปลอดภัยและการป้องกันในปัจจุบันของคอมพิวเตอร์, สถานะการป้องกันสูงสุด หากเป็นสีเขียวจะแสดงว่ามีการป้องกันสูงสุดและตัวโปรแกรมทำงานปกติ นอกจากนี้หน้าต่างสถานะยังแสดงเมนูที่ใช้บ่อยในโปรแกรม ESET Endpoint Antivirus ดังรูปที่ (5)



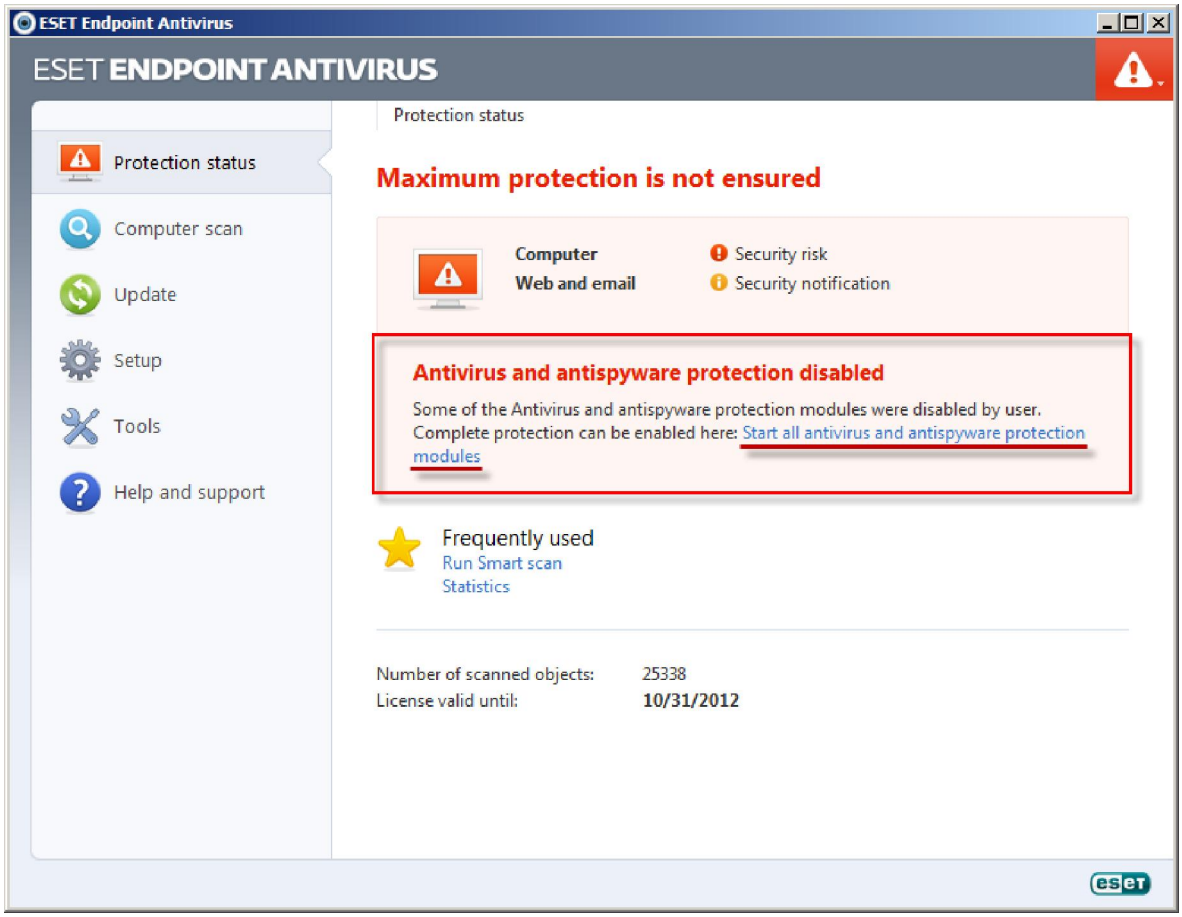
รูปที่ (5)

ถ้าโมดูลที่เปิดใช้งานทำงานได้อย่างถูกต้อง จะมีการระบุเป็นเครื่องหมายถูกสีเขียว แต่ถ้าโปรแกรมทำงานไม่ถูกต้อง จะปรากฏ เครื่องหมายอัศเจรีย์สีแดงหรือไอคอนการแจ้งเตือนสีเหลือง

- ❖ ไอคอนสีแดงเป็นสัญลักษณ์ของปัญหาร้ายแรง - ไม่มีการใช้การป้องกันสูงสุดของคอมพิวเตอร์ สาเหตุที่เป็นไปได้คือ :
  - การทำงานของระบบไฟล์แบบเรียลไทม์ถูกปิดการใช้งาน
  - ฐานข้อมูลไวรัสไม่ได้อัพเดท

- ❖ ไอคอนสีเหลืองแสดงให้ทราบว่าการป้องกันการเข้าถึงเว็บหรืออีเมลไคลเอ็นต์ถูกปิดการใช้งาน, มีปัญหาในการอัพเดทโปรแกรม (ฐานข้อมูลไวรัสที่ไม่ได้อัพเดท ,ไม่สามารถอัพเดทได้)

วิธีแก้ไขคือ คลิกที่ “Start all antivirus and antispyware protection modules” เพื่อเปิดใช้งานการป้องกันสูงสุด ดังรูปที่ (6)



รูปที่ (6)

2. Computer scan (การสแกนคอมพิวเตอร์)

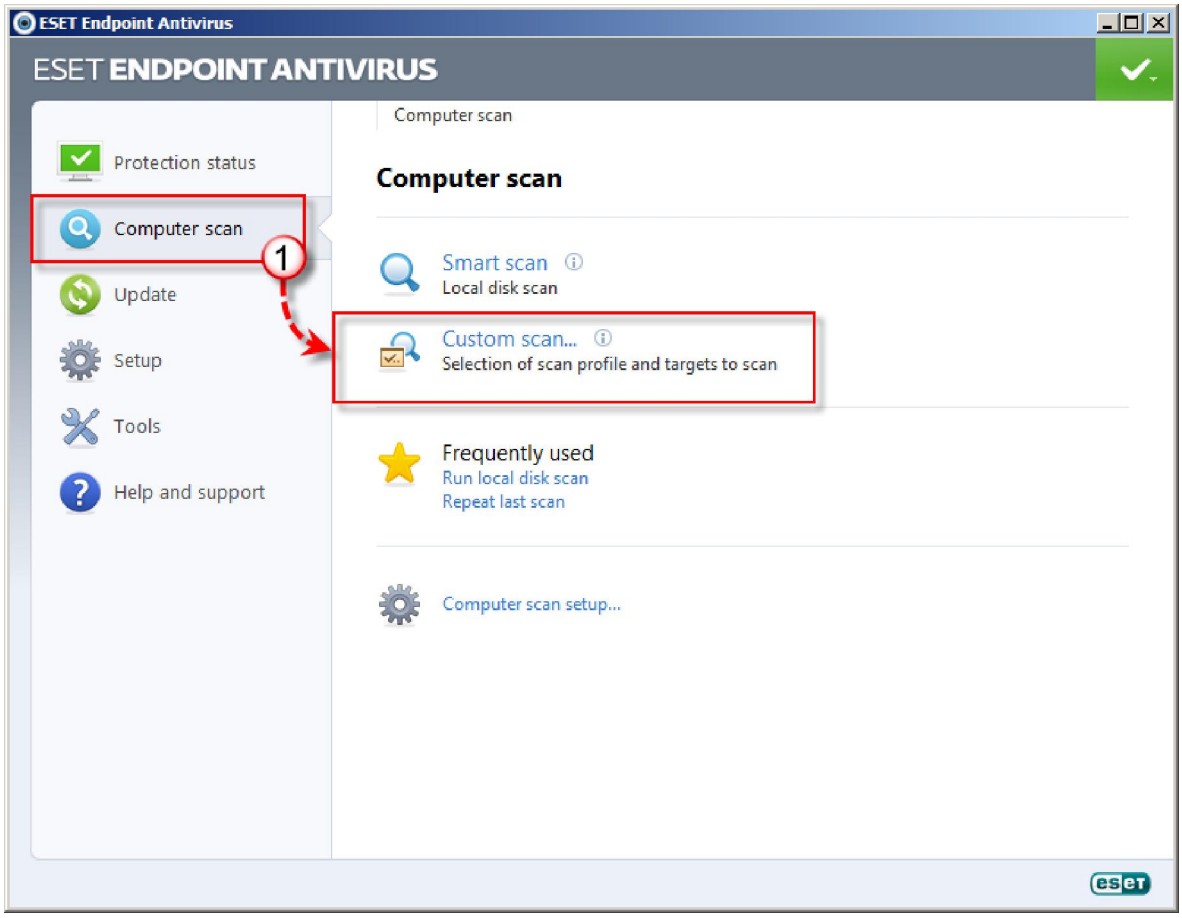
2.1 หลังจากติดตั้ง ESET Endpoint Antivirus ควรดำเนินการสแกนคอมพิวเตอร์เพื่อตรวจหาไฟล์ที่เป็นอันตราย ในหน้าต่างหลักของโปรแกรมให้คลิก “Computer scan”

การสแกนคอมพิวเตอร์แบ่งออกเป็น 2 ประเภท คือ

❖ ***Smart scan*** การสแกนแบบสมาร์ทจะช่วยให้การสแกนคอมพิวเตอร์และกำจัดไฟล์ที่ติดไวรัสได้อย่างรวดเร็ว โดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อดีของการสแกนแบบสมาร์ทก็คือ สามารถใช้งานง่ายและไม่ต้องมีการกำหนดค่าการสแกนโดยละเอียด การสแกนแบบสมาร์ทจะตรวจสอบทุกไฟล์ในไดรฟ์ ในระบบ รวมทั้งกำจัดหรือลบการแฝงตัวที่ตรวจพบโดยอัตโนมัติ

❖ ***Custom scan*** จะช่วยให้สามารถเลือกโปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าได้ และเลือกเป้าหมายการสแกนได้อย่างเจาะจง

สำหรับในที่นี้ขอแนะนำให้ เลือก ***Custom scan*** ดังรูปที่ (7)

