ESET NOD32 Antivirus 4

Business Edition สำหรับ Mac OS X

คู่มือการติดตั้งและคู่มือผู้ใช้

คลิกที่นี่เพื่อดาวน์โหลดเอกสารรุ่นใหม่ล่าสุด http://download.eset.com/manuals/eset_eavbe_mac_4_userguide_tha.pdf

ESET NOD32 Antivirus 4

Copyright ©2011 by ESET, spol. s r.o.

ESET NOD32 Antivirus ได้รับการพัฒนาโดย ESET, spol. s r.o.

สำหรับข้อมูลเพิ่มเติม โปรดไปที่ www.eset.co.th

สงวนลิขสิทธิ์ ห้ามนำส่วนหนึ่งส่วนใดของเอกสารนี้ไปทำซ้ำ เก็บไว้ในระบบที่เรียกคืนได้ หรือส่งในรูปแบบหรือวิธีการใดๆ กลไกทางอิเล็กทรอนิกส์ การถ่ายสำเนา การบันทึก การสแกน หรือโดยไม่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษรจากผู้เขียน

ESET, spol. s r.o. ขอสงวนลิขสิทธิ์ในการเปลี่ยนแปลงซอฟต์แวร์แอพพลิเคชันที่อธิบายไว้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

การดูแลลูกค้า: www.eset.co.th/support

แก้ไข 2011

สารบัญ

ESET NOD32 Antivirus 6

ความต้องการของระบบ 6

การติดตั้ง 6

การติดตั้งปกติ 7

การติดตั้งแบบกำหนดเอง 8

การติดตั้งระยะไกล 8

การสร้างแพคเกจการติดตั้งระยะไกล 8

การติดตั้งระยะไกลในคอมพิวเตอร์เป้าหมาย 10

การถอนการติดตั้งระยะไกล 10

การอัพเกรดระยะไกล 10

การป้อนชื่อผู้ใช้และรหัสผ่าน 10

การสแกนคอมพิวเตอร์ตามต้องการ 10

คู่มือระดับเริ่มต้น 10

ส่วนติดต่อผู้ใช้ 10

การตรวจสอบการทำงานของระบบ 12

ควรทำอย่างไรเมื่อโปรแกรมทำงานไม่ถูกต้อง 13

ทำงานกับ ESET NOD32 Antivirus 13

การป้องกันไวรัสและสปายแวร์ 13

การป้องกันระบบไฟล์แบบเรียลไทม์ 13

การสแกนคอมพิวเตอร์ตามต้องการ 16

การตั้งค่าพารามิเตอร์กลไก ThreatSense 19

ตรวจพบการแฝงตัว 21

การอัพเดทโปรแกรม 22

การอัพเกรดเป็นรุ่นใหม่ 23

การตั้งค่าการอัพเดท 23

วิธีสร้างงานการอัพเดท 24

เครื่องมือวางกำหนดการ **24**

วัตถุประสงค์ของการวางกำหนดการงาน 25

การสร้างงานใหม่ 25

กักเก็บ **26**

การกักเก็บไฟล์ 27

การเรียกคืนจากการกักเก็บ 27

การส่งไฟล์จากการกักเก็บ 27

ไฟล์บันทึก **27**

การบำรุงรักษาการบันทึก 27

การกรองบันทึก 28

ส่วนติดต่อผู้ใช้ **28**

การเตือนและการแจ้งเตือน 28

สิทธิ์ 29

เมนูบริบท 30

ThreatSense.Net **30**

ไฟล์ที่น่าสงสัย 31

ผู้ใช้ขั้นสูง **31**

การตั้งค่าการนำเข้าและส่งออก **31**

การตั้งค่าการนำเข้า 32

การตั้งค่าการส่งออก 32

การตั้งค่าพร็อกซีเซิร์ฟเวอร์ **32**

การปิดกั้นสื่อที่ถอดเข้าออกได้ **33**

การดูแลระบบระยะไกล **33**

ประมวลศัพท์ **34**

ประเภทของการแฝงตัว **34**

ไวรัส 34

เวิร์ม 34

ม้าโทรจัน 35

แอดแวร์ 35

สปายแวร์ 35

แอพพลิเคชันที่อาจไม่ปลอดภัย 36

แอพพลิเคชันที่อาจไม่พึงประสงค์ 36

ESET NOD32 Antivirus

เนื่องจากจำนวนของระบบปฏิบัติการที่ใช้ Unix เพิ่มมากขึ้น ผู้เขียนมัลแวร์จึงได้พยายามพัฒนาภัยคุกคามมากขึ้นไปยังผู้ใช้ Mac เป้าหมาย ESET NOD32 Antivirus มีการป้องกันที่มีประสิทธิภาพและประสิทธิผลต่อภัยคุกคามที่เกิดขึ้นเหล่านี้ ESET NOD32 Antivirus ยังมีความสามารถในการตรวจหาภัยคุกคามของ Windows ซึ่งจะช่วยคุ้มครองผู้ใช้ Mac เมื่อทำงานร่วมกับผู้ใช้ Windows และในทางกลับกัน แม้ว่ามัลแวร์ของ Windows จะไม่ถือว่าเป็นภัยคุกคามโดยตรงต่อ Mac การปิดใช้งานมัลแวร์ที่มีผลต่อเครื่อง Mac จะช่วยป้องกันการแพร่กระจายไปยังคอมพิวเตอร์ที่ใช้ Windows ผ่านเครือข่ายภายในระบบหรืออินเทอร์เน็ต

ความต้องการของระบบ

เพื่อให้ ESET NOD32 Antivirus มีประสิทธิภาพสูงสุด ระบบของคุณควรตรงตามข้อกำหนดด้านฮาร์ดแวร์และซอฟต์แวร์ต่อไปนี้:

ESET NOD32 Antivirus:

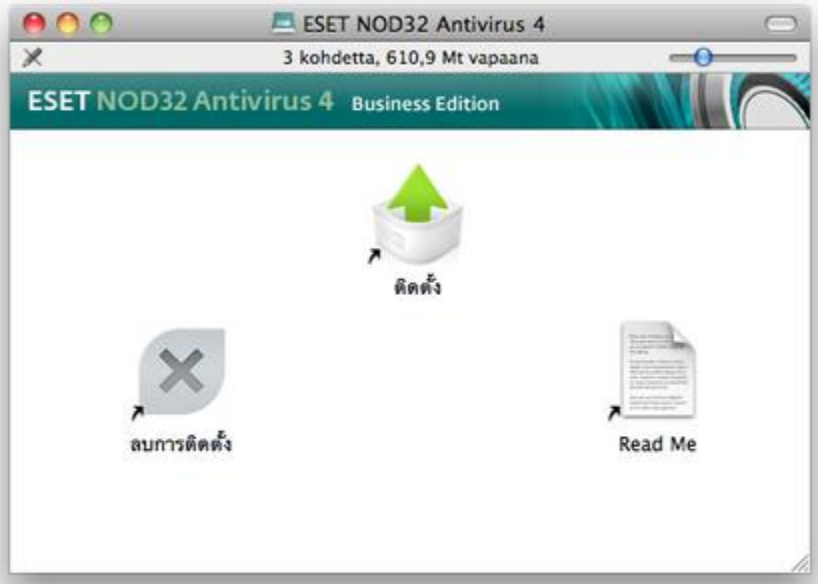
	ความต้องการของระบบ
สถาปัตยกรรมของตัวประมวลผล	Intel® 32 บิต, 64 บิต
ระบบปฏิบัติการ	Mac OS X 10.5 ขึ้นไป
หน่วยความจำ	512 เมกะไบต์
พื้นที่ว่างในดิสก์	100 เมกะไบต์

การติดตั้ง

ก่อนที่คุณจะเริ่มต้นกระบวนการติดตั้ง โปรดปิดโปรแกรมที่เปิดไว้ทั้งหมดในคอมพิวเตอร์ ESET NOD32 Antivirus มีองค์ประกอบที่อาจขัดแย้งกับโปรแกรมป้องกันไวรัสอื่นๆ ที่อาจมีการติดตั้งไว้ในคอมพิวเตอร์ของคุณแล้ว ESET ขอแนะนำให้คุณลบโปรแกรมป้องกันไวรัสอื่นๆ ออกเพื่อป้องกันปัญหาที่อาจเกิดขึ้น คุณสามารถติดตั้ง ESET NOD32 Antivirus จากซีดีการติดตั้งหรือจากไฟล์ที่มีให้บริการในเว็บไซต์ ESET

เมื่อต้องการเริ่มต้นวิซาร์ดการติดตั้ง ให้ดำเนินการอย่างใดอย่างหนึ่งต่อไปนี้:

- ถ้าคุณกำลังติดตั้งจากซีดีการติดตั้ง ให้ใส่ซีดีลงในไดรฟ์ CD-ROM คลิกสองครั้งที่ไอคอนการติดตั้งของ ESET NOD32 Antivirus เพื่อเริ่มต้นโปรแกรมติดตั้ง
- ถ้าคุณกำลังติดตั้งจากไฟล์ที่ดาวน์โหลดไว้ ให้คลิกสองครั้งที่ไฟล์ที่คุณดาวน์โหลดเพื่อเริ่มต้นโปรแกรมติดตั้ง



เริ่มต้นการติดตั้งโปรแกรม และวิซาร์ดการติดตั้งจะนำคุณเข้าสู่การตั้งค่าพื้นฐาน หลังจากยอมรับข้อตกลงการอนุญาตสำหรับผู้ใช้ปลายทาง

คุณสามารถเลือกประเภทการติดตั้งได้จากประเภทต่อไปนี้:

- การติดตั้งปกติ
- การติดตั้งแบบกำหนดเอง
- การติดตั้งระยะไกล

การติดตั้งปกติ

โหมดการติดตั้งปกติจะมีตัวเลือกการกำหนดค่าที่เหมาะสมสำหรับผู้ใช้งานส่วนใหญ่ การตั้งค่าเหล่านี้จะมีการรักษาความปลอดภัยสูงสุดรวมกับประสิทธิภาพการทำงานของระบบที่ยอดเยี่ยม การติดตั้งปกติเป็นตัวเลือกเริ่มต้นและแนะนำให้ใช้ถ้าคุณไม่มีความต้องการเป็นพิเศษสำหรับการตั้งค่าแบบเจาะจง

หลังจากเลือกโหมดการติดตั้ง **ปกติ (แนะนำ)** คุณจะได้รับพรอมต์ให้ป้อนชื่อผู้ใช้และรหัสผ่านเพื่อเปิดใช้งานการอัพเดทอัตโนมัติของโปรแกรม การดำเนินการนี้จะมีบทบาทสำคัญในการให้การป้องกันระบบของคุณที่แน่นอน ป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ของคุณ (ข้อมูลการตรวจสอบสิทธิ์ที่คุณได้รับหลังจากซื้อหรือลงทะเบียนผลิตภัณฑ์) ลงในฟิลด์ที่สอดคล้องกัน ถ้าคุณไม่มีชื่อผู้ใช้และรหัสผ่านที่ใช้ได้ คุณสามารถเลือกตัวเลือก **ตั้งค่าพารามิเตอร์การอัพเดทในภายหลัง** เพื่อดำเนินการติดตั้งต่อ

ระบบการเตือนล่วงหน้า ThreatSense.Net ช่วยให้แน่ใจได้ว่า ESET จะได้รับการแจ้งในทันทีและอย่างต่อเนื่องเกี่ยวกับการแฝงตัวใหม่เพื่อการป้องกันลูกค้าได้อย่างรวดเร็ว ระบบจะอนุญาตให้ส่งภัยคุกคามใหม่ไปยังแล็บภัยคุกคามของ ESET ซึ่งภัยคุกคามจะถูกวิเคราะห์ ประมวลผล และเพิ่มไปยังฐานข้อมูลไวรัส ตามค่าเริ่มต้น ตัวเลือก **เปิดใช้ระบบการเตือนล่วงหน้า ThreatSense.Net** จะถูกเลือกไว้ คลิก **ตั้งค่า...** เพื่อแก้ไขรายละเอียดการตั้งค่าสำหรับการส่งไฟล์ที่น่าสงสัย (สำหรับข้อมูลเพิ่มเติม โปรดดู ThreatSense.Net)

ขั้นตอนต่อไปในกระบวนการติดตั้งคือการกำหนดค่าการตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์ แอพพลิเคชันที่อาจไม่พึงประสงค์ไม่จำเป็นต้องมีอันตราย แต่มักจะมีผลเสียกับการทำงานของระบบปฏิบัติการ แอพพลิเคชันเหล่านี้มักจะมาพร้อมกับโปรแกรมอื่นและอาจสังเกตได้ยากในระหว่างกระบวนการการติดตั้ง แม้ว่าแอพพลิเคชันเหล่านี้มักจะแสดงการแจ้งระหว่างการติดตั้ง แต่ระบบจะสามารถติดตั้งแอพพลิเคชันได้อย่างง่ายดายโดยไม่ต้องรับการยินยอมจากคุณ เลือกตัวเลือก **เปิดใช้งานการตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์** เพื่ออนุญาตให้ ESET NOD32 Antivirus ตรวจหาภัยคุกคามประเภทนี้ (แนะนำ) ถ้าคุณไม่ต้องการเปิดใช้งานคุณลักษณะนี้ ให้เลือกตัวเลือก **ปิดการใช้งานการตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์**

คลิก **ติดตั้ง** เพื่อติดตั้ง ESET NOD32 Antivirus ในดิสก์ **Macintosh HD** มาตรฐาน ถ้าคุณต้องการเลือกดิสก์อื่น ให้คลิก **เปลี่ยนแปลงตำแหน่งการติดตั้ง...**

การติดตั้งแบบกำหนดเอง

โหมดการติดตั้งแบบกำหนดเองได้รับการออกแบบมาเพื่อผู้ใช้ที่มีประสบการณ์ ซึ่งต้องการแก้ไขการตั้งค่าขั้นสูงในระหว่างกระบวนการติดตั้ง