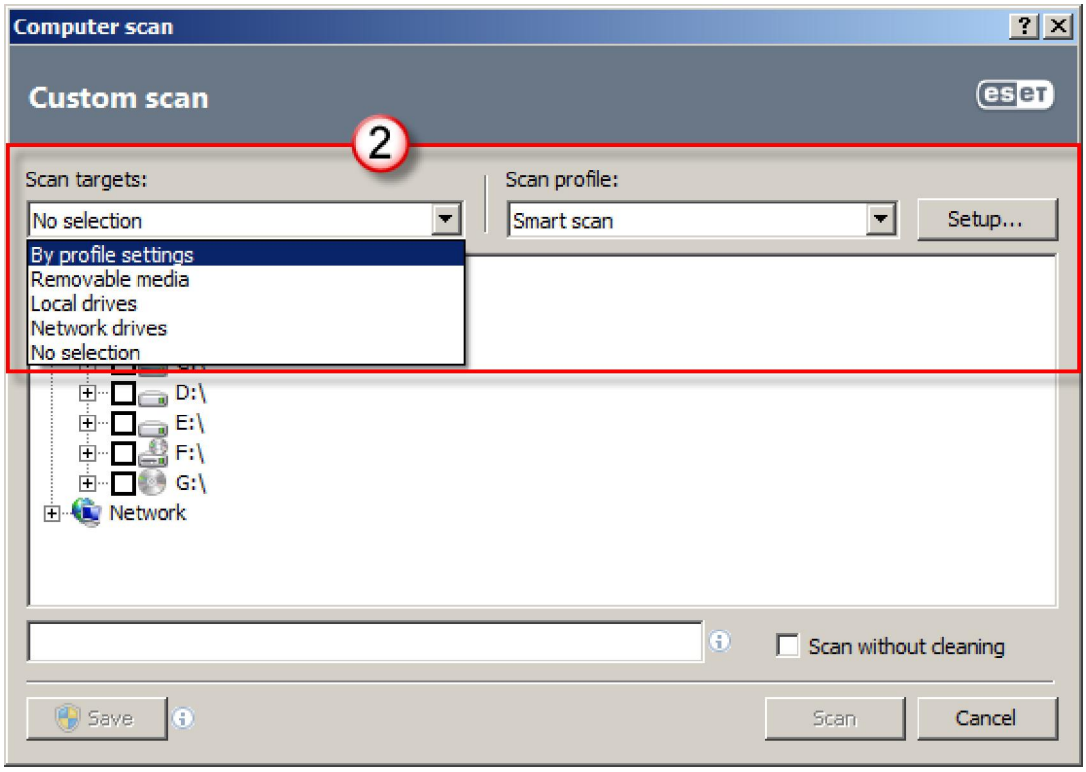


รูปที่ (7)

2.2 หลังจากคลิกปุ่ม Custom scan แล้วจะแสดงหน้าต่างเพื่อให้เลือกเป้าหมายในการในช่อง “Scan targets” และเลือก Profile ที่จะใช้ในการสแกนในช่อง “Scan profile” ดังรูปที่ (8)

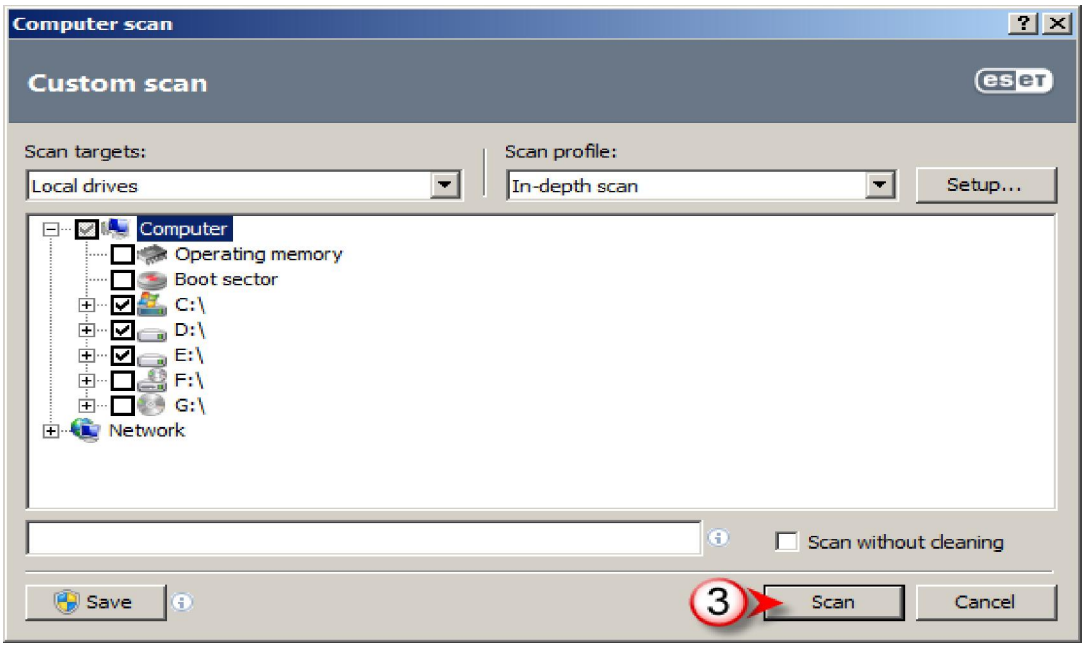
หน้าต่างเป้าหมายการสแกนช่วยให้สามารถกำหนดว่าจะสแกนการแฝงตัวของสิ่งใด (หน่วยความจำ ไดรฟ์ เซคเตอร์ ไฟล์ และโฟลเดอร์) ผู้ใช้สามารถเลือกเป้าหมายการสแกนที่กำหนดไว้ล่วงหน้าจากเมนู

- By profile setting – เลือกเป้าหมายที่กำหนดในโปรไฟล์การสแกนที่ได้เลือกไว้
- Removable media – เลือกดิสเก็ตต์,อุปกรณ์เก็บข้อมูล, USB ,ซีดี/ดีวีดี
- Local drives - เลือกฮารด์ไดรฟ์ของระบบทั้งหมด
- Network drives – เลือกไดรฟ์เครือข่ายที่แมปทั้งหมด
- No selection – ยกเลิกการเลือกทั้งหมด



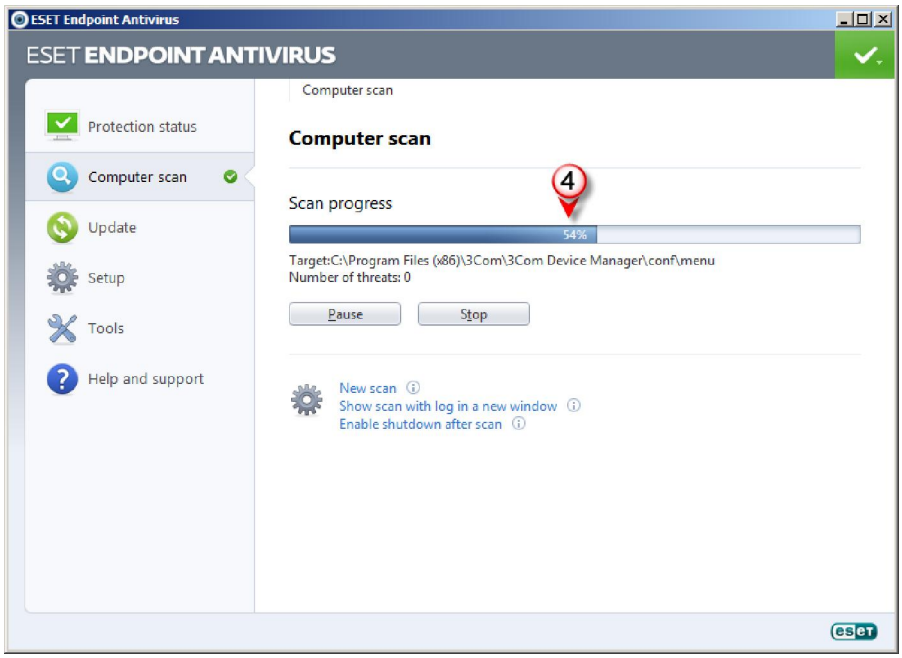
รูปที่ (8)

2.3 เมื่อเลือกเป้าหมายและ Profile ในการสแกนเรียบร้อยแล้ว ให้คลิกปุ่ม Scan ดังรูปที่ (9)



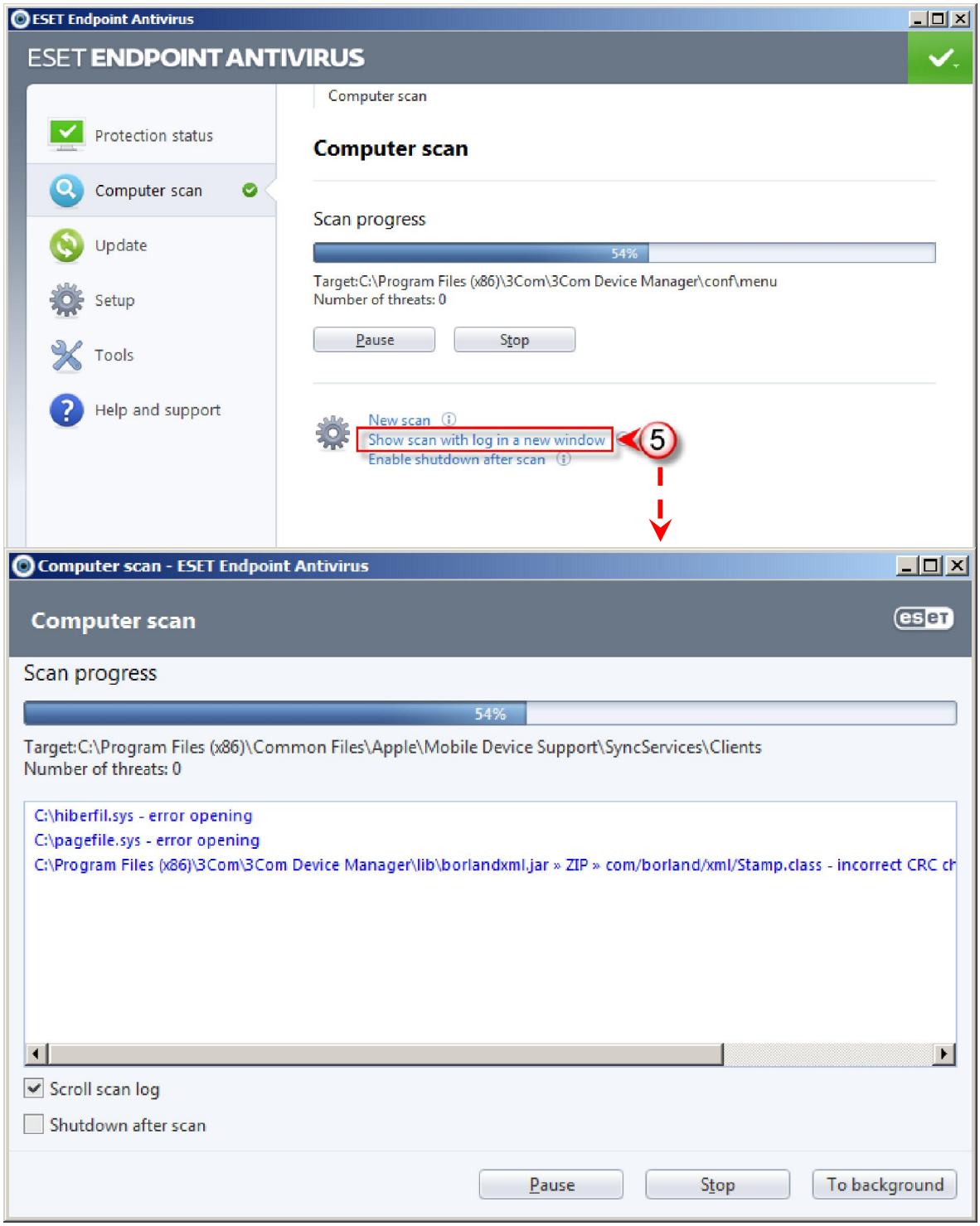
รูปที่ (9)

2.4 หลังจากคลิกปุ่ม Scan แล้ว จะเห็นการดำเนินการสแกนหาไวรัสและสปายแวร์ ดังรูปที่ (10)



รูปที่ (10)

2.5 สามารถคลิกที่ “Show scan with log in a new windows” เพื่อแสดงหน้าต่างความคืบหน้าของการสแกนไฟล์ ดังรูปที่ (11)



รูปที่ (11)

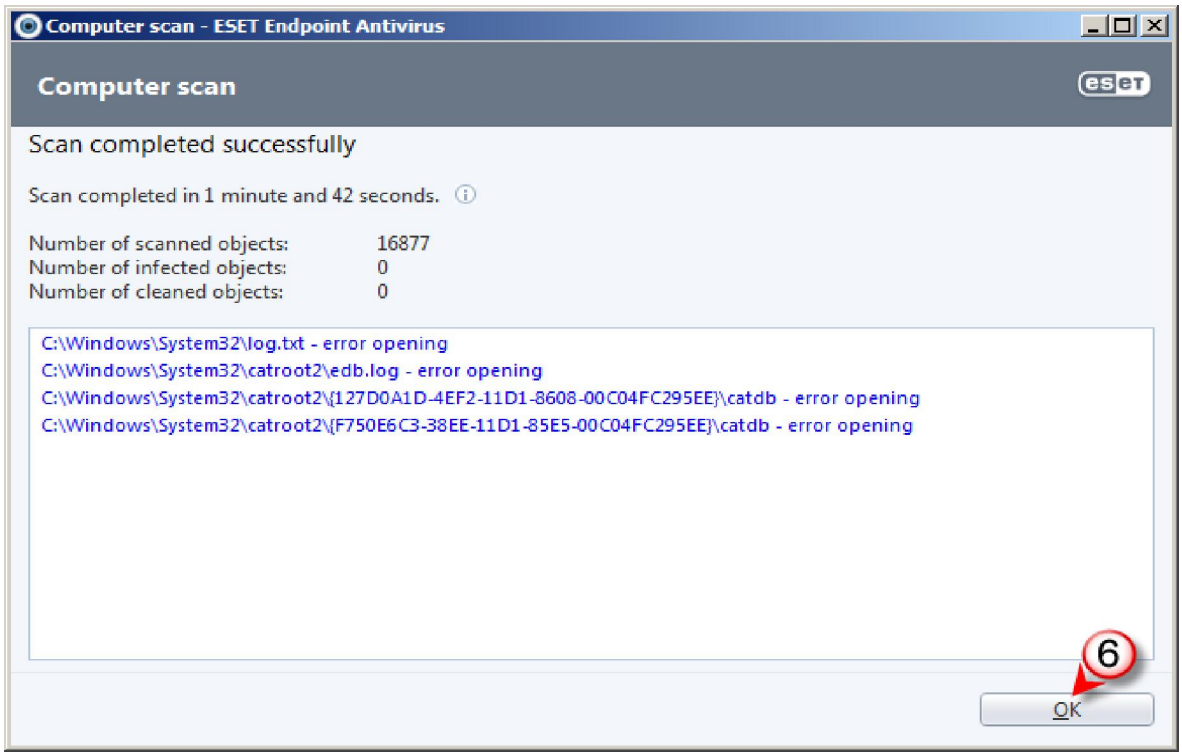
หมายเหตุ: เป็นเรื่องปกติที่โปรแกรมไม่สามารถสแกนบางไฟล์ได้ เช่น ไฟล์ที่ป้องกันด้วยรหัสผ่านหรือไฟล์ที่ระบบใช้งานโดยเฉพาะ (โดยทั่วไปคือ pagefile.sys และไฟล์บันทึก)

- ❖ Scan progress – แถบความคืบหน้าจะแสดงเปอร์เซ็นต์ของไฟล์ที่สแกนเสร็จแล้ว เปรียบเทียบกับไฟล์ที่รอการสแกนอยู่ ค่าจะได้มาจากจำนวนไฟล์ทั้งหมดที่สแกน
- ❖ Target – ชื่อของไฟล์ที่สแกนในปัจจุบันและตำแหน่งของไฟล์
- ❖ Number of threats – แสดงจำนวนภัยคุกคามโดยรวมที่พบในระหว่างการสแกน
- ❖ Pause - หยุดการสแกนชั่วคราว
- ❖ Stop – สิ้นสุดการสแกน
- ❖ To background - สามารถเรียกใช้การสแกนอื่นๆ โดยการสแกนที่ทำงานอยู่ก็จะยังดำเนินการอยู่

2.6 เมื่อโปรแกรมทำการสแกนเสร็จเรียบร้อยแล้ว ให้คลิกปุ่ม OK เพื่อออกจากหน้าต่างการสแกน ดังรูปที่ (12)

ในหน้าต่างนี้จะแสดงผลการสแกนดังนี้

- Number of scanned objects : หมายถึงจำนวนไฟล์ที่ถูกสแกนทั้งหมด
- Number of infected objects : หมายถึงจำนวนภัยคุกคามที่ตรวจพบ
- Number of cleaned objects : หมายถึงจำนวนภัยคุกคามที่ถูกกำจัดแล้ว



รูปที่ (12)

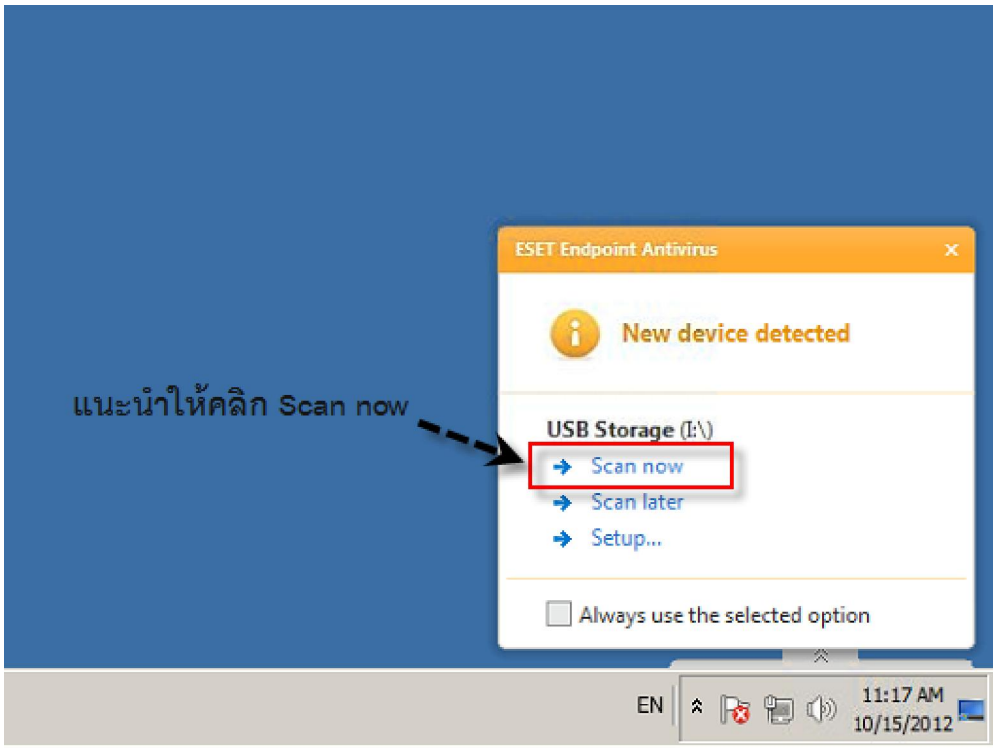
การสแกนไวรัสใน External drive หรือ USB drive

1. การสแกน External drive หรือ USB drive จากหน้าต่างการแจ้งเตือน

1.1 ทำการเชื่อมต่อ External drive หรือ USB drive เข้ากับเครื่องคอมพิวเตอร์

1.2 จะมีหน้าต่างแจ้งเตือนขึ้นมาที่มุมล่างขวามือ ท่านสามารถเลือกว่าจะทำการสแกน External drive หรือ USB drive หรือไม่ ดังรูปที่ (13)