หลังจากเลือกโหมดการติดตั้งแบบ **กำหนดเอง** คุณจะต้องป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** (ข้อมูลการตรวจสอบสิทธิ์ทีุุ่่คุณได้รับหลังจากซื้อหรือลงทะเบียนผลิตภัณฑ์) ลงในฟิลด์ที่สอดคล้องกัน ถ้าคุณไม่มีชื่อผู้ใช้และรหัสผ่านที่ใช้ได้ คุณสามารถเลือกตัวเลือก **ตั้งค่าพารามิเตอร์การอัพเดทในภายหลัง** เพื่อดำเนินการติดตั้งต่อ คุณสามารถป้อนชื่อผู้ใช้และรหัสผ่านได้ในภายหลัง

ถ้าคุณใช้พร็อกซีเซิร์ฟเวอร์ คุณสามารถกำหนดพารามิเตอร์ได้ โดยเลือกตัวเลือก **ฉันใช้พร็อกซีเซิร์ฟเวอร์** ป้อนที่อยู่ IP หรือ URL ของพร็อกซีเซิร์ฟเวอร์ของคุณในฟิลด์ **ที่อยู่** ในฟิลด์ **พอร์ต** ให้ระบุพอร์ตที่พร็อกซีเซิร์ฟเวอร์ยอมรับการเชื่อมต่อ (3128 ตามค่าเริ่มต้น) ในกรณีที่พร็อกซีเซิร์ฟเวอร์ต้องการการตรวจสอบสิทธิ์ ให้ป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่ถูกต้อง เพื่อให้สิทธิ์ในการเข้าถึงพร็อกซีเซิร์ฟเวอร์ ถ้าคุณแน่ใจว่าไม่มีการใช้งานพร็อกซีเซิร์ฟเวอร์ ให้เลือกตัวเลือก **ฉันไม่ใช้พร็อกซีเซิร์ฟเวอร์**ถ้าคุณไม่แน่ใจว่า คุณสามารถใช้การตั้งค่าระบบในปัจจุบัน โดยเลือก **ใช้การตั้งค่าระบบ (แนะนำ)**

ถ้าจะมีการจัดการ ESET NOD32 Antivirus โดย ESET Remote Administrator (ERA) คุณสามารถตั้งค่าพารามิเตอร์ของ ERA Server (ชื่อเซิร์ฟเวอร์ พอร์ต และรหัสผ่าน) เพื่อเชื่อมต่อ ESET NOD32 Antivirus โดยอัตโนมัติไปยัง ERA Server หลังจากการติดตั้ง

ในขั้นตอนถัดไป คุณสามารถ **กำหนดผู้ใช้ที่มีสิทธิ์** ที่จะสามารถแก้ไขการกำหนดค่าโปรแกรมได้ จากรายการผู้ใช้ที่ด้านซ้าย ให้เลือกผู้ใช้และ **เพิ่ม** ผู้ใช้ไปยังรายการ **ผู้ใช้ที่มีสิทธิ์** เมื่อต้องการแสดงผู้ใช้ระบบทั้งหมด ให้เลือกตัวเลือก **แสดงผู้ใช้ทั้งหมด**

ระบบการเตือนล่วงหน้า ThreatSense.Net ช่วยให้แน่ใจได้ว่า ESET จะได้รับการแจ้งในทันทีและอย่างต่อเนื่องเกี่ยวกับการแฝงตัวใหม่เพื่อการป้องกันลูกค้าได้อย่างรวดเร็ว ระบบจะอนุญาตให้ส่งภัยคุกคามใหม่ไปยังแล็บภัยคุกคามของ ESET ซึ่งภัยคุกคามจะถูกวิเคราะห์ ประมวลผล และเพิ่มไปยังฐานข้อมูลไวรัส ตามค่าเริ่มต้น ตัวเลือก **เปิดใช้ระบบการเตือนล่วงหน้า ThreatSense.Net** จะถูกเลือกไว้ คลิก **ตั้งค่า...** เพื่อแก้ไขรายละเอียดการตั้งค่าสำหรับการส่งไฟล์ที่น่าสงสัย สำหรับข้อมูลเพิ่มเติม โปรดดู ThreatSense.Net

ขั้นตอนต่อไปในกระบวนการติดตั้งคือการกำหนดค่าการตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์ แอพพลิเคชันที่อาจไม่พึงประสงค์ไม่จำเป็นต้องมีอันตราย แต่มักจะมีผลเสียกับการทำงานของระบบปฏิบัติการ แอพพลิเคชันเหล่านี้มักจะมาพร้อมกับโปรแกรมอื่นและอาจสังเกตได้ยากในระหว่างกระบวนการการติดตั้ง แม้ว่าแอพพลิเคชันเหล่านี้มักจะแสดงการแจ้งระหว่างการติดตั้ง แต่ระบบจะสามารถติดตั้งแอพพลิเคชันได้อย่างง่ายดายโดยไม่ต้องรับการยินยอมจากคุณ เลือกตัวเลือก **เปิดใช้งานการตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์** เพื่ออนุญาตให้ ESET NOD32 Antivirus ตรวจหาภัยคุกคามประเภทนี้ (แนะนำ)

คลิก **ติดตั้ง** เพื่อติดตั้ง ESET NOD32 Antivirus ในดิสก์ **Macintosh HD** มาตรฐาน ถ้าคุณต้องการเลือกดิสก์อื่น ให้คลิก **เปลี่ยนแปลงตำแหน่งการติดตั้ง...**

การติดตั้งระยะไกล

การติดตั้งระยะไกลจะช่วยให้คุณสามารถสร้างแพ็คเกจการติดตั้งที่สามารถติดตั้งบนคอมพิวเตอร์เป้าหมายโดยใช้ซอฟต์แวร์สำหรับเดสก์ท็อประยะไกล ESET NOD32 Antivirus สามารถได้รับการจัดการจากระยะไกลผ่าน ESET Remote Administrator

การติดตั้งระยะไกลสามารถดำเนินการได้ในสองช่วง:

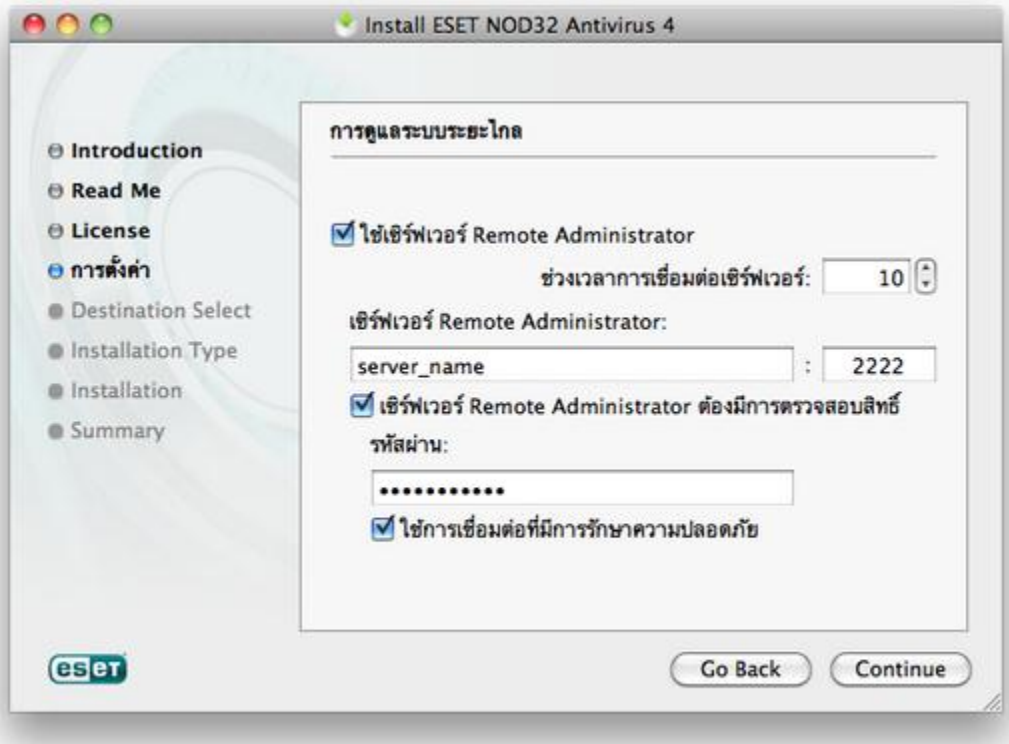
1. การสร้างแพ็คเกจการติดตั้งระยะไกลโดยโปรแกรมติดตั้ง ESET
2. การติดตั้งระยะไกลโดยใช้ซอฟต์แวร์สำหรับเดสก์ท็อประยะไกล

การสร้างแพคเกจการติดตั้งระยะไกล

หลังจากเลือกโหมดการติดตั้ง **ระยะไกล** คุณจะได้รับพรอมต์ให้ป้อนชื่อผู้ใช้และรหัสผ่านเพื่อเปิดใช้งานการอัพเดทอัตโนมัติของ ESET NOD32 Antivirus ป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ของคุณ (ข้อมูลการตรวจสอบสิทธิ์ที่คุณได้รับหลังจากซื้อหรือลงทะเบียนผลิตภัณฑ์) ลงในฟิลด์ที่สอดคล้องกัน ถ้าคุณไม่มีชื่อผู้ใช้และรหัสผ่านที่ใช้ได้ คุณสามารถเลือกตัวเลือก **ตั้งค่าพารามิเตอร์การอัพเดทในภายหลัง** เพื่อดำเนินการติดตั้งต่อ คุณสามารถป้อนชื่อผู้ใช้และรหัสผ่านได้โดยตรงลงในโปรแกรมได้ในภายหลัง

ขั้นตอนถัดไปคือการกำหนดค่าการเชื่อมต่ออินเทอร์เน็ต ถ้าคุณใช้พร็อกซีเซิร์ฟเวอร์ คุณสามารถกำหนดพารามิเตอร์ได้ โดยเลือกตัวเลือก **ฉันใช้พร็อกซีเซิร์ฟเวอร์** ถ้าคุณแน่ใจว่าไม่มีการใช้งานพร็อกซีเซิร์ฟเวอร์ ให้เลือกตัวเลือก **ฉันไม่ใช้พร็อกซีเซิร์ฟเวอร์** ถ้าคุณไม่แน่ใจว่า คุณสามารถใช้การตั้งค่าระบบในปัจจุบัน โดยเลือก **ใช้การตั้งค่าระบบ**

ในขั้นตอนถัดไป คุณสามารถตั้งค่าพารามิเตอร์ของ ERA Server เพื่อเชื่อมต่อ ESET NOD32 Antivirus โดยอัตโนมัติไปยัง ERA Server หลังจากการติดตั้ง เมื่อต้องการเปิดใช้งานการดูแลระบบระยะไกล ให้เลือกตัวเลือก **ใช้เซิร์ฟเวอร์ Remote Administrator ช่วงเวลาการเชื่อมต่อเซิร์ฟเวอร์** จะกำหนดความถี่ที่ ESET NOD32 Antivirus จะเชื่อมต่อกับ ERA Server ในฟิลด์ **เซิร์ฟเวอร์ Remote Administrator** ให้ระบุที่อยู่ของเซิร์ฟเวอร์ (ที่มีการติดตั้ง ERA Server) และหมายเลขพอร์ต ฟิลด์นี้จะมีพอร์ตของเซิร์ฟเวอร์ที่กำหนดไว้ล่วงหน้า ซึ่งใช้สำหรับการเชื่อมต่อเครือข่าย เราขอแนะนำให้ใช้การตั้งค่าพอร์ตที่เป็นค่าเริ่มต้น คือ *2222* ถ้าการเชื่อมต่อกับ ERA Server ถูกป้องกันด้วยรหัสผ่าน ให้เลือกช่องทำเครื่องหมาย **เซิร์ฟเวอร์ Remote Administrator ต้องการการตรวจสอบสิทธิ์** และพิมพ์รหัสผ่านในฟิลด์ **รหัสผ่าน**



ในขั้นตอนถัดไป คุณสามารถ **กำหนดผู้ใช้ที่มีสิทธิ์** ที่จะสามารถแก้ไขการกำหนดค่าโปรแกรมได้ จากรายการผู้ใช้ที่ด้านซ้าย ให้เลือกผู้ใช้และ **เพิ่ม** ผู้ใช้ไปยังรายการ **ผู้ใช้ที่มีสิทธิ์** เมื่อต้องการแสดงผู้ใช้ระบบทั้งหมด ให้เลือกตัวเลือก **แสดงผู้ใช้ทั้งหมด**

ระบบการเตือนล่วงหน้า ThreatSense.Net ช่วยให้แน่ใจได้ว่า ESET จะได้รับการแจ้งในทันทีและอย่างต่อเนื่องเกี่ยวกับการแฝงตัวใหม่เพื่อการป้องกันลูกค้าได้อย่างรวดเร็ว ระบบจะอนุญาตให้ส่งภัยคุกคามใหม่ไปยังแล็บภัยคุกคามของ ESET ซึ่งภัยคุกคามจะถูกวิเคราะห์ ประมวลผล และเพิ่มไปยังฐานข้อมูลไวรัส ตามค่าเริ่มต้น ตัวเลือก **เปิดใช้ระบบการเตือนล่วงหน้า ThreatSense.Net** จะถูกเลือกไว้ คลิก **ตั้งค่า...** เพื่อแก้ไขรายละเอียดการตั้งค่าสำหรับการส่งไฟล์ที่น่าสงสัย สำหรับข้อมูลเพิ่มเติม โปรดดู ThreatSense.Net