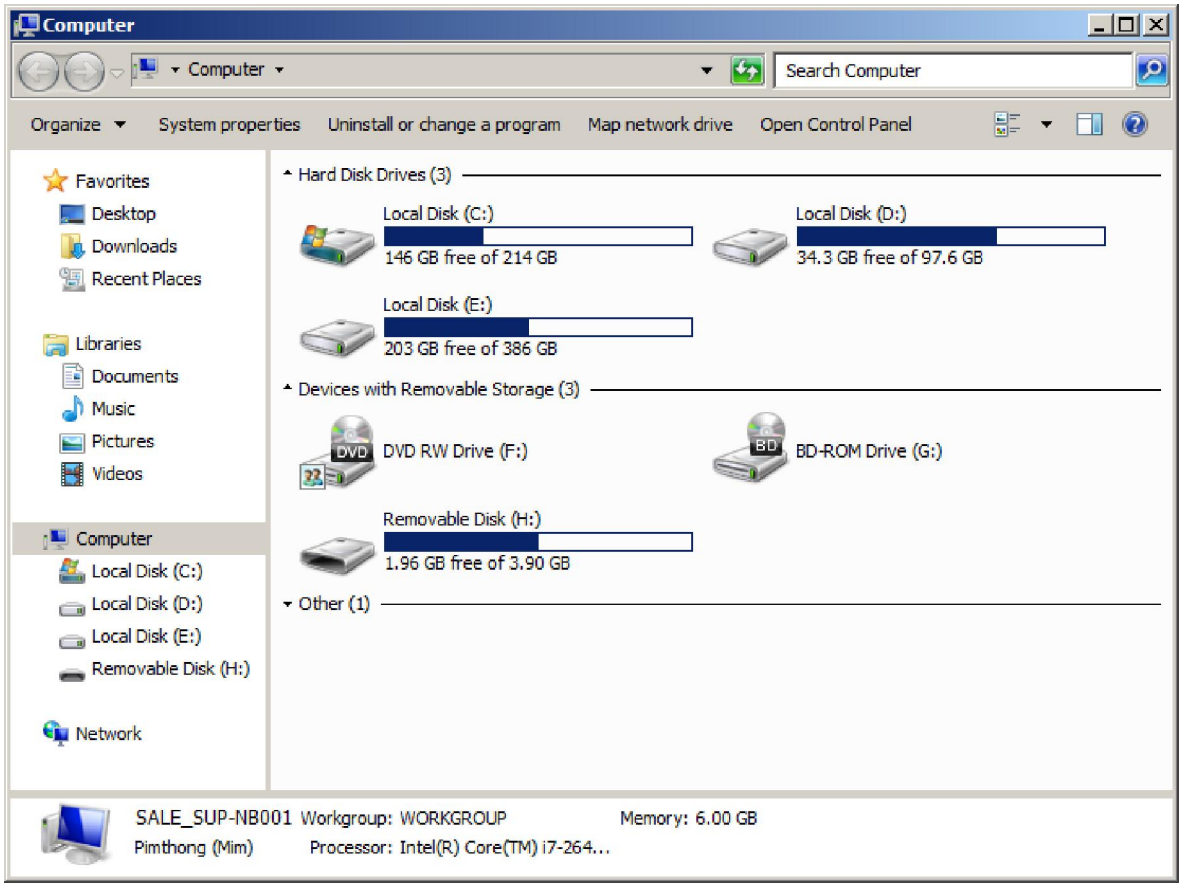
- ❖ Scan now - โปรแกรมจะทำการสแกน USB หรือ Flash drive ให้ท่านทันที
- ❖ Scan later - โปรแกรมจะไม่ทำการสแกน USB หรือ Flash drive
- ❖ Setup... - เข้าสู่หน้าต่างการตั้งค่า



รูปที่ (13)

2. การสแกน USB หรือ Flash drive โดยการคลิกขวา

2.1 ทำการเชื่อมต่อ External drive หรือ USB drive เข้ากับเครื่องคอมพิวเตอร์
2.2 เปิด My Computer ขึ้นมาดังรูปที่ (14)

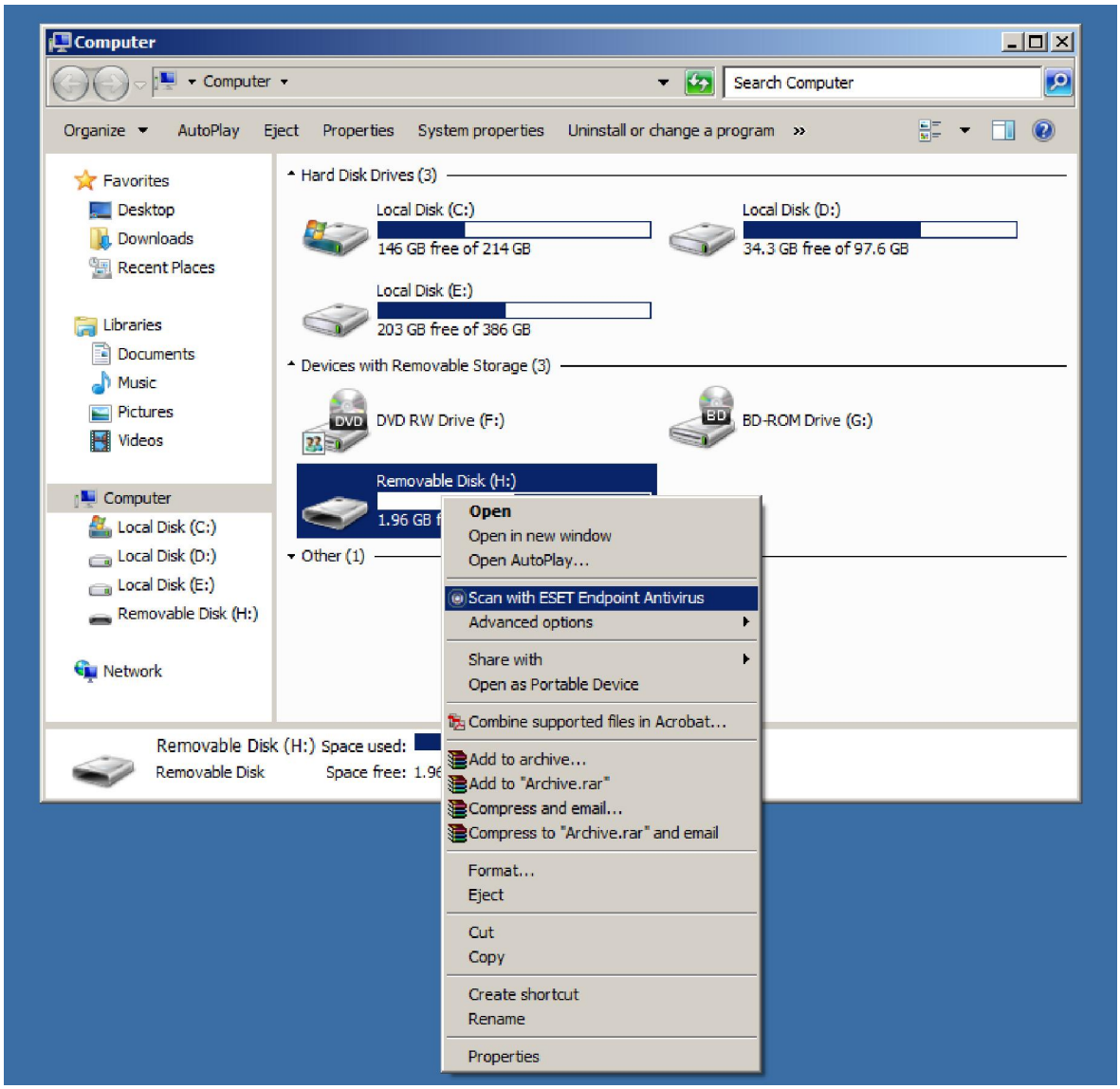


รูปที่ (14)

2.3 จากนั้นให้คลิกขวาบน External drive หรือ USB drive ที่ต้องการสแกน เช่น ไดร์ฟ (H:)

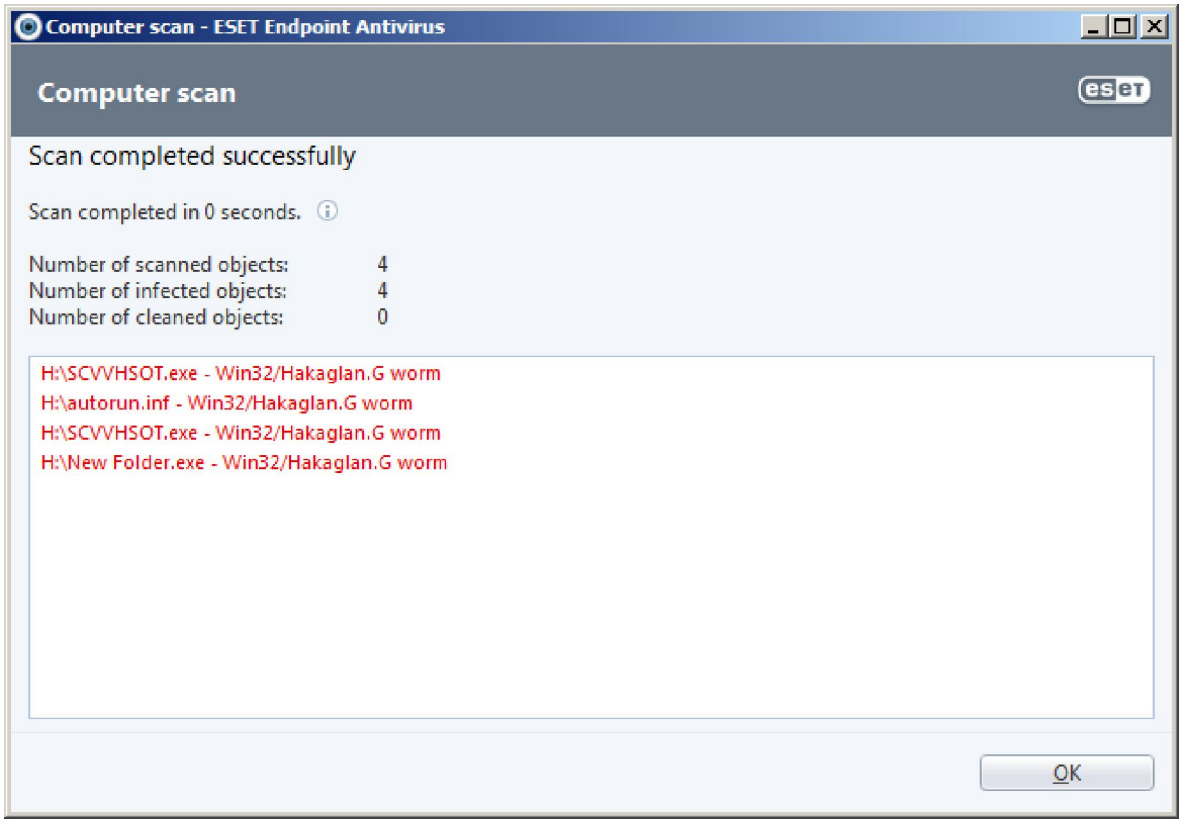
วิธีการสแกนมี 2 แบบ ดังนี้ :

<u>แบบที่ 1.</u> เลือก “Scan with ESET Endpoint Antivirus” เพื่อต้องการสแกนหาไวรัสใน External drive หรือ USB drive เท่านั้น โดยที่โปรแกรมป้องกันไวรัส ESET Endpoint Antivirus จะทำการสแกนตรวจหาไวรัสอย่างเดียวจะไม่ทำการกำจัดไวรัสให้อัตโนมัติ ดังรูปที่ (15)



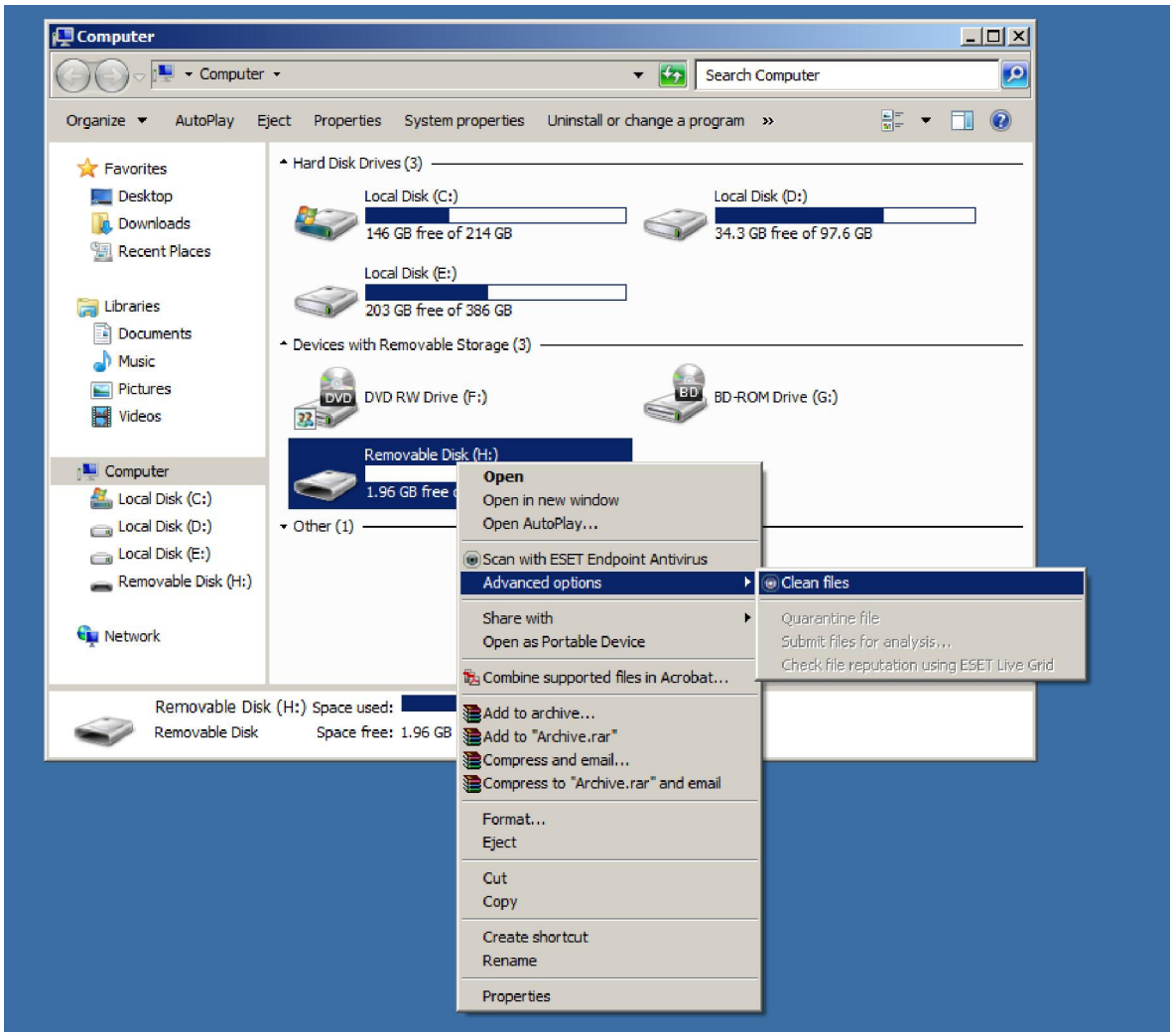
รูปที่ (15)

จากรูปที่ (16) หลังจากทำการสแกนแล้วจะพบว่าใน External drive หรือ USB drive ของท่านมีไวรัสอยู่ ซึ่งจะแสดงเป็นข้อความสีแดง แต่โปรแกรมยังไม่ได้ทำการกำจัดไวรัสให้



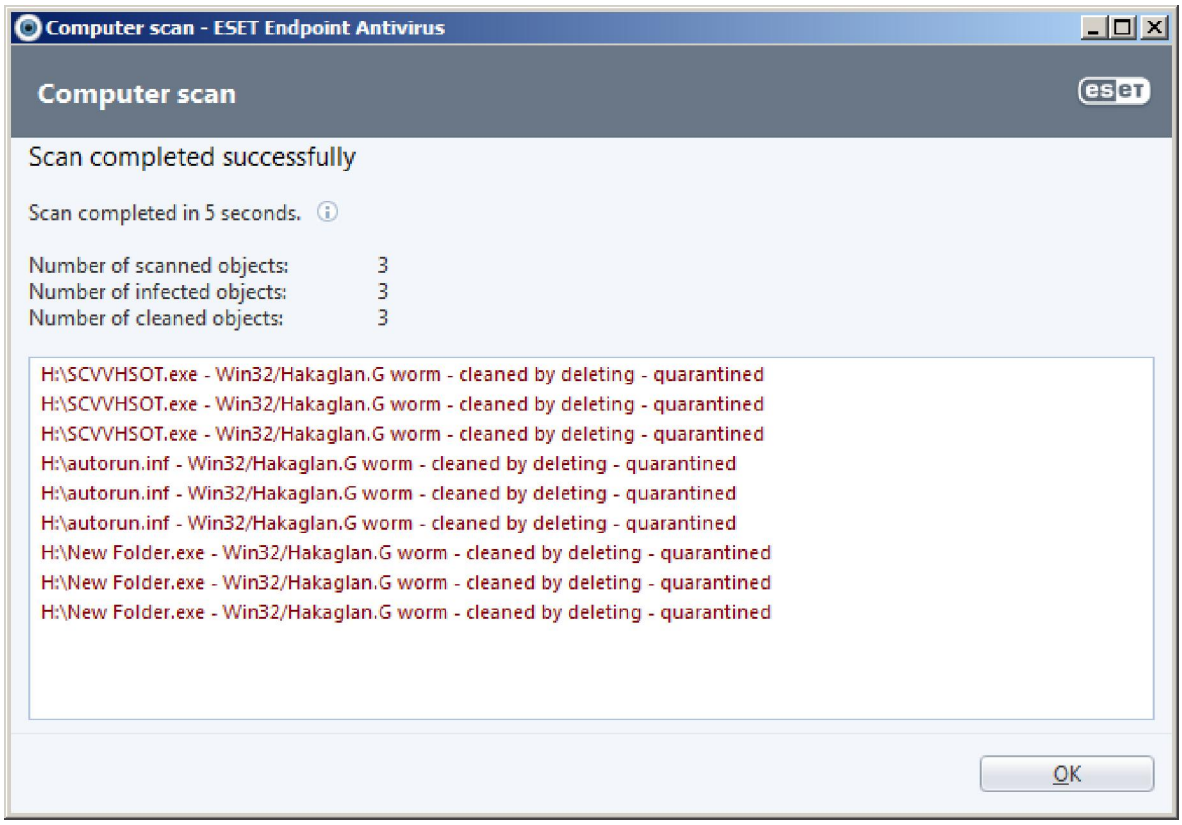
รูปที่ (16)

<u>แบบที่ 2.</u> เลือก “Advanced option -> Clean files” เพื่อต้องการสแกนหาไวรัสใน External drive หรือ USB drive โดยที่โปรแกรมป้องกันไวรัส ESET Endpoint Antivirus จะทำการกำจัดไวรัสให้อัตโนมัติ ดังรูปที่ (17)



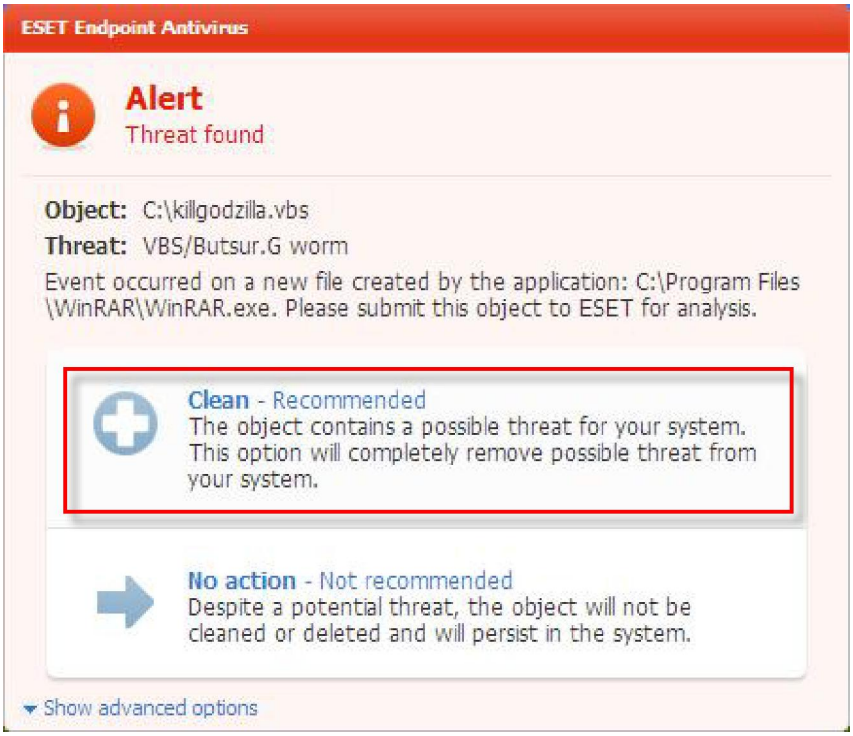
รูปที่ (17)

จากรูปที่ (18) หลังจากทำการสแกนแล้วจะพบว่าใน External drive หรือ USB drive ของท่านมีไวรัสอยู่ โปรแกรมป้องกันไวรัส ESET Endpoint Antivirus จะทำการกำจัดไวรัสให้อัตโนมัติ



รูปที่ (18)