ขั้นตอนต่อไปในกระบวนการติดตั้งคือการกำหนดค่าการตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์ แอพพลิเคชันที่อาจไม่พึงประสงค์ไม่จำเป็นต้องมีอันตราย แต่มักจะมีผลเสียกับการทำงานของระบบปฏิบัติการ แอพพลิเคชันเหล่านี้มักจะมาพร้อมกับโปรแกรมอื่นและอาจสังเกตได้ยากในระหว่างกระบวนการการติดตั้ง แม้ว่าแอพพลิเคชันเหล่านี้มักจะแสดงการแจ้งระหว่างการติดตั้ง แต่ระบบจะสามารถติดตั้งแอพพลิเคชันได้อย่างง่ายดายโดยไม่ต้องรับการยินยอมจากคุณ เลือกตัวเลือก **เปิดใช้งานการตรวจหาแอพพลิเคชันที่อาจไม่พึงประสงค์** เพื่ออนุญาตให้ ESET NOD32 Antivirus ตรวจหาภัยคุกคามประเภทนี้ (แนะนำ)

ในขั้นตอนสุดท้ายของวิซาร์ดการติดตั้ง ให้เลือกโฟลเดอร์ปลายทางสำหรับแพ็คเกจการติดตั้ง *(EAV4_Remote_Install.pkg)* และสคริปต์เชลล์ของการถอนการติดตั้ง *(EAV4_Remote_UnInstall.sh)*

การติดตั้งระยะไกลในคอมพิวเตอร์เป้าหมาย

ESET NOD32 Antivirus สามารถติดตั้งในคอมพิวเตอร์เป้าหมาย โดยใช้เดสก์ท็อประยะไกลของ Apple หรือเครื่องมืออื่นๆ ที่สนับสนุนการติดตั้งของแพ็คเกจมาตรฐานของ Mac (*.pkg*) ซึ่งจะคัดลอกไฟล์และเรียกใช้สคริปต์เชลล์ในคอมพิวเตอร์เป้าหมาย

เมื่อต้องการติดตั้ง ESET NOD32 Antivirus โดยใช้เดสก์ท็อประยะไกลของ Apple ให้เรียกใช้คำสั่ง **ติดตั้งการแพ็คเกจ...** ค้นหาไฟล์ *EAV4_Remote_Install.pkg* และคลิก **ติดตั้ง**

สำหรับคำแนะนำโดยละเอียดเกี่ยวกับวิธีดูแลระบบคอมพิวเตอร์ไคลเอ็นต์โดยใช้ ESET Remote Administrator โปรดอ่านคู่มือผู้ใช้ของ ESET Remote Administrator

การถอนการติดตั้งระยะไกล

เมื่อต้องการถอนการติดตั้ง ESET NOD32 Antivirus ออกจากคอมพิวเตอร์ไคลเอ็นต์:

1. ใช้คำสั่ง **คัดลอกรายการ...** ในเดสก์ท็อประยะไกลของ Apple ค้นหาสคริปต์เชลล์ของการถอนการติดตั้ง *(EAV4_Remote_UnInstall.sh* ซึ่งสร้างขึ้นพร้อมกับแพ็คเกจการติดตั้ง) และคัดลอกสคริปต์เชลล์ไปยังคอมพิวเตอร์เป้าหมาย
2. เรียกใช้ **ส่งคำสั่ง Unix...** ในเดสก์ท็อประยะไกลของ Apple หลังจากถอนการติดตั้งสำเร็จ การบันทึกของคอนโซลจะปรากฏ

การอัพเกรดระยะไกล

การอัพเกรดระยะไกลของ ESET NOD32 Antivirus มีการดำเนินการโดยคำสั่ง **ติดตั้งแพ็คเกจ...** ในเดสก์ท็อประยะไกลของ Apple

หมายเหตุ: การตั้งค่าที่บันทึกไว้ในแพ็คเกจการติดตั้งระยะไกลของ ESET จะไม่มีการนำไปใช้กับคอมพิวเตอร์เป้าหมายในระหว่างกระบวนการอัพเกรด ควรใช้ ESET Remote Administrator เพื่อกำหนดค่า ESET NOD32 Antivirus จากระยะไกลหลังจากการอัพเกรด

การป้อนชื่อผู้ใช้และรหัสผ่าน

เพื่อให้การทำงานมีประสิทธิภาพสูงสุด สิ่งสำคัญคือการตั้งค่าโปรแกรมให้ดาวน์โหลดการอัพเดทฐานข้อมูลไวรัสได้โดยอัตโนมัติ การดำเนินการนี้จะเกิดขึ้นต่อเมื่อมีการป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่ถูกต้องใน ตั้งค่าการอัพเดท

การสแกนคอมพิวเตอร์ตามต้องการ

หลังจากติดตั้ง ESET NOD32 Antivirus คุณควรดำเนินการสแกนคอมพิวเตอร์เพื่อหารหัสที่เป็นอันตราย จากหน้าต่างหลักของโปรแกรม ให้คลิก **การสแกนคอมพิวเตอร์** แล้วคลิก **การสแกนแบบสมาร์ท** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสแกนคอมพิวเตอร์ตามต้องการ ให้ดูส่วน การสแกนคอมพิวเตอร์ตามต้องการ

คู่มือระดับเริ่มต้น

บทนี้จะให้ภาพรวมเริ่มต้นของ ESET NOD32 Antivirus และการตั้งค่าพื้นฐานของโปรแกรม

ส่วนติดต่อผู้ใช้

หน้าต่างหลักของโปรแกรม ESET NOD32 Antivirus จะถูกแบ่งออกเป็นสองส่วนหลัก หน้าต่างหลักที่ด้านขวาจะแสดงข้อมูลที่เกี่ยวข้องกับตัวเลือกที่เลือกจากเมนูหลักทางด้านซ้าย

ข้อมูลต่อไปนี้จะเป็นคำอธิบายของตัวเลือกภายในเมนูหลัก:

- **สถานะการป้องกัน** - ให้ข้อมูลเกี่ยวกับสถานะการป้องกันของ ESET NOD32 Antivirus ถ้าเปิดใช้งาน **โหมดขั้นสูง** เมนูย่อยของ **สถิติ** จะปรากฏ
- **การสแกนคอมพิวเตอร์** - ตัวเลือกนี้จะช่วยให้คุณสามารถกำหนดค่าและเปิดใช้ **การสแกนคอมพิวเตอร์ตามต้องการ**
- **อัพเดท** - แสดงข้อมูลเกี่ยวกับการอัพเดทฐานข้อมูลไวรัส
- **ตั้งค่า** - เลือกตัวเลือกนี้เพื่อปรับระดับการรักษาความปลอดภัยของคอมพิวเตอร์ ถ้าเปิดใช้งาน **โหมดขั้นสูง** เมนูย่อยของ **การป้องกันไวรัสและสปายแวร์** จะปรากฏ
- **เครื่องมือ** - ให้การเข้าถึง **ไฟล์บันทึก การกักเก็บ** และ **เครื่องมือวางกำหนดการ** ตัวเลือกนี้จะปรากฏเฉพาะใน **โหมดขั้นสูง**
- **วิธีใช้** - ให้ข้อมูลของโปรแกรม เข้าถึงไฟล์วิธีใช้ ฐานข้อมูลความรู้ทางอินเทอร์เน็ต และเว็บไซต์ ESET

ส่วนติดต่อผู้ใช้ของ ESET NOD32 Antivirus จะช่วยให้ผู้ใช้สามารถสลับระหว่างโหมดมาตรฐานและขั้นสูง

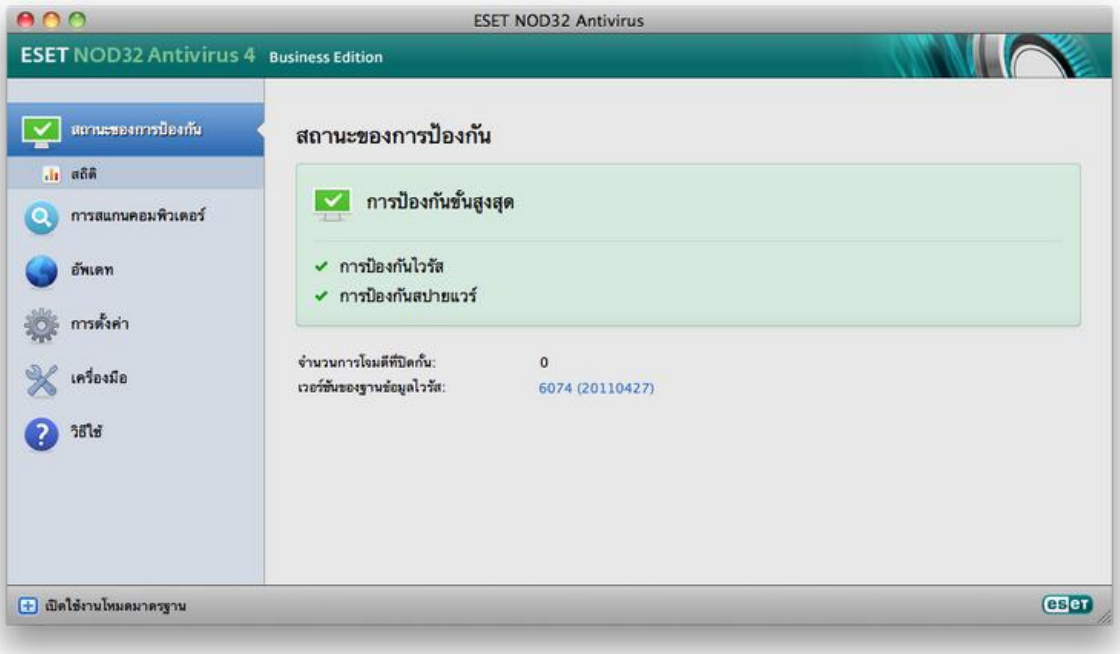
โหมดมาตรฐานจะให้การเข้าถึงคุณลักษณะที่ต้องการสำหรับการดำเนินการทั่วไป ซึ่งจะไม่แสดงตัวเลือกขั้นสูง เมื่อต้องการสลับระหว่างโหมด ให้คลิกที่ไอคอนบวก **(+)** ที่อยู่ถัดจาก **เปิดใช้งานโหมดขั้นสูง/เปิดใช้งานโหมดมาตรฐาน** ในมุมซ้ายล่างของหน้าต่างหลักของโปรแกรม

โหมดมาตรฐานจะให้การเข้าถึงคุณลักษณะที่ต้องการสำหรับการดำเนินการทั่วไป ซึ่งจะไม่แสดงตัวเลือกขั้นสูง

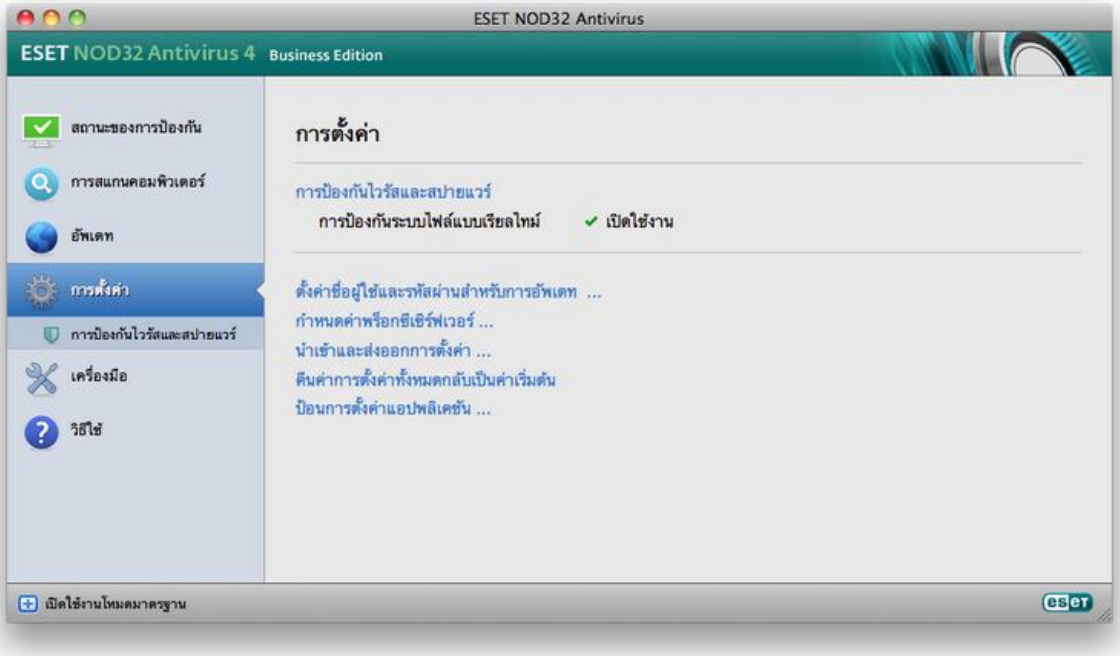
การสลับไปยังโหมดขั้นสูงจะช่วยเพิ่มตัวเลือก **เครื่องมือ** ไปยังเมนูหลัก ตัวเลือก **เครื่องมือ** จะช่วยให้คุณสามารถเข้าถึงเมนูย่อยสำหรับ **ไฟล์บันทึก การกักเก็บ** และ **เครื่องมือวางกำหนดการ**

หมายเหตุ: คำแนะนำทั้งหมดที่มีอยู่ในคู่มือนี้จะดำเนินการใน **โหมดขั้นสูง**

โหมดมาตรฐาน:

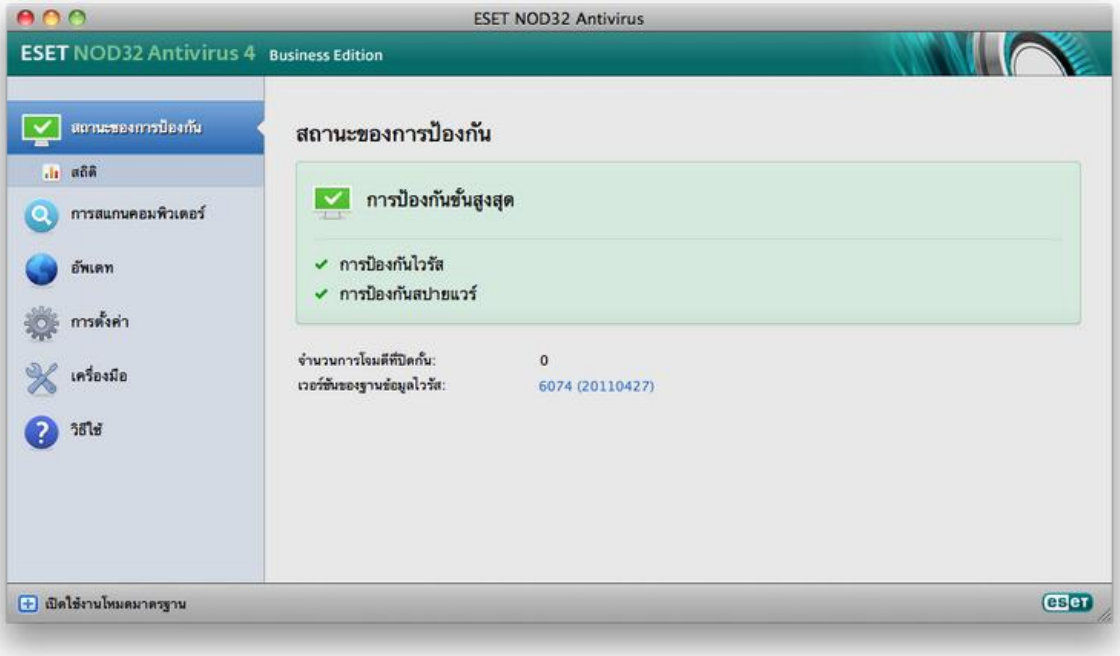


โหมดขั้นสูง:



การตรวจสอบการทำงานของระบบ

เมื่อต้องการดู **สถานะการป้องกัน** ให้คลิกตัวเลือกบนสุดจากเมนูหลัก ข้อมูลสรุปของสถานะเกี่ยวกับการทำงานของ ESET NOD32 Antivirus จะปรากฏในหน้าต่างหลักและเมนูย่อยพร้อมกับ **สถิติ** เลือกเพื่อดูข้อมูลโดยละเอียดมากขึ้นและสถิติเกี่ยวกับการสแกนคอมพิวเตอร์ที่มีการดำเนินการในระบบของคุณ หน้าต่างสถิติจะสามารถใช้ได้ในโหมดขั้นสูงเท่านั้น

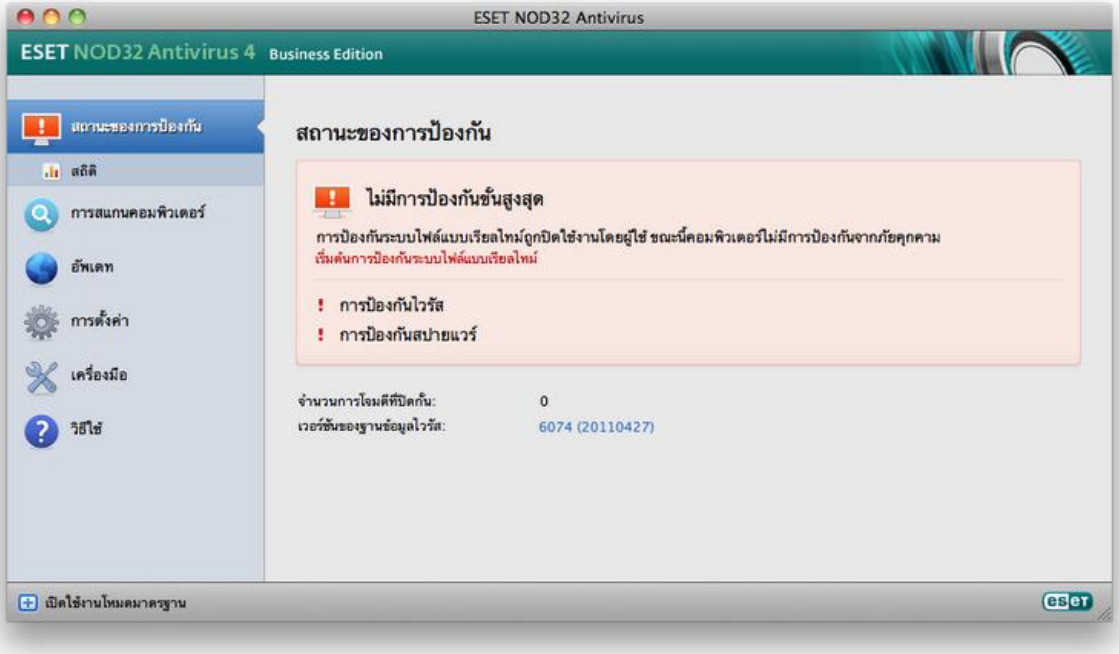


ควรทำอย่างไรเมื่อโปรแกรมทำงานไม่ถูกต้อง

ถ้าโมดูลที่เปิดใช้งานทำงานได้อย่างถูกต้อง จะมีการระบุเป็นไอคอนถูกสีเขียว ถ้าไม่ใช่ เครื่องหมายอัศเจรีย์สีแดงหรือไอคอนการแจ้งสีส้มจะปรากฏขึ้น และระบบจะแสดงข้อมูลเพิ่มเติมเกี่ยวกับโมดูลที่ส่วนบนของหน้าต่าง ทางแก้ไขที่แนะนำสำหรับการแก้ไขโมดูลจะปรากฏขึ้นเช่นกัน เมื่อต้องการเปลี่ยนสถานะของแต่ละโมดูล ให้คลิก **ตั้งค่า** ในเมนูหลักและคลิกที่โมดูลที่ต้องการ

ถ้าคุณไม่สามารถแก้ไขปัญหาโดยใช้ทางแก้ไขที่แนะนำได้ ให้คลิก **วิธีใช้** เพื่อเข้าถึงไฟล์วิธีใช้หรือค้นหาฐานข้อมูล

ถ้าคุณต้องการความช่วยเหลือ คุณสามารถติดต่อขอรับการสนับสนุนจากฝ่ายการดูแลลูกค้าของ ESET ที่ เว็บไซต์ ESET ฝ่ายดูแลลูกค้าของ ESET จะตอบคำถามของคุณอย่างรวดเร็วและช่วยระบุการแก้ไขปัญหา



ทำงานกับ ESET NOD32 Antivirus

การป้องกันไวรัสและสปายแวร์

การป้องกันไวรัสจะช่วยป้องกันการโจมตีจากระบบที่เป็นอันตรายโดยการแก้ไขไฟล์ที่อาจเป็นภัยคุกคาม หากตรวจพบภัยคุกคามที่มีรหัสที่เป็นอันตราย โมดูลป้องกันไวรัสสามารถล้างรหัสดังกล่าวด้วยการปิดกั้น จากนั้นจึงกำจัด ลบ หรือย้ายไปยังที่กักเก็บ

การป้องกันระบบไฟล์แบบเรียลไทม์

การป้องกันระบบไฟล์แบบเรียลไทม์จะควบคุมเหตุการณ์ที่เกี่ยวกับการป้องกันไวรัสทั้งหมดในระบบ โปรแกรมจะสแกนไฟล์ทั้งหมดเพื่อหารหัสที่เป็นอันตรายเมื่อเปิด สร้าง หรือเรียกใช้ไฟล์ในคอมพิวเตอร์ โปรแกรมจะเริ่มต้นการป้องกันระบบไฟล์แบบเรียลไทม์เมื่อเริ่มต้นระบบ

การตั้งค่าการป้องกันแบบเรียลไทม์

การป้องกันระบบไฟล์แบบเรียลไทม์จะตรวจสอบสื่อทุกประเภท และจะเรียกใช้การสแกนตามเหตุการณ์ต่างๆ เมื่อใช้วิธีการตรวจหาเทคโนโลยี ThreatSense (ดังที่อธิบายไว้ในส่วน การตั้งค่าพารามิเตอร์กลไก ThreatSense) การป้องกันระบบไฟล์แบบเรียลไทม์อาจแตกต่างกันตามไฟล์ที่สร้างใหม่และไฟล์ที่มีอยู่ สำหรับไฟล์ที่สร้างขึ้นใหม่ อาจใช้การควบคุมในระดับที่ลึกกว่า

ตามค่าเริ่มต้น การป้องกันแบบเรียลไทม์จะเริ่มต้นทำงานเมื่อเริ่มต้นระบบและให้การสแกนทำงานต่อเนื่อง ในกรณีพิเศษ (เช่น ถ้ามีข้อขัดแย้งกับเครื่องสแกนแบบเรียลไทม์อื่น) คุณสามารถสิ้นสุดการทำงานของการป้องกันแบบเรียลไทม์ได้โดยคลิกที่ไอคอน ESET NOD32 Antivirus ซึ่งอยู่ในแถบเมนูของคุณ (ด้านบนของหน้าจอ) แล้วเลือกตัวเลือก **ปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** นอกจากนี้ คุณสามารถสิ้นสุดการทำงานของการป้องกันแบบเรียลไทม์ได้จากหน้าต่างหลักของโปรแกรม (**ตั้งค่า > การป้องกันไวรัสและสปายแวร์ > ปิดใช้งาน**)

เมื่อต้องการแก้ไขการตั้งค่าขั้นสูงของการป้องกันแบบเรียลไทม์ ให้ไปที่ **ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > การป้องกัน > การป้องกันแบบเรียลไทม์** และคลิกปุ่ม **ตั้งค่า...** ที่อยู่ถัดจาก **ตัวเลือกขั้นสูง** (ดังที่อธิบายไว้ในส่วน ตัวเลือกการสแกนขั้นสูง)

สแกนเมื่อ (เหตุการณ์ที่ทำให้มีการสแกน)

ตามค่าเริ่มต้น ไฟล์ทั้งหมดจะถูกสแกนเมื่อมี **การเปิดไฟล์, การสร้างไฟล์** หรือ **การเรียกใช้ไฟล์** ขอแนะนำให้คุณคงการตั้งค่าเริ่มต้นไว้ เนื่องจากการตั้งค่าเหล่านี้จะให้การป้องกันแบบเรียลไทม์ในระดับสูงสุดสำหรับคอมพิวเตอร์ของคุณ

ตัวเลือกการสแกนขั้นสูง

ในหน้าต่างนี้ คุณสามารถกำหนดประเภทวัตถุที่จะสแกนได้ด้วยกลไก ThreatSense และเปิดใช้งาน/ปิดใช้งาน **การวิเคราะห์พฤติกรรมขั้นสูง** และแก้ไขการตั้งค่าสำหรับอาร์ไคฟ์และแคชของไฟล์

เราไม่แนะนำให้เปลี่ยนค่าเริ่มต้นในส่วน **การตั้งค่าอาร์ไคฟ์เริ่มต้น** ยกเว้นถ้าจำเป็นสำหรับการแก้ไขปัญหา เนื่องจากค่าการซ้อนของอาร์ไคฟ์ที่สูงขึ้นอาจทำให้ประสิทธิภาพการทำงานของระบบลดลง

คุณสามารถสลับการสแกนการวิเคราะห์พฤติกรรมขั้นสูงของ ThreatSense สำหรับไฟล์ที่เรียกใช้ สร้าง และแก้ไขได้แยกกัน โดยคลิกที่ช่องทำเครื่องหมาย **การวิเคราะห์พฤติกรรมขั้นสูง** ในส่วนพารามิเตอร์แต่ละส่วนของ ThreatSense ที่สอดคล้องกัน

เพื่อให้มีขอบเขตของระบบน้อยที่สุดเมื่อใช้การป้องกันแบบเรียลไทม์ คุณสามารถกำหนดขนาดของแคชประสิทธิภาพ การทำงานนี้จะใช้งานได้เมื่อคุณใช้ตัวเลือก **เปิดใช้งานแคชของไฟล์ที่ไม่ติดไวรัส** ถ้าปิดใช้งานตัวเลือกนี้ ไฟล์ทั้งหมดจะถูกสแกนในแต่ละครั้งที่มีการเข้าถึง ไฟล์จะไม่ถูกสแกนซ้ำหลังจากอยู่ในแคช (ยกเว้นจะได้รับการแก้ไข) ซึ่งจะไม่เกินขนาดของแคชที่กำหนดไว้ ไฟล์จะถูกสแกนอีกครั้งทันทีหลังจากการอัพเดทฐานข้อมูลไวรัสแต่ละครั้ง

คลิก **เปิดใช้งานแคชของไฟล์ที่ไม่ติดไวรัส** เพื่อเปิดใช้งาน/ปิดใช้งานฟังก์ชันนี้ เมื่อต้องการตั้งค่าจำนวนไฟล์ที่จะให้อยู่ในแคช ให้ป้อนค่าที่ต้องการในฟิลด์ป้อนข้อมูลที่อยู่ถัดจาก **ขนาดแคช**

สามารถตั้งค่าพารามิเตอร์การสแกนเพิ่มเติมได้ในหน้าต่าง **ตั้งค่ากลไก ThreatSense** คุณสามารถกำหนดได้ว่าจะสแกน **วัตถุ** ประเภทใด โดยใช้ **ตัวเลือก** และระดับ **การล้าง** ใด และกำหนด **นามสกุล** และ **ขีดจำกัด** ของขนาดไฟล์สำหรับการป้องกันระบบไฟล์แบบเรียลไทม์ คุณสามารถเข้าสู่หน้าต่างการตั้งค่ากลไก ThreatSense โดยคลิกที่ปุ่ม **ตั้งค่า...** ที่อยู่ถัดจาก **กลไก ThreatSense** ในหน้าต่างการตั้งค่าขั้นสูง สำหรับข้อมูลโดยละเอียดเพิ่มเติมเกี่ยวกับพารามิเตอร์กลไก ThreatSense โปรดดู การตั้งค่าพารามิเตอร์กลไก ThreatSense

การยกเว้นจากการสแกน

ส่วนนี้จะช่วยให้คุณสามารถยกเว้นไฟล์และโฟลเดอร์บางรายการจากการสแกนได้

- **พาธ** - พาธไปยังไฟล์และโฟลเดอร์ที่ยกเว้น
- **ภัยคุกคาม** - ถ้ามีชื่อของภัยคุกคามถัดจากไฟล์ที่ยกเว้น หมายความว่า ไฟล์ดังกล่าวจะถูกยกเว้นสำหรับภัยคุกคามที่กำหนดเท่านั้น แต่ไม่ใช่ทั้งหมด ด้วยเหตุนี้ ถ้าไฟล์นั้นติดไวรัสในภายหลังด้วยมัลแวร์อื่น โมดูลป้องกันไวรัสจะตรวจพบไฟล์ดังกล่าว