ในระหว่างสแกน หากโปรแกรมป้องกันไวรัส ESET Endpoint Antivirus ตรวจพบไวรัสต่างๆ อาจจะขึ้นหน้าต่างดังรูปที่ (19) ให้ท่านทำการตรวจสอบชื่อไฟล์ที่ถูกตรวจพบว่าเป็นไฟล์งานหรือไฟล์โปรแกรมที่สำคัญของท่านหรือไม่ หากไม่ใช่ไฟล์งานหรือไฟล์โปรแกรมที่สำคัญของท่าน ขอแนะนำให้ทำการลบไฟล์ทิ้ง โดยการคลิกที่ปุ่ม “Clean”



รูปที่ (19)

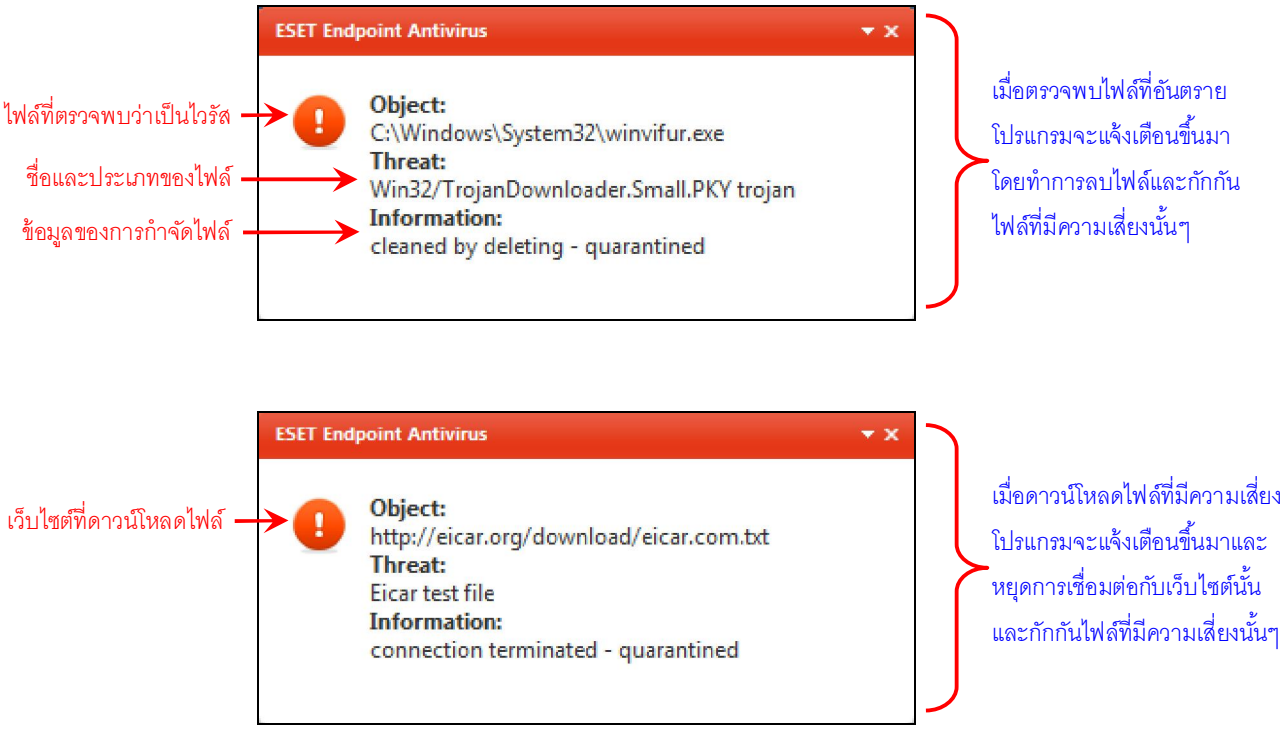
การตรวจพบการแฝงตัว

การบุกรุกจากภัยคุกคามสามารถเข้าสู่ระบบได้จากจุดที่เข้าใช้งานต่างๆ เช่น หน้าเว็บ, โฟลเดอร์ที่ใช้ร่วมกัน, ผ่านอีเมล หรือจากอุปกรณ์ที่ถอดเข้าออกได้ (USB, ดิสก์ภายนอก, ซีดี, ดีวีดี, ดิสเก็ตต์ เป็นต้น)

สำหรับตัวอย่างทั่วไปที่ ESET Endpoint Antivirus จัดการกับการบุกรุก และระบบจะตรวจพบการบุกรุกโดยใช้

- การป้องกันระบบไฟล์แบบเรียลไทม์
- การป้องกันการเข้าถึงเว็บ
- การป้องกันอีเมลไคลเอ็นต์
- การสแกนคอมพิวเตอร์ตามต้องการ

หน้าต่างการแจ้งเตือนจะปรากฏขึ้นในพื้นที่การแจ้งเตือนในมุมขวาล่างของหน้าจอ ดังรูปที่ (20)



รูปที่ (20)

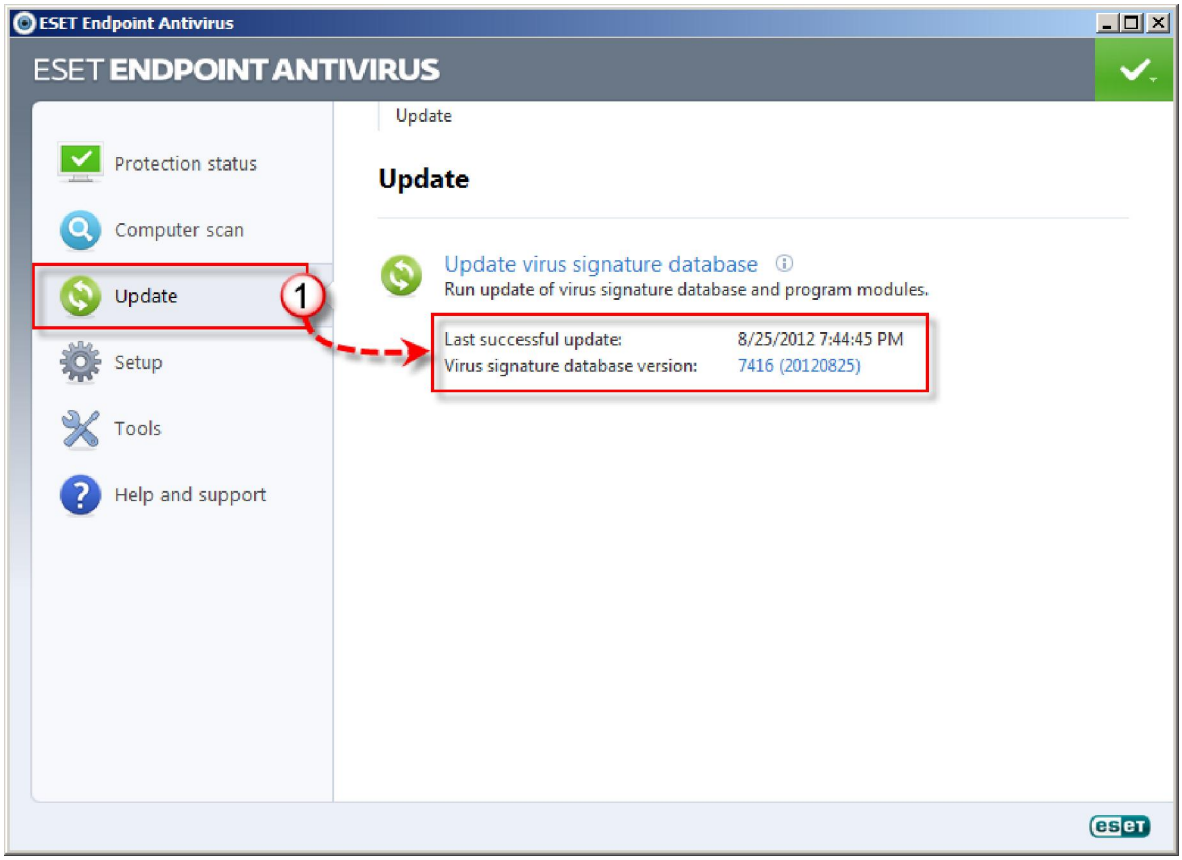
หมายเหตุ : ค่าที่โปรแกรมกำหนดเป็นค่า Default เมื่อตรวจพบไวรัสและสปายแวร์ จะดำเนินการทำความสะอาดไฟล์ (Clean) แต่ถ้า Clean ไม่สำเร็จจะทำการลบ (Delete) ไฟล์ที่ติดไวรัสทิ้ง และทำการกักกันไฟล์ไว้ (Quarantine) ซึ่งผู้ใช้สามารถทำการกู้ไฟล์คืนได้

3. Update (การอัพเดทโปรแกรม)

3.1 การอัพเดท ESET Endpoint Antivirus เป็นประจำเป็นวิธีการที่ดีที่สุดเพื่อให้คอมพิวเตอร์มีระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะทำให้มั่นใจว่าโปรแกรมนั้น มีความทันสมัยอยู่เสมอโดยใช้สองวิธี คือ โดยการอัพเดทฐานข้อมูลไวรัส และการอัพเดทองค์ประกอบของโปรแกรม

เมื่อคลิกอัพเดทในหน้าต่างโปรแกรมหลัก จะพบสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และแสดงว่าจะต้องมีการอัพเดทหรือไม่
หน้าต่างหลักจะมีเวอร์ชั่นของฐานข้อมูลไวรัส เมื่อคลิกตัวเลขนี้จะลิงค์ไปยังเว็บไซต์ของ ESET ซึ่งจะแสดงฐานข้อมูลทั้งหมดที่เพิ่มขึ้นมา

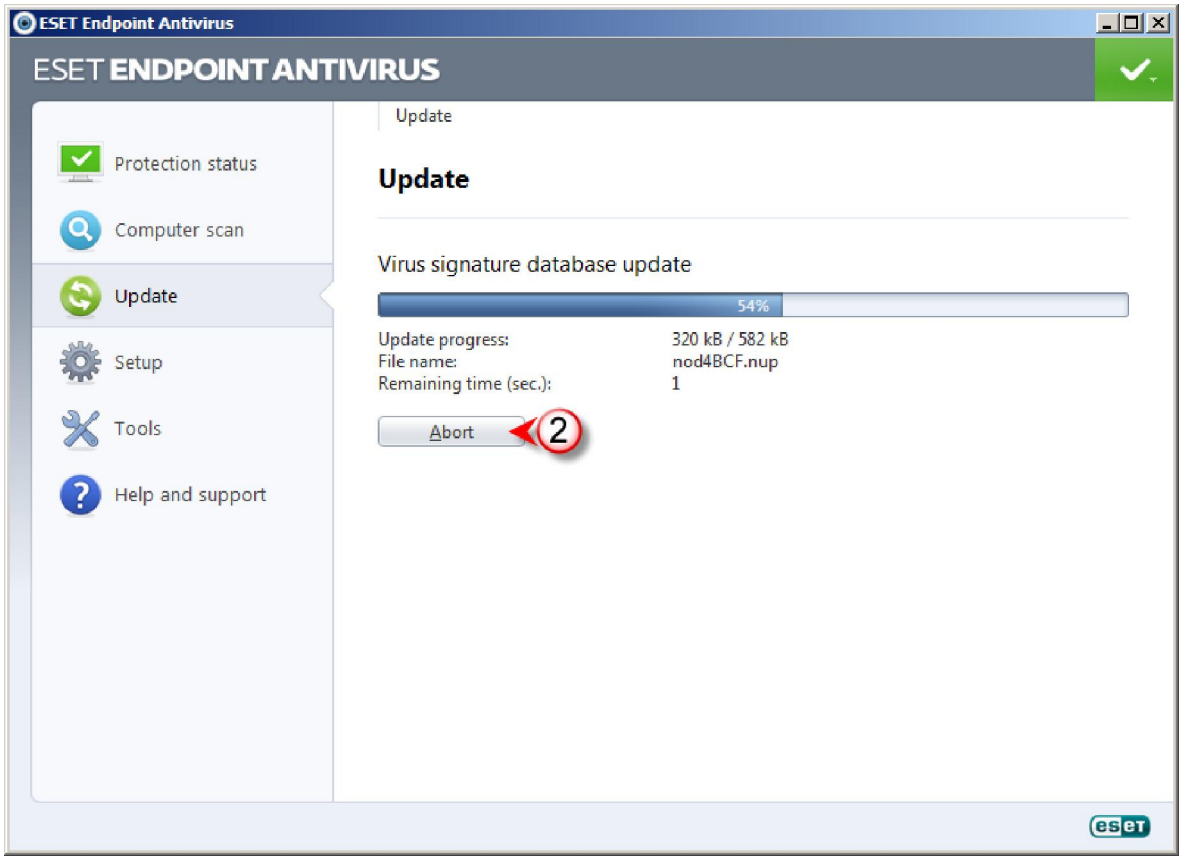
- ❖ Last successful update – วันที่ล่าสุดที่อัพเดทฐานข้อมูล
- ❖ Version signature database version - หมายเลขฐานข้อมูลไวรัสที่อัพเดตไว้ล่าสุด ซึ่งเมื่อคลิกจะลิงค์ไปยังเว็บไซต์ของ ESET เพื่อดูรายการของฐานข้อมูลที่เพิ่มขึ้นมา



รูปที่ (21)

3.2 กระบวนการอัพเดท

หลังจากคลิก “Update virus signature database” กระบวนการดาวน์โหลดจะเริ่มต้นทำงาน จะแสดงแถบความคืบหน้าการดาวน์โหลดและเวลาที่เหลือสำหรับการดาวน์โหลดจะปรากฏขึ้น หากต้องการยกเลิกการอัพเดทให้คลิก “Abort” ดังรูปที่ (22)



รูปที่ (22)

4. Setup (การตั้งค่า)

เมนู Setup มีตัวเลือกดังต่อไปนี้ :

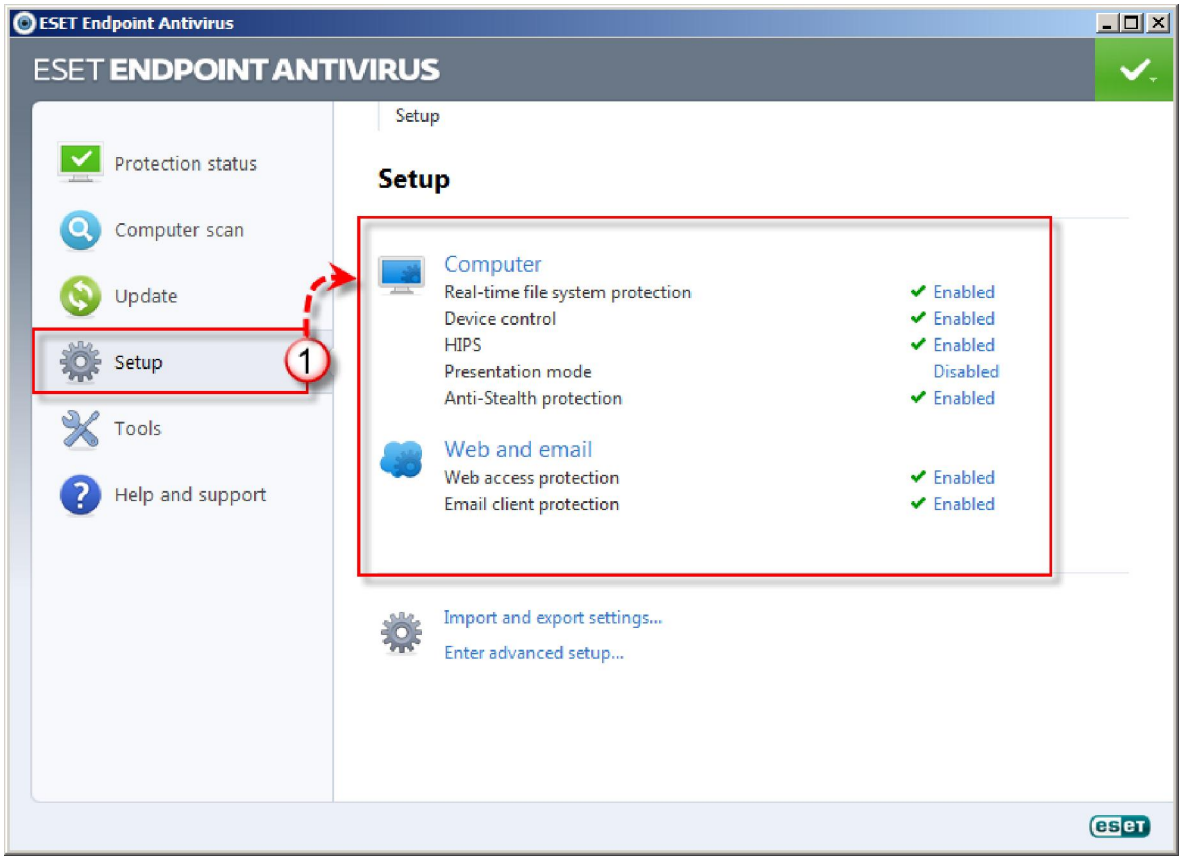
- ❖ Computer
- ❖ Web and email

การตั้งค่าการป้องกัน Computer จะช่วยให้สามารถเปิดหรือปิดการใช้งานต่อไปนี้ :

- ❖ Real-time file system protection - การป้องกันระบบไฟล์แบบเรียลไทม์
- ❖ Device control - การควบคุมอุปกรณ์
- ❖ HIPS - ระบบป้องกันการบุกรุกที่ใช้โฮสต์
- ❖ Presentation mode – โหมดการนำเสนอ (เมื่อใช้งานโปรแกรมอื่นแบบ Full Screen)
- ❖ Anti-Stealth protection – ระบบป้องกันไวรัสประเภทรูทคิทส์

การตั้งค่าการป้องกัน Web and email จะช่วยให้สามารถเปิดหรือปิดใช้งานต่อไปนี้ :

- ❖ Web access protection – ระบบสแกนการรับส่งข้อมูลทั้งหมดผ่าน HTTP หรือ HTTPS
- ❖ Email client protection – การควบคุมการสื่อสารทางอีเมลที่ได้รับผ่านโปรโตคอล POP3 และ IMAP

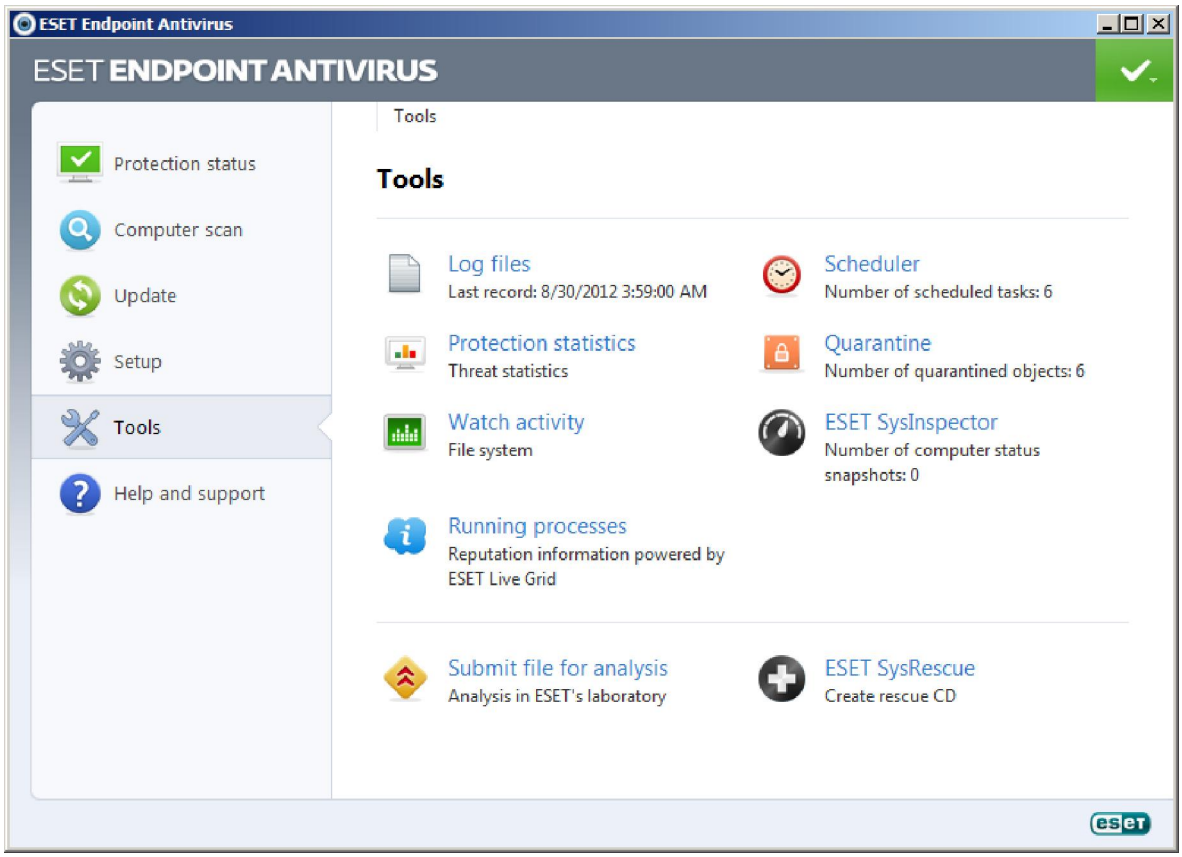


รูปที่ (23)