- **เพิ่ม...** - ยกเว้นวัตถุจากการตรวจหา ป้อนพาธไปยังวัตถุ (และคุณสามารถใช้สัญลักษณ์ * และ ?) หรือเลือกโฟลเดอร์หรือไฟล์จากลำดับโครงสร้าง
- **แก้ไข...** - ช่วยให้คุณสามารถแก้ไขรายการที่เลือก
- **ลบ** - ลบรายการที่เลือกออก
- **ค่าเริ่มต้น** - ยกเลิกการยกเว้นทั้งหมด

เมื่อใดควรแก้ไขการกำหนดค่าการป้องกันแบบเรียลไทม์

การป้องกันแบบเรียลไทม์เป็นองค์ประกอบที่สำคัญที่สุดในการรักษาระบบที่ปลอดภัย โปรดใช้ความระมัดระวังเมื่อแก้ไขพารามิเตอร์ของการป้องกันแบบเรียลไทม์ เราขอแนะนำให้คุณแก้ไขพารามิเตอร์เหล่านี้ในกรณีพิเศษเท่านั้น ตัวอย่างเช่น ในกรณีที่มีข้อขัดแย้งกับบางแอพพลิเคชันหรือเครื่องมือสแกนแบบเรียลไทม์ของโปรแกรมป้องกันไวรัสอื่น

หลังจากการติดตั้ง ESET NOD32 Antivirus การตั้งค่าทั้งหมดจะได้รับการเพิ่มประสิทธิภาพเพื่อให้การรักษาความปลอดภัยให้กับระบบในระดับสูงสุดสำหรับผู้ใช้ เมื่อต้องการเรียกคืนการตั้งค่าเริ่มต้น ให้คลิกปุ่ม **ค่าเริ่มต้น** ที่อยู่บริเวณด้านซ้ายล่างของหน้าต่าง **การป้องกันแบบเรียลไทม์ (ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > การป้องกัน > การป้องกันแบบเรียลไทม์)**

การตรวจสอบการป้องกันแบบเรียลไทม์

เมื่อต้องการตรวจสอบว่าการป้องกันแบบเรียลไทม์กำลังทำงานและตรวจหาไวรัสอยู่ ให้ใช้ไฟล์ทดสอบของ eicar.com ไฟล์ทดสอบนี้เป็นไฟล์พิเศษที่ไม่มีอันตราย ซึ่งจะตรวจพบได้โดยโปรแกรมป้องกันไวรัสทุกโปรแกรม ไฟล์นี้สร้างขึ้นโดยสถาบัน EICAR (European Institute for Computer Antivirus Research) เพื่อทดสอบการทำงานของโปรแกรมป้องกันไวรัส

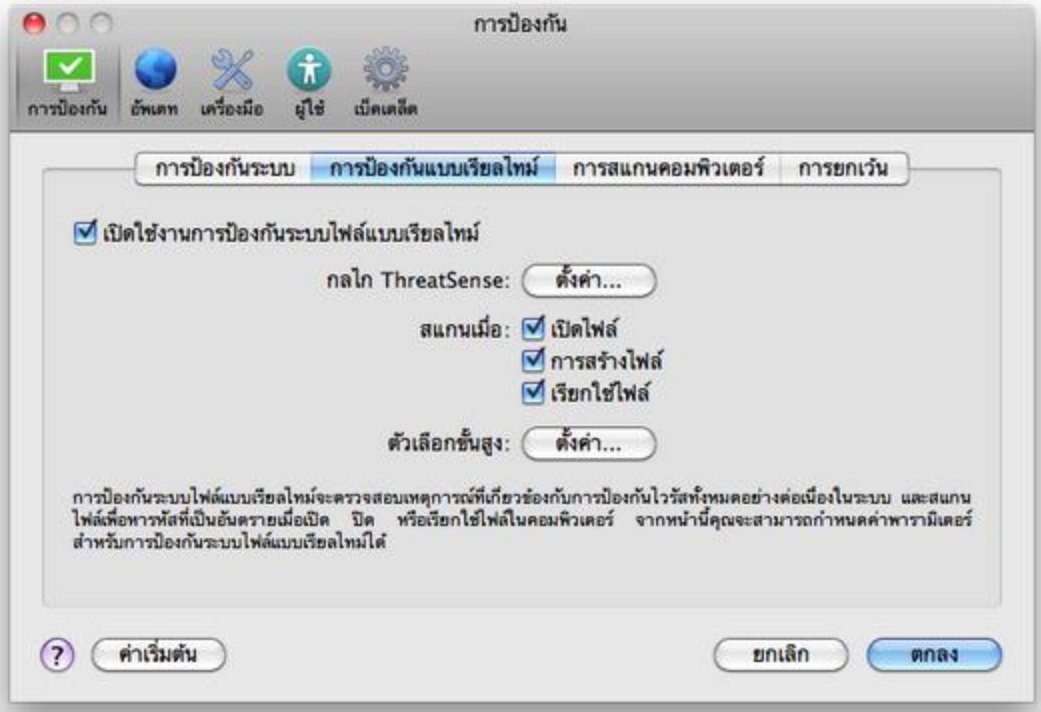
ควรทำอย่างไรเมื่อการป้องกันแบบเรียลไทม์ไม่ทำงาน

ในบทนี้ เราจะอธิบายสถานการณ์ของปัญหาที่อาจเกิดขึ้นเมื่อใช้การป้องกันแบบเรียลไทม์ รวมถึงการแก้ปัญหาดังกล่าวด้วย

การป้องกันแบบเรียลไทม์ถูกปิดใช้งาน

หากผู้ใช้ปิดการป้องกันแบบเรียลไทม์โดยไม่ได้ตั้งใจ ผู้ใช้จะต้องเปิดการใช้งานใหม่อีกครั้ง เมื่อต้องการเปิดใช้งานการป้องกันแบบเรียลไทม์อีกครั้ง ให้นำทางไปยัง **ตั้งค่า > การป้องกันไวรัสและสปายแวร์** และคลิกลิงค์ **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์** (ทางด้านขวา) ในหน้าต่างหลักของโปรแกรม

หรือคุณสามารถเปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์ได้ในหน้าต่างการตั้งค่าขั้นสูงที่อยู่ใต้ **การป้องกัน > การป้องกันแบบเรียลไทม์** โดยเลือกตัวเลือก **เปิดใช้งานการป้องกันระบบไฟล์แบบเรียลไทม์**



การป้องกันแบบเรียลไทม์ไม่พบหรือไม่ล้างการแฝงตัว

ตรวจสอบว่าไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอื่นในคอมพิวเตอร์ของคุณ หากมีการใช้การป้องกันแบบเรียลไทม์สองชนิดในเวลาเดียวกัน อาจมีข้อขัดแย้งเกิดขึ้นระหว่างกัน ขอแนะนำให้คุณถอนการติดตั้งโปรแกรมป้องกันไวรัสอื่นที่อาจมีอยู่ในระบบของคุณ

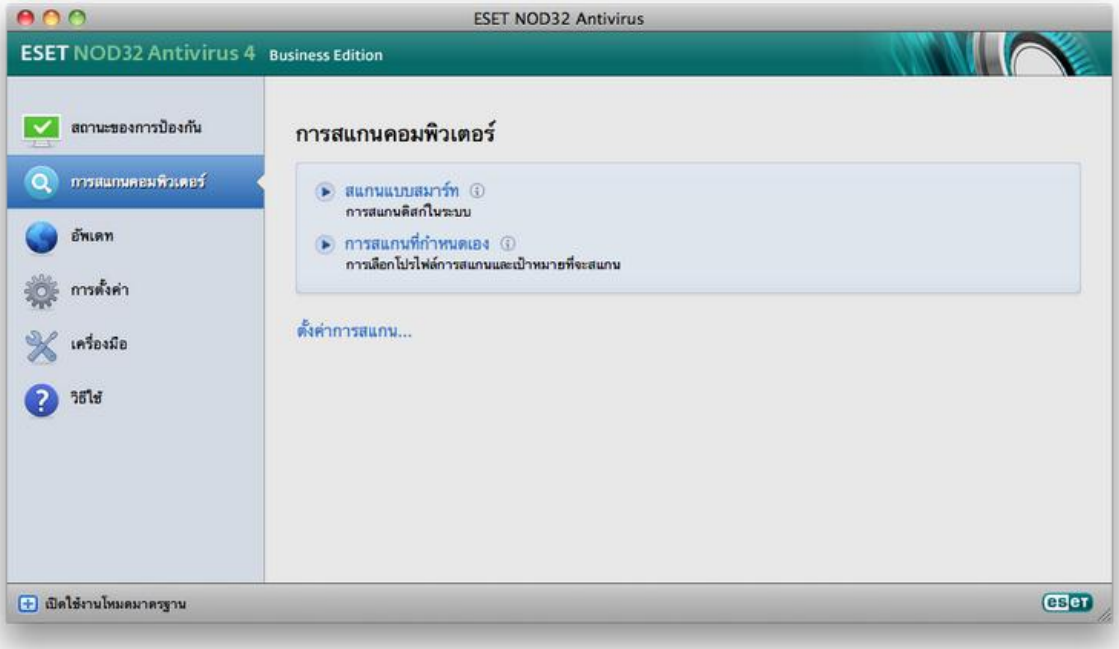
การป้องกันแบบเรียลไทม์ไม่เริ่มต้นทำงาน

ถ้าการป้องกันแบบเรียลไทม์ไม่เริ่มต้นทำงานเมื่อเริ่มต้นระบบ โปรแกรมอาจเกิดข้อขัดแย้งกับโปรแกรมอื่น ถ้าเป็นกรณีนี้ โปรดปรึกษาผู้เชี่ยวชาญที่ฝ่ายดูแลลูกค้าของ ESET

<u>การสแกนคอมพิวเตอร์ตามต้องการ</u>

หากคุณสงสัยว่าคอมพิวเตอร์ของคุณติดไวรัส (คอมพิวเตอร์ทำงานผิดปกติ) ให้เรียกใช้ **การสแกนคอมพิวเตอร์ > การสแกนแบบสมาร์ท** เพื่อตรวจหาการแฝงตัวในคอมพิวเตอร์ของคุณ เพื่อให้มีการป้องกันสูงสุด ควรเรียกใช้การสแกนคอมพิวเตอร์สม่ำเสมอในฐานะเป็นส่วนหนึ่งของมาตรการรักษาความปลอดภัย ไม่ใช่เรียกใช้เมื่อสงสัยว่ามีการติดไวรัส การสแกนเป็นประจำสามารถตรวจหาการแฝงตัวที่เครื่องมือสแกนแบบเรียลไทม์ตรวจไม่พบเมื่อมีการบันทึกไปยังดิสก์ ซึ่งอาจเกิดขึ้นในกรณีที่เครื่องมือสแกนแบบเรียลไทม์ถูกปิดการใช้งานในขณะที่มีการติดไวรัส หรือฐานข้อมูลไวรัสไม่ได้อัพเดท

ขอแนะนำให้คุณเรียกใช้การสแกนคอมพิวเตอร์ตามต้องการอย่างน้อยเดือนละหนึ่งครั้ง คุณสามารถกำหนดค่าการสแกนเป็นงานตามกำหนดการได้จาก **เครื่องมือ > เครื่องมือวางกำหนดการ**



ประเภทการสแกน

มีการสแกนคอมพิวเตอร์ตามต้องการสองประเภท **สแกนแบบสมาร์ท** จะสแกนระบบอย่างรวดเร็ว โดยไม่ต้องมีการกำหนดค่าพารามิเตอร์การสแกนเพิ่มเติม **การสแกนที่กำหนดเอง** จะช่วยให้คุณสามารถเลือกโปรไฟล์การสแกนที่กำหนดไว้ล่วงหน้าได้ และเลือกเป้าหมายการสแกนได้อย่างเจาะจง

สแกนแบบสมาร์ท

การสแกนแบบสมาร์ทจะช่วยให้คุณเริ่มต้นการสแกนคอมพิวเตอร์และล้างไฟล์ที่ติดไวรัสได้อย่างรวดเร็ว โดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ประโยชน์สำคัญคือการดำเนินการที่ง่ายโดยไม่ต้องกำหนดค่าการสแกนโดยละเอียด การสแกนแบบสมาร์ทจะตรวจสอบทุกไฟล์ในโฟลเดอร์ทั้งหมด รวมทั้งล้างและลบการแฝงตัวที่ตรวจพบโดยอัตโนมัติ โปรแกรมจะตั้งค่าระดับการล้างเป็นค่าเริ่มต้นโดยอัตโนมัติ สำหรับข้อมูลโดยละเอียดเกี่ยวกับประเภทการล้าง โปรดดูที่ส่วน การล้าง

การสแกนที่กำหนดเอง

การสแกนที่กำหนดเอง เป็นการสแกนที่เหมาะสมถ้าคุณต้องการระบุพารามิเตอร์การสแกน เช่น เป้าหมายการสแกน และวิธีการสแกน ประโยชน์ของการเรียกใช้การสแกนที่กำหนดเองคือ คุณสามารถกำหนดค่ารายละเอียดของพารามิเตอร์ได้ คุณสามารถบันทึกการกำหนดค่าอื่นๆ ไว้เป็นโปรไฟล์การสแกนที่ผู้ใช้กำหนด ซึ่งจะเป็นประโยชน์ถ้ามีการสแกนซ้ำกับพารามิเตอร์เดียวกัน