5. Tools (เครื่องมือ)

เมนูเครื่องมือ ประกอบด้วยโมดูลที่ช่วยให้การจัดการโปรแกรมง่ายขึ้นและมีตัวเลือกเพิ่มเติมสำหรับผู้ใช้ขั้นสูง เมนูนี้จะมีเครื่องมือต่อไปนี้ : ดังรูปที่ (24)

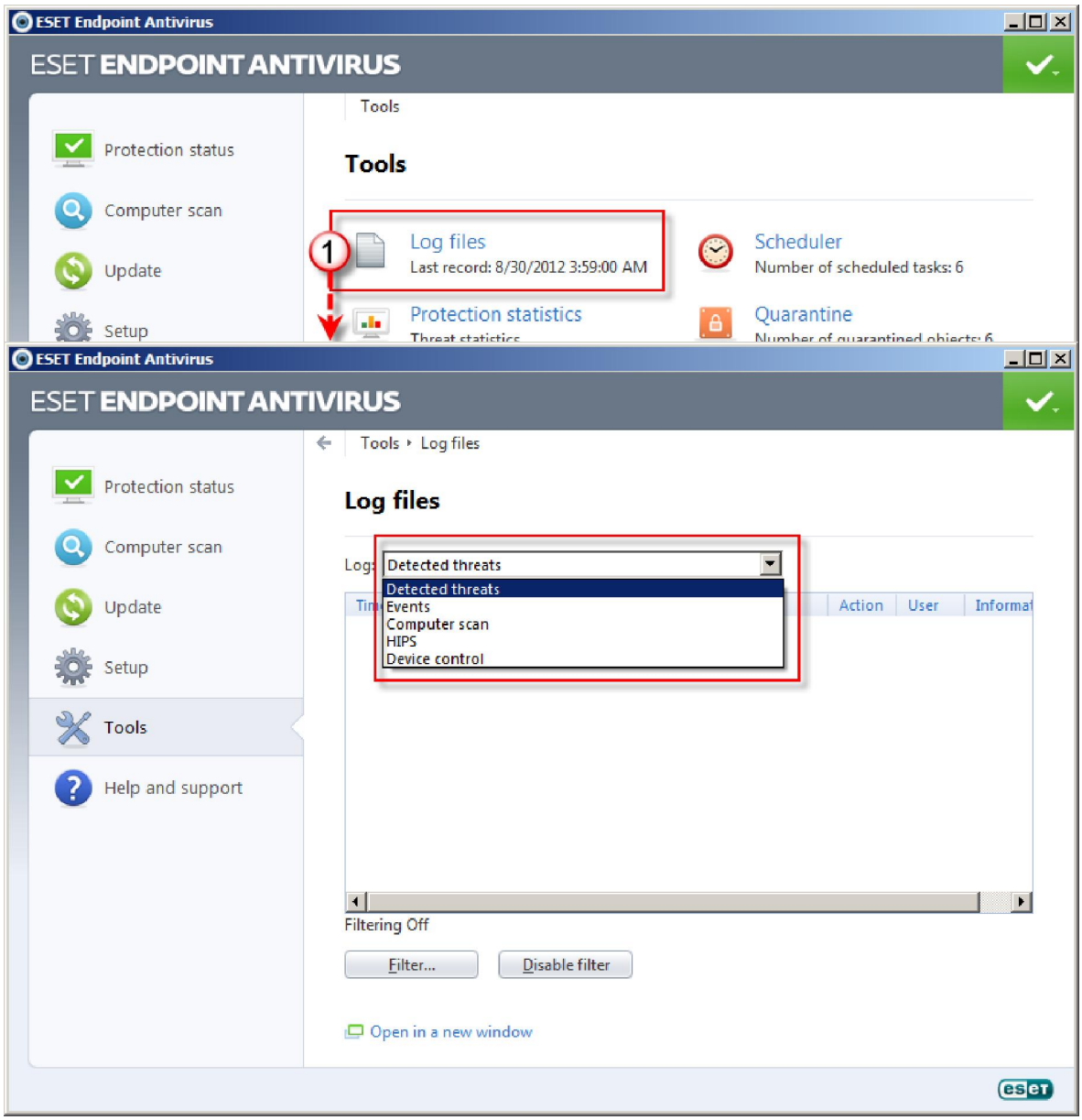
- ❖ Log files
- ❖ Protection statistics
- ❖ Watch activity
- ❖ Running processes
- ❖ Scheduler
- ❖ Quarantine
- ❖ ESET SysInspector
- ❖ Submit file for analysis
- ❖ ESET SysRescue



รูปที่ (24)

5.1 Log files: การเก็บข้อมูลเหตุการณ์ การทำงานต่างๆ ของโปรแกรม

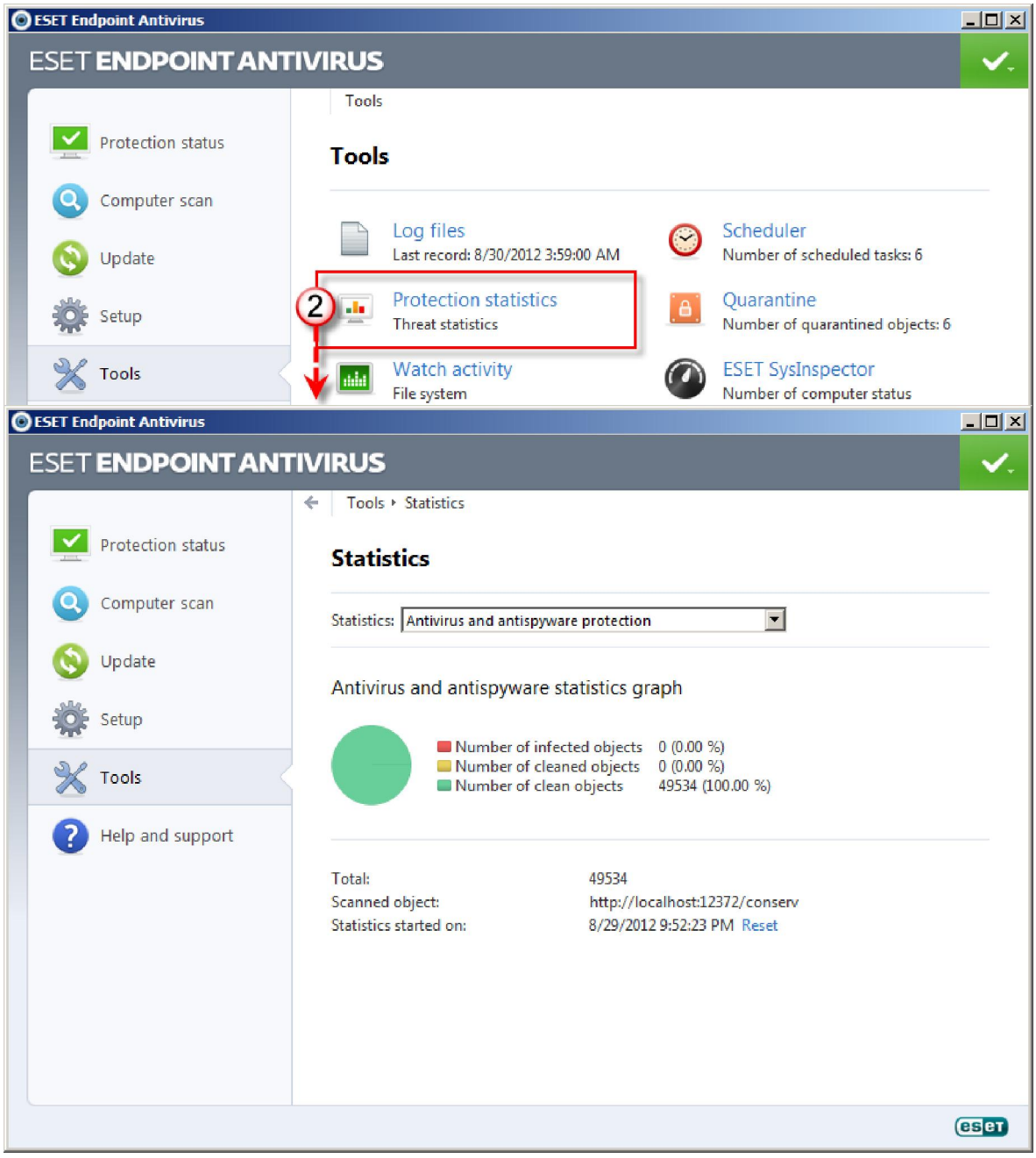
ไฟล์บันทึกประกอบด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมที่สำคัญที่เกิดขึ้นทั้งหมด และให้ภาพรวมของภัยคุกคามที่พบ Log files เป็นเครื่องมือที่จำเป็นในการวิเคราะห์ระบบ การตรวจหาภัยคุกคาม และการแก้ไขปัญหา ท่านสามารถตรวจสอบเหตุการณ์ต่างๆ ที่เกิดขึ้นได้ เช่น การตรวจจับไฟล์ (Detected threats), เหตุการณ์ต่างๆ (Events), การสแกนคอมพิวเตอร์ (Computer scan), HIPS และ การควบคุมอุปกรณ์ (Device Control) ดังรูปที่ (25)



รูปที่ (25)

5.2 Protection statistics: สถิติการป้องกัน ดังรูปที่ (26)

- ❖ Antivirus and antispyware – แสดงจำนวนวัตถุที่ติดไวรัสและถูกกำจัด
- ❖ File system protection – แสดงเฉพาะวัตถุที่มีการอ่านและเขียนไปยังระบบไฟล์เท่านั้น
- ❖ Email client protection – แสดงเฉพาะวัตถุที่รับหรือส่งด้วยอีเมลไคลเอ็นต์เท่านั้น
- ❖ Web access protection – แสดงเฉพาะวัตถุที่ดาวน์โหลดโดยเว็บเบราว์เซอร์เท่านั้น



รูปที่ (26)