เมื่อต้องการเลือกเป้าหมายการสแกน ให้เลือก **การสแกนคอมพิวเตอร์ > การสแกนที่กำหนดเอง** และเลือก **เป้าหมายการสแกน** ที่เจาะจงจากลำดับโครงสร้าง นอกจากนี้ คุณสามารถระบุเป้าหมายการสแกนได้อย่างแม่นยำมากขึ้นโดยป้อนพาธไปยังโฟลเดอร์หรือไฟล์ที่คุณต้องการให้รวมไว้ ถ้าคุณต้องการเพียงสแกนระบบโดยไม่ต้องมีการล้าง ให้เลือกตัวเลือก **สแกนโดยไม่ล้าง** นอกจากนี้ คุณยังสามารถเลือกระดับการล้างได้สามระดับโดยคลิกที่ **ตั้งค่า... > การล้าง**

ขอแนะนำให้ดำเนินการสแกนคอมพิวเตอร์โดยใช้การสแกนที่กำหนดเองสำหรับผู้ใช้ขั้นสูงที่มีประสบการณ์การใช้โปรแกรมป้องกันไวรัสมาก่อนหน้านี้

เป้าหมายการสแกน

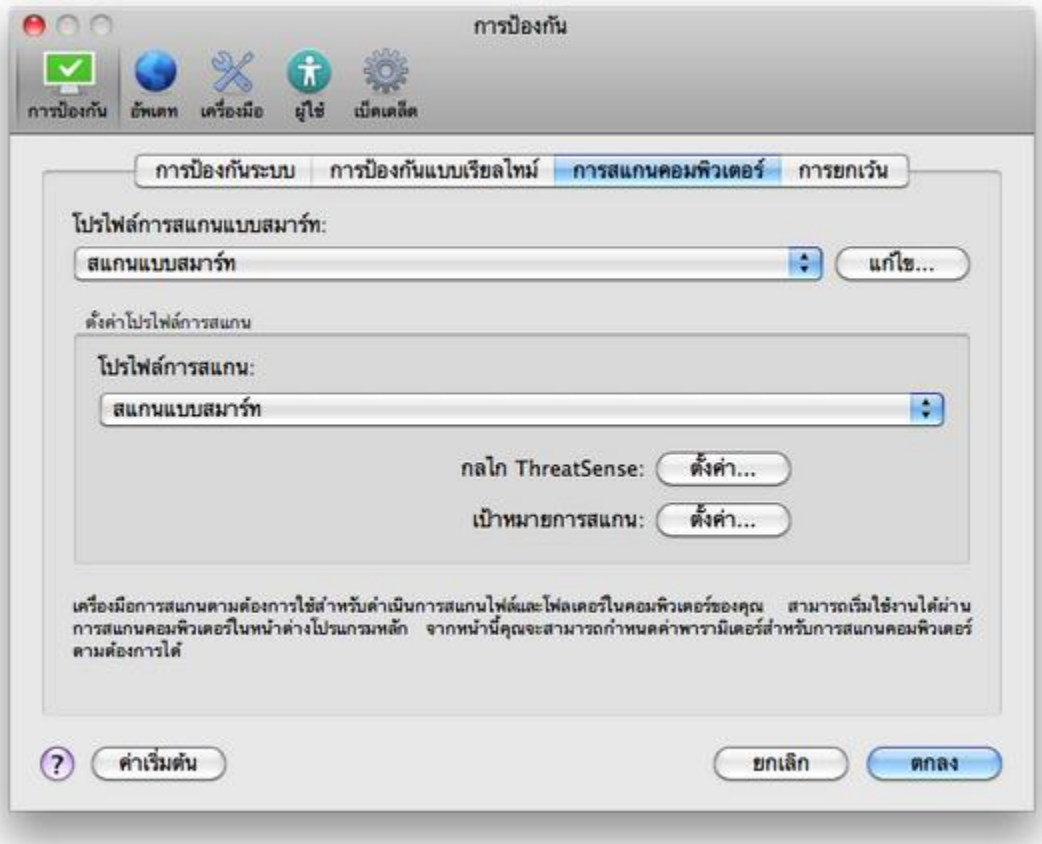
ลำดับโครงสร้างของเป้าหมายการสแกนจะช่วยให้คุณสามารถเลือกไฟล์และโฟลเดอร์ที่จะสแกนหาไวรัส โฟลเดอร์อาจถูกเลือกตามการตั้งค่าโปรไฟล์

คุณสามารถกำหนดเป้าหมายการสแกนได้อย่างแม่นยำมากขึ้นโดยป้อนพาธไปยังโฟลเดอร์หรือไฟล์ที่คุณต้องการให้รวมไว้ในการสแกน เลือกเป้าหมายจากลำดับโครงสร้างที่แสดงโฟลเดอร์ที่ใช้ได้ทั้งหมดในคอมพิวเตอร์

โปรไฟล์การสแกน

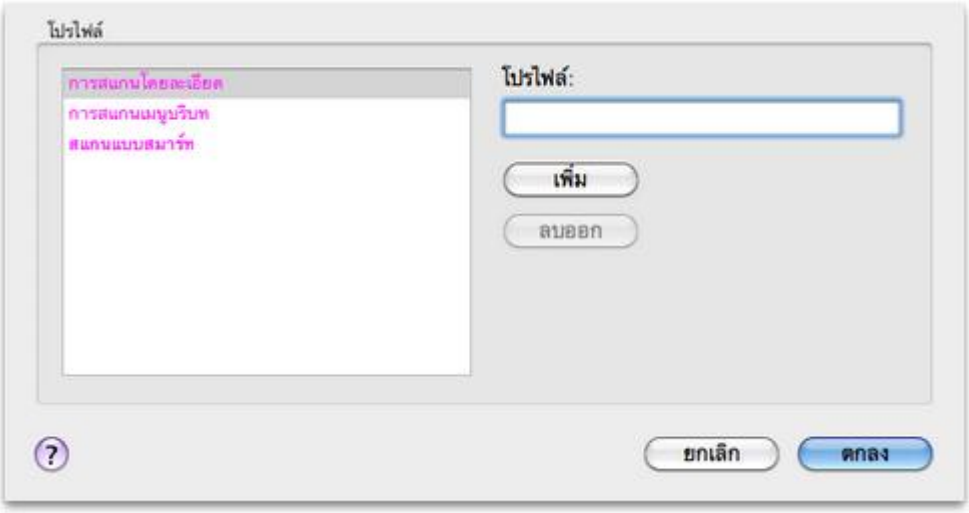
คุณสามารถบันทึกการตั้งค่าการสแกนที่ต้องการได้เพื่อการสแกนในอนาคต ขอแนะนำให้คุณสร้างโปรไฟล์อีกโปรไฟล์หนึ่ง (ที่มีเป้าหมายการสแกน วิธีการสแกน และพารามิเตอร์อื่นๆ) สำหรับแต่ละการสแกนที่ใช้เป็นประจำ

เมื่อต้องการสร้างโปรไฟล์ใหม่ ให้ไปที่ **ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > การป้องกัน > การสแกนคอมพิวเตอร์** และคลิก **แก้ไข...** ที่อยู่ถัดจากรายการโปรไฟล์ปัจจุบัน



เพื่อช่วยให้คุณสร้างโปรไฟล์การสแกนให้เหมาะสมกับความต้องการ โปรดดูคำอธิบายของพารามิเตอร์แต่ละรายการของการตั้งค่าการสแกนที่ส่วน การตั้งค่าพารามิเตอร์กลไก ThreatSense

ตัวอย่าง: สมมติว่าคุณต้องการสร้างโปรไฟล์การสแกนของคุณเอง และการกำหนดค่าการสแกนแบบสมาร์ทก็เหมาะสมเพียงบางส่วน แต่คุณไม่ต้องการสแกนรันไทม์แพ็คเกอร์หรือแอพพลิเคชันที่อาจไม่ปลอดภัย นอกจากนี้ คุณยังต้องการใช้การล้างอย่างเข้มงวดอีกด้วย ในหน้าต่าง **รายการโปรไฟล์ของเครื่องมือสแกนตามต้องการ** ให้พิมพ์ชื่อโปรไฟล์ แล้วคลิกปุ่ม **เพิ่ม** และยืนยันด้วยการคลิก **ตกลง** จากนั้นให้ปรับพารามิเตอร์เพื่อให้ตรงตามความต้องการของคุณ โดยตั้งค่า **กลไก ThreatSense** และ **เป้าหมายการสแกน**



การตั้งค่าพารามิเตอร์กลไก ThreatSense

ThreatSense เป็นเทคโนโลยีกรรมสิทธิ์ของ ESET ที่ประกอบไปด้วยวิธีการตรวจหาภัยคุกคามที่ซับซ้อนหลายรูปแบบร่วมกัน เทคโนโลยีนี้เป็นการป้องกันในเชิงรุก ซึ่งหมายความว่าจะมีการป้องกันตั้งแต่ช่วงต้นที่มีการแพร่กระจายของภัยคุกคามใหม่ เทคโนโลยีนี้จะใช้หลายวิธีร่วมกัน (การวิเคราะห์รหัส การจำลองรหัส ฐานข้อมูลทั่วไป ฐานข้อมูลไวรัส) ซึ่งทำงานร่วมกันอย่างสอดคล้อง เพื่อเพิ่มประสิทธิภาพของการรักษาความปลอดภัยให้กับระบบได้อย่างมาก กลไกการสแกนสามารถควบคุมสตรีมข้อมูลต่างๆ ได้พร้อมกัน ซึ่งเพิ่มประสิทธิภาพและอัตราการตรวจพบสูงสุด นอกจากนี้ เทคโนโลยี ThreatSense ยังช่วยล้างรูทคิทด้วย

ตัวเลือกการตั้งค่าของเทคโนโลยี ThreatSense ช่วยให้ผู้ใช้สามารถระบุพารามิเตอร์การสแกนต่างๆ ได้:

- ประเภทไฟล์และนามสกุลที่จะสแกน
- การใช้วิธีการตรวจหาต่างๆ ร่วมกัน
- ระดับการล้าง เป็นต้น

เมื่อต้องการเข้าสู่หน้าต่างการตั้งค่า ให้คลิก **ตั้งค่า > การป้องกันไวรัสและสปายแวร์ > ตั้งค่าการป้องกันไวรัสและสปายแวร์ขั้นสูง** แล้วคลิกปุ่ม **ตั้งค่า...** ที่อยู่ในสัญลักษณ์ **การป้องกันระบบ การป้องกันแบบเรียลไทม์** และ **การสแกนคอมพิวเตอร์** ซึ่งทั้งหมดใช้เทคโนโลยี ThreatSense (ดูด้านล่าง)

สถานการณ์การรักษาความปลอดภัยต่างกันอาจต้องใช้การกำหนดค่าที่ต่างกัน โปรดทราบว่า ThreatSense สามารถกำหนดค่าแยกกันได้สำหรับโมดูลการป้องกันต่อไปนี้:

- **การป้องกันระบบ >** การตรวจสอบไฟล์เมื่อเริ่มต้นอัตโนมัติ
- **การป้องกันแบบเรียลไทม์ >** การป้องกันระบบไฟล์แบบเรียลไทม์
- **การสแกนคอมพิวเตอร์ >** การสแกนคอมพิวเตอร์ตามต้องการ

พารามิเตอร์ ThreatSense มีการปรับให้เหมาะสำหรับแต่ละโมดูลโดยเฉพาะ และการแก้ไขเหล่านี้จะมีผลกับการทำงานของระบบมากด้วยเช่นกัน ตัวอย่างเช่น การเปลี่ยนการตั้งค่าเพื่อให้สแกนรันไทม์แพ็คเกอร์อยู่ตลอดเวลาหรือการเปิดใช้งานการวิเคราะห์พฤติกรรมขั้นสูงในโมดูลการป้องกันระบบไฟล์แบบเรียลไทม์อาจทำให้ระบบทำงานช้าลง ดังนั้น เราขอแนะนำให้คุณคงพารามิเตอร์ ThreatSense เริ่มต้นไว้สำหรับโมดูลทั้งหมด ยกเว้นการสแกนคอมพิวเตอร์

วัตถุ

ส่วน **วัตถุ** จะช่วยให้คุณสามารถกำหนดว่าจะสแกนหาการแฝงตัวจากไฟล์คอมพิวเตอร์ใด

- **ไฟล์ -** ให้การสแกนไฟล์ประเภทปกติทั้งหมด (โปรแกรม รูปภาพ เสียง ไฟล์วิดีโอ ไฟล์ฐานข้อมูล เป็นต้น)
- **ลิงค์สัญลักษณ์ -** (เครื่องมือการสแกนตามต้องการเท่านั้น)
  สแกนไฟล์ประเภทพิเศษที่มีสตริงข้อความที่ได้รับการตีความและตามด้วยระบบปฏิบัติการในฐานะที่เป็นพาธไปยังไฟล์หรือไดเรกทอรีอื่น
- **ไฟล์อีเมล -** (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) สแกนไฟล์พิเศษที่มีข้อความอีเมล

- **กล่องจดหมาย** - (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) สแกนกล่องจดหมายของผู้ใช้ในระบบ การใช้งานตัวเลือกนี้อย่างไม่ถูกต้องอาจทำให้เกิดข้อขัดแย้งกับอีเมลไคลเอ็นต์ของคุณ เมื่อต้องการเรียนรู้เพิ่มเติมเกี่ยวกับข้อดีและข้อเสียของตัวเลือกนี้ โปรดอ่าน บทความฐานความรู้ ต่อไปนี้
- **อาร์ไคฟ์** - (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) ให้การสแกนไฟล์ที่บีบอัดในอาร์ไคฟ์ (.rar, .zip, .arj, .tar เป็นต้น)
- **อาร์ไคฟ์ที่ขยายในตัว** - (ไม่สามารถใช้ได้ในการป้องกันแบบเรียลไทม์) สแกนไฟล์ที่อยู่ในไฟล์อาร์ไคฟ์ที่ขยายในตัว
- **รันไทม์แพ็คเกอร์** - แตกต่างจากอาร์ไคฟ์ประเภทมาตรฐาน รันไทม์แพ็คเกอร์จะขยายในหน่วยความจำ นอกเหนือจากแพ็คเกอร์คงที่แบบมาตรฐาน (UPX, yoda, ASPack, FGS เป็นต้น)

ตัวเลือก

ในส่วน **ตัวเลือก** คุณสามารถเลือกวิธีที่ใช้ระหว่างการสแกนระบบเพื่อหาการแฝงตัว ตัวเลือกที่ใช้ได้มีดังนี้:

- **ฐานข้อมูลไวรัส** - ฐานข้อมูลสามารถตรวจหาและระบุการแฝงตัวตามชื่อได้อย่างเชื่อถือได้ โดยใช้ฐานข้อมูลไวรัส
- **การวิเคราะห์พฤติกรรม** - การวิเคราะห์พฤติกรรมใช้อัลกอริทึมที่วิเคราะห์การทำงาน (ที่เป็นอันตราย) ของโปรแกรม
  ประโยชน์สำคัญของการตรวจหาการวิเคราะห์พฤติกรรมคือความสามารถในการตรวจหาซอฟต์แวร์ที่เป็นอันตรายใหม่ที่ไม่เคยมีมาก่อน หรือไม่อยู่ในรายการไวรัสที่รู้จัก (ฐานข้อมูลไวรัส)
- **การวิเคราะห์พฤติกรรมขั้นสูง** - การวิเคราะห์พฤติกรรมขั้นสูงประกอบด้วยอัลกอริทึมการวิเคราะห์พฤติกรรมที่ไม่ซ้ำกัน ที่พัฒนาโดย ESET มีการปรับปรุงประสิทธิภาพสำหรับการตรวจหาเวิร์มของคอมพิวเตอร์และม้าโทรจัน ซึ่งเขียนในภาษาที่ใช้เขียนโปรแกรมระดับสูง ความสามารถในการตรวจหาของโปรแกรมจะสูงขึ้นอย่างเห็นได้ชัดอันเนื่องมาจากการวิเคราะห์พฤติกรรมขั้นสูง
- **แอดแวร์/สปายแวร์/ริสก์แวร์** - ประเภทนี้รวมถึงซอฟต์แวร์ที่เก็บข้อมูลสำคัญเกี่ยวกับผู้ใช้โดยมิได้รับความยินยอม ประเภทนี้รวมถึงซอฟต์แวร์ที่แสดงเนื้อหาโฆษณาด้วย
- **แอพพลิเคชันที่อาจไม่พึงประสงค์** - แอพพลิเคชันเหล่านี้ไม่จำเป็นจะต้องเป็นอันตราย แต่อาจมีผลเสียกับประสิทธิภาพการทำงานของคอมพิวเตอร์ แอพพลิเคชันดังกล่าวมักจะขอให้มีการยินยอมก่อนติดตั้ง หากแอพพลิเคชันเหล่านี้ปรากฏบนคอมพิวเตอร์ของคุณ ระบบจะทำงานแตกต่างไป (เมื่อเทียบกับวิธีการทำงานก่อนการติดตั้งแอพพลิเคชันเหล่านี้) การเปลี่ยนแปลงที่สำคัญที่สุด ได้แก่ หน้าต่างป๊อปอัปที่ไม่พึงประสงค์ การเปิดใช้งานและการเรียกใช้กระบวนการที่ซ่อนอยู่ การใช้งานทรัพยากรระบบเพิ่มขึ้น การเปลี่ยนแปลงผลลัพธ์การค้นหา และการสื่อสารของแอพพลิเคชันกับเซิร์ฟเวอร์ระยะไกล
- **แอพพลิเคชันที่อาจไม่ปลอดภัย** - แอพพลิเคชันเหล่านี้จะอ้างอิงถึงซอฟต์แวร์เชิงพาณิชย์ที่ถูกต้อง ซึ่งอาจถูกละเมิดโดยนักโจมตี ถ้ามีการติดตั้งโดยผู้ใช้ที่ขาดความรู้ การจำแนกประเภทจะรวมถึงโปรแกรมต่างๆ เช่น เครื่องมือการเข้าถึงระยะไกล ซึ่งเป็นสาเหตุที่ทำให้มีการปิดใช้งานตัวเลือกนี้เป็นค่าเริ่มต้น

การกำจัด

การตั้งค่าการล้างจะเป็นตัวกำหนดรูปแบบที่เครื่องมือสแกนล้างไฟล์ที่ติดไวรัส การล้างมี 3 ระดับ:

- **ไม่มีการล้าง** - โปรแกรมจะไม่ล้างไฟล์ที่ติดไวรัสโดยอัตโนมัติ โปรแกรมจะแสดงหน้าต่างคำเตือน และช่วยให้คุณเลือกการดำเนินการ
- **การล้างมาตรฐาน** - โปรแกรมจะพยายามล้างหรือลบไฟล์ที่ติดไวรัสโดยอัตโนมัติ ถ้าไม่สามารถเลือกการดำเนินการที่ถูกต้องโดยอัตโนมัติ โปรแกรมจะเสนอตัวเลือกของการดำเนินการ ตัวเลือกของการดำเนินการจะปรากฏในกรณีที่ไม่สามารถดำเนินการตามที่กำหนดไว้ล่วงหน้าด้วย
- **การล้างอย่างเข้มงวด** - โปรแกรมจะล้างหรือลบไฟล์ที่ติดไวรัสทั้งหมด (รวมถึงอาร์ไคฟ์ด้วย) แต่จะยกเว้นไฟล์ของระบบ หากไม่สามารถล้างไฟล์ที่ติดไวรัส คุณจะมีตัวเลือกสำหรับการดำเนินการในหน้าต่างคำเตือน

คำเตือน: ในโหมดการล้างมาตรฐานที่เป็นค่าเริ่มต้น ไฟล์อาร์ไคฟ์ทั้งหมดจะถูกลบต่อเมื่อไฟล์ทั้งหมดในอาร์ไคฟ์ติดไวรัส ถ้าอาร์ไคฟ์มีไฟล์ที่ถูกต้องอยู่ โปรแกรมจะไม่ลบอาร์ไคฟ์ดังกล่าว หากตรวจพบไฟล์อาร์ไคฟ์ที่ติดไวรัสในโหมดการล้างอย่างเข้มงวด โปรแกรมจะลบทั้งอาร์ไคฟ์ แม้ว่าจะมีไฟล์ที่ไม่ติดไวรัสอยู่ก็ตาม

นามสกุล

นามสกุลเป็นส่วนหนึ่งของชื่อไฟล์ ซึ่งคั่นด้วยเครื่องหมายจุด นามสกุลจะกำหนดประเภทและเนื้อหาของไฟล์ ส่วนนี้ของการตั้งค่าพารามิเตอร์ ThreatSense จะช่วยให้คุณสามารถกำหนดประเภทไฟล์ที่จะยกเว้นจากการสแกน

โดยปกติแล้ว โปรแกรมจะสแกนไฟล์ทั้งหมดโดยไม่คำนึงถึงนามสกุลไฟล์ คุณสามารถเพิ่มนามสกุลในรายการไฟล์ที่จะยกเว้นจากการสแกน เมื่อใช้ปุ่ม **เพิ่ม** และ **ลบออก** คุณสามารถเปิดใช้หรือยกเว้นการสแกนนามสกุลที่ต้องการได้

ในบางครั้ง การยกเว้นไฟล์จากการสแกนจะเป็นสิ่งจำเป็น ถ้าประเภทไฟล์บางประเภทของการสแกนป้องกันโปรแกรมเพื่อไม่ให้ทำงานอย่างถูกต้อง ตัวอย่างเช่น ขอแนะนำให้ยกเว้นนามสกุล *.log*, *.cfg* และ *.tmp*

ขีดจำกัด

ส่วน **ขีดจำกัด** ช่วยให้คุณสามารถระบุขนาดสูงสุดของวัตถุ และระดับของอาร์ไคฟ์ที่ซ้อนที่จะสแกน:

- **ขนาดสูงสุด:** กำหนดขนาดสูงสุดของวัตถุที่จะสแกน โมดูลป้องกันไวรัสจะสแกนเฉพาะวัตถุที่เล็กกว่าขนาดที่ระบุเท่านั้น เราไม่แนะนำให้แก้ไขค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดๆ ที่จะต้องแก้ไขค่านี้ ผู้ที่สามารถแก้ไขตัวเลือกนี้ควรเป็นผู้ใช้ขั้นสูง ซึ่งมีเหตุผลบางอย่างสำหรับการยกเว้นวัตถุขนาดใหญ่จากการสแกน
- **เวลาสแกนสูงสุด:** กำหนดค่าเวลาสูงสุดสำหรับการสแกนวัตถุ หากมีการป้อนค่าที่ผู้ใช้กำหนดไว้ โมดูลป้องกันไวรัสจะหยุดสแกนวัตถุเมื่อพ้นระยะเวลาดังกล่าว ไม่ว่าการสแกนจะเสร็จสิ้นแล้วหรือไม่
- **ระดับการซ้อนสูงสุด:** ระบุความลึกสูงสุดของการสแกนอาร์ไคฟ์ เราไม่แนะนำให้แก้ไขค่า 10 ซึ่งเป็นค่าเริ่มต้น เนื่องจากไม่มีเหตุผลใดที่จะต้องแก้ไขค่านี้ในสถานการณ์ปกติ หากการสแกนสิ้นสุดลงก่อนกำหนด เนื่องจากจำนวนอาร์ไคฟ์ที่ซ้อนกัน อาร์ไคฟ์จะไม่ได้รับการตรวจสอบ
- **ขนาดไฟล์สูงสุด:** ตัวเลือกนี้ช่วยให้คุณสามารถระบุขนาดไฟล์สูงสุดสำหรับไฟล์ที่อยู่ในอาร์ไคฟ์ (เมื่อดึงข้อมูล) ที่จะสแกน ถ้าการสแกนสิ้นสุดก่อนกำหนดด้วยผลของขีดจำกัดนี้ อาร์ไคฟ์จะไม่ได้รับการตรวจสอบ

อื่นๆ

เมื่อเปิดใช้การเพิ่มประสิทธิภาพแบบสมาร์ท ระบบจะใช้การตั้งค่าที่มีประสิทธิภาพสูงสุดเพื่อให้ระดับการสแกนมีประสิทธิภาพสูงสุด และรักษาความเร็วในการสแกนสูงสุดไว้พร้อมกันด้วย โมดูลการป้องกันต่างๆ จะสแกนข้อมูลอย่างชาญฉลาด โดยใช้ประโยชน์จากวิธีการสแกนต่างๆ ในขณะที่นำมาใช้งานกับประเภทไฟล์ที่ระบุ

การเพิ่มประสิทธิภาพแบบสมาร์ทจะไม่ได้กำหนดไว้อย่างแน่ชัดภายในผลิตภัณฑ์ ทีมพัฒนา ESET จะคงใช้งานการเปลี่ยนแปลงใหม่ๆ อย่างต่อเนื่อง ซึ่งจะนำมารวมกับ ESET NOD32 Antivirus ผ่านการอัพเดทเป็นประจำ ถ้าปิดใช้การเพิ่มประสิทธิภาพแบบสมาร์ท ระบบจะใช้เฉพาะการตั้งค่าที่ผู้ใช้กำหนดในกลไก ThreatSense ของโมดูลเมื่อดำเนินการสแกน

สแกนสตรีมข้อมูลสำรอง (เฉพาะเครื่องสแกนตามต้องการเท่านั้น)

สตรีมข้อมูลสำรอง (การแยกทรัพยากร/ข้อมูล) ที่ใช้งานโดยระบบไฟล์เป็นการเชื่อมโยงไฟล์และโฟลเดอร์ซึ่งจะไม่ปรากฏสำหรับเทคนิคการสแกนทั่วไป การแฝงตัวจำนวนมากพยายามหลีกเลี่ยงการตรวจสอบนี้ โดยปลอมแปลงตัวเองเป็นสตรีมข้อมูลสำรอง

ตรวจพบการแฝงตัว

การแฝงตัวสามารถเข้าสู่ระบบได้จากจุดเข้าใช้ต่างๆ เช่น หน้าเว็บ โฟลเดอร์ที่ใช้ร่วมกัน อีเมล หรือจากอุปกรณ์คอมพิวเตอร์ที่ถอดเข้าออกได้ (USB, ดิสก์ภายนอก, ซีดี, ดีวีดี, ดิสเก็ตต์ เป็นต้น)

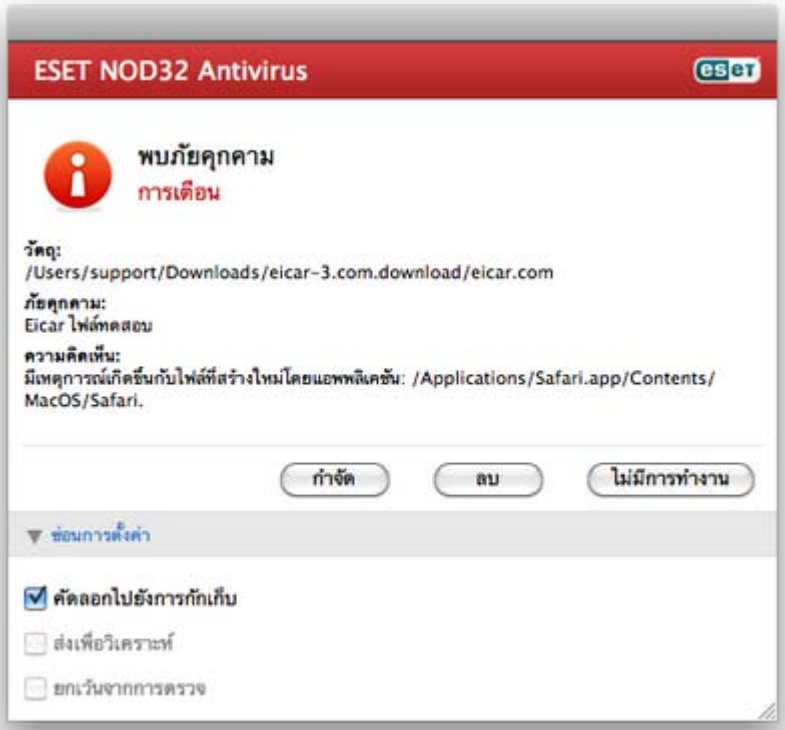
ถ้าคอมพิวเตอร์ของคุณแสดงสัญญาณการติดไวรัสจากมัลแวร์ เช่น ทำงานช้า ค้างบ่อยๆ เป็นต้น เราขอแนะนำให้ดำเนินการตามขั้นตอนต่อไปนี้:

1. เปิด ESET NOD32 Antivirus และคลิก **การสแกนคอมพิวเตอร์**
2. คลิก **การสแกนแบบสมาร์ท** (สำหรับข้อมูลเพิ่มเติม โปรดดูส่วน การสแกนแบบสมาร์ท)
3. หลังจากสแกนเสร็จสิ้นแล้ว ให้ตรวจดูบันทึกสำหรับจำนวนไฟล์ที่สแกน ไฟล์ที่ติดไวรัส และไฟล์ที่ล้าง

หากคุณต้องการสแกนเฉพาะบางส่วนของดิสก์ ให้คลิก **การสแกนที่กำหนดเอง** และเลือกเป้าหมายที่จะสแกนหาไวรัส

ต่อไปนี้เป็นตัวอย่างทั่วไปสำหรับวิธีจัดการกับการแฝงตัวใน ESET NOD32 Antivirus สมมติว่าการแฝงตัวถูกตรวจพบโดยการตรวจสอบระบบไฟล์แบบเรียลไทม์ ซึ่งใช้ระดับการล้างเริ่มต้น โปรแกรมจะพยายามล้างหรือลบไฟล์ หากไม่มีการดำเนินการที่กำหนดไว้ล่วงหน้าสำหรับโมดูลการป้องกันแบบเรียลไทม์ ระบบจะให้คุณเลือกตัวเลือกในหน้าต่างการเตือน โดยทั่วไปแล้วจะมีตัวเลือก **ล้าง, ลบ** และ **ไม่มีการทำงาน** ไม่แนะนำให้เลือก **ไม่มีการทำงาน** เนื่องจากไฟล์ที่ติดไวรัสจะคงอยู่โดยไม่มีการแก้ไข ข้อยกเว้นคือ เมื่อคุณแน่ใจว่าไฟล์ดังกล่าวไม่มีอันตราย และตรวจพบผิดพลาดว่ามีไวรัส

การล้างและการลบ ใช้การล้างถ้าไฟล์ถูกโจมตีโดยไวรัส ซึ่งทำให้มีการแนบรหัสที่เป็นอันตรายกับไฟล์นั้น ในกรณีนี้ ขั้นแรกให้พยายามล้างไฟล์ที่ติดเชื้อ เพื่อคืนกลับสู่สภาวะเดิม ถ้าไฟล์มีเฉพาะรหัสที่เป็นอันตราย ไฟล์ดังกล่าวจะถูกลบ



การลบไฟล์ในอาร์ไคฟ์ ในโหมดการล้างเริ่มต้น ระบบจะลบทั้งอาร์ไคฟ์ต่อเมื่อมีไฟล์ที่ติดไวรัส และไม่มีไฟล์ที่ปลอดไวรัสเลย กล่าวอีกนัยหนึ่งก็คือ โปรแกรมจะไม่ลบอาร์ไคฟ์ ถ้ายังมีไฟล์ที่ไม่เป็นอันตรายรวมอยู่ด้วย อย่างไรก็ตาม โปรดใช้ความระมัดระวังเมื่อสแกน **การล้างอย่างเข้มงวด** เนื่องจากเมื่อใช้การล้างอย่างเข้มงวด โปรแกรมจะลบอาร์ไคฟ์แม้ว่าจะมีไฟล์ที่ติดไวรัสเพียงไฟล์เดียวก็ตาม โดยไม่คำนึงถึงสถานะของไฟล์อื่นๆ ในอาร์ไคฟ์

การอัพเดทโปรแกรม

การอัพเดท ESET NOD32 Antivirus เป็นประจำเป็นสิ่งจำเป็นเพื่อรักษาระดับการรักษาความปลอดภัยสูงสุด โมดูลการอัพเดทจะดำเนินการให้มั่นใจว่าโปรแกรมนั้นมีความทันสมัยอยู่เสมอโดยการดาวน์โหลดฐานข้อมูลไวรัสล่าสุด

เมื่อคลิก **อัพเดท** จากเมนูหลัก คุณจะพบสถานะการอัพเดทในปัจจุบัน รวมถึงวันที่และเวลาของการอัพเดทที่สำเร็จครั้งล่าสุด และดูว่าจะต้องมีการอัพเดทหรือไม่ เมื่อต้องการเริ่มต้นกระบวนการอัพเดทด้วยตนเอง ให้คลิก **อัพเดทฐานข้อมูลไวรัส**

ภายใต้สภาวะปกติ เมื่อดาวน์โหลดการอัพเดทอย่างถูกต้องแล้ว ข้อความ **ฐานข้อมูลไวรัสอัพเดทแล้ว** จะปรากฏในหน้าต่างการอัพเดท ถ้าฐานข้อมูลไวรัสไม่สามารถอัพเดทได้ เราขอแนะนำให้คุณตรวจสอบ การตั้งค่าการอัพเดท - สาเหตุทั่วไปส่วนใหญ่สำหรับข้อผิดพลาดนี้คือข้อมูลการตรวจสอบสิทธิ์ที่ป้อนไม่ถูกต้อง (ชื่อผู้ใช้และรหัสผ่าน) หรือกำหนดค่าไม่ถูกต้อง การตั้งค่าการเชื่อมต่อ

หน้าต่างการอัพเดทจะมีข้อมูลเกี่ยวกับเวอร์ชันของฐานข้อมูลไวรัสด้วย สัญลักษณ์ที่เป็นตัวเลขนี้คือลิงค์ไปยังเว็บไซต์ของ ESET ซึ่งจะแสดงรายการฐานข้อมูลทั้งหมดที่เพิ่มไว้ภายในวันที่ที่กำหนด

หมายเหตุ: ESET จะให้ชื่อผู้ใช้และรหัสผ่านหลังจากการซื้อ ESET NOD32 Antivirus

การอัพเกรดเป็นรุ่นใหม่

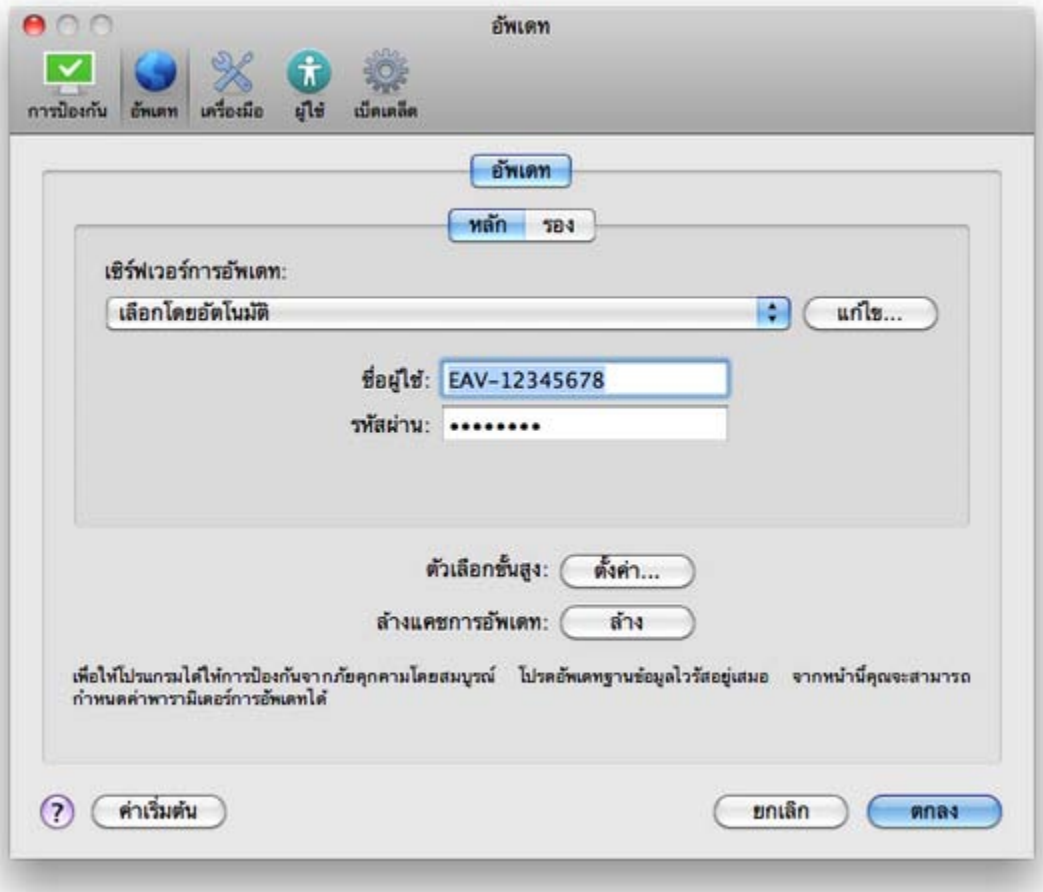
เพื่อให้มีการป้องกันสูงสุด สิ่งสำคัญคือจะต้องใช้ ESET NOD32 Antivirus รุ่นล่าสุด เมื่อต้องการตรวจสอบเวอร์ชันใหม่ ให้คลิก **อัพเดท** จากเมนูหลักทางด้านซ้าย ถ้ามีรุ่นใหม่ ข้อความ *สามารถใช้เวอร์ชันใหม่ของผลิตภัณฑ์นี้ได้แล้ว!* จะปรากฏที่ด้านล่างของหน้าต่าง คลิก **เรียนรู้เพิ่มเติม...** เพื่อแสดงหน้าต่างใหม่ที่มีหมายเลขเวอร์ชันของรุ่นใหม่และบันทึกการเปลี่ยนแปลง

คลิก **ดาวน์โหลด** เพื่อดาวน์โหลดรุ่นใหม่ล่าสุด คลิก **ปิด** เพื่อปิดหน้าต่างและดาวน์โหลดการอัพเกรดในภายหลัง

ถ้าคุณคลิก **ดาวน์โหลด** ไฟล์จะถูกดาวน์โหลดไปยังโฟลเดอร์การดาวน์โหลดของคุณ (หรือโฟลเดอร์เริ่มต้นที่ตั้งขึ้นโดยเบราว์เซอร์ของคุณ) เมื่อเสร็จสิ้นการดาวน์โหลดไฟล์ ให้เริ่มต้นไฟล์และดำเนินการตามคำแนะนำการติดตั้ง ชื่อผู้ใช้และรหัสผ่านจะถูกโอนไปยังการติดตั้งใหม่โดยอัตโนมัติ ขอแนะนำให้ตรวจสอบการอัพเกรดเป็นประจำ โดยเฉพาะเมื่อติดตั้ง ESET NOD32 Antivirus ผ่านซีดี/ดีวีดี

การตั้งค่าการอัพเดท

ส่วนการตั้งค่าการอัพเดทจะระบุข้อมูลที่มาของการอัพเดท เช่น เซิร์ฟเวอร์การอัพเดทและข้อมูลการตรวจสอบสิทธิ์สำหรับเซิร์ฟเวอร์เหล่านี้ ตามค่าเริ่มต้น เมนูแบบเลื่อนลง **เซิร์ฟเวอร์การอัพเดท** จะถูกตั้งค่าเป็น **เลือกโดยอัตโนมัติ** เพื่อให้แน่ใจว่าไฟล์การอัพเดทจะดาวน์โหลดโดยอัตโนมัติจากเซิร์ฟเวอร์ของ ESET โดยมีการรับส่งในเครือข่ายน้อยที่สุด



รายการของเซิร์ฟเวอร์การอัพเดทที่ใช้ได้จะสามารถเข้าถึงได้ผ่านเมนูแบบเลื่อนลง **เซิร์ฟเวอร์การอัพเดท** เมื่อต้องการเพิ่มเซิร์ฟเวอร์การอัพเดทใหม่ ให้คลิก **แก้ไข...** จากนั้นให้ป้อนที่อยู่ของเซิร์ฟเวอร์ใหม่ในฟิลด์ป้อนข้อมูล **เซิร์ฟเวอร์การอัพเดท** และคลิกปุ่ม **เพิ่ม** การตรวจสอบสิทธิ์สำหรับเซิร์ฟเวอร์การอัพเดทจะขึ้นอยู่กับ **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่สร้างขึ้นและส่งให้กับคุณหลังจากการซื้อ

เมื่อต้องการเปิดใช้งานโหมดทดสอบ (การอัพเดทก่อนออกของการดาวน์โหลด) ให้คลิกปุ่ม **ตั้งค่า...** ที่อยู่ถัดจาก **ตัวเลือกขั้นสูง** และเลือกช่องทำเครื่องหมาย **เปิดใช้งานการอัพเดทก่อนออก** เมื่อต้องการปิดใช้งานการแจ้งเตือนของถาดข้อมูลของระบบที่ปรากฏหลังจากการอัพเดทสำเร็จแต่ละครั้ง ให้เลือกช่องทำเครื่องหมาย **ไม่แสดงการแจ้งเตือนเกี่ยวกับอัพเดทที่สำเร็จ**

เมื่อต้องการลบข้อมูลการอัพเดทที่เก็บไว้ชั่วคราวทั้งหมด ให้คลิกปุ่ม **ล้าง** ที่อยู่ถัดจาก **ล้างแคชการอัพเดท** ใช้ตัวเลือกนี้ถ้าคุณพบปัญหาในระหว่างการอัพเดท

วิธีสร้างงานการอัพเดท

คุณสามารถเรียกการอัพเดทได้ด้วยตนเองโดยคลิก **อัพเดทฐานข้อมูลไวรัส** ในหน้าต่างหลักที่ปรากฏหลังจากคลิก **อัพเดท** จากเมนูหลัก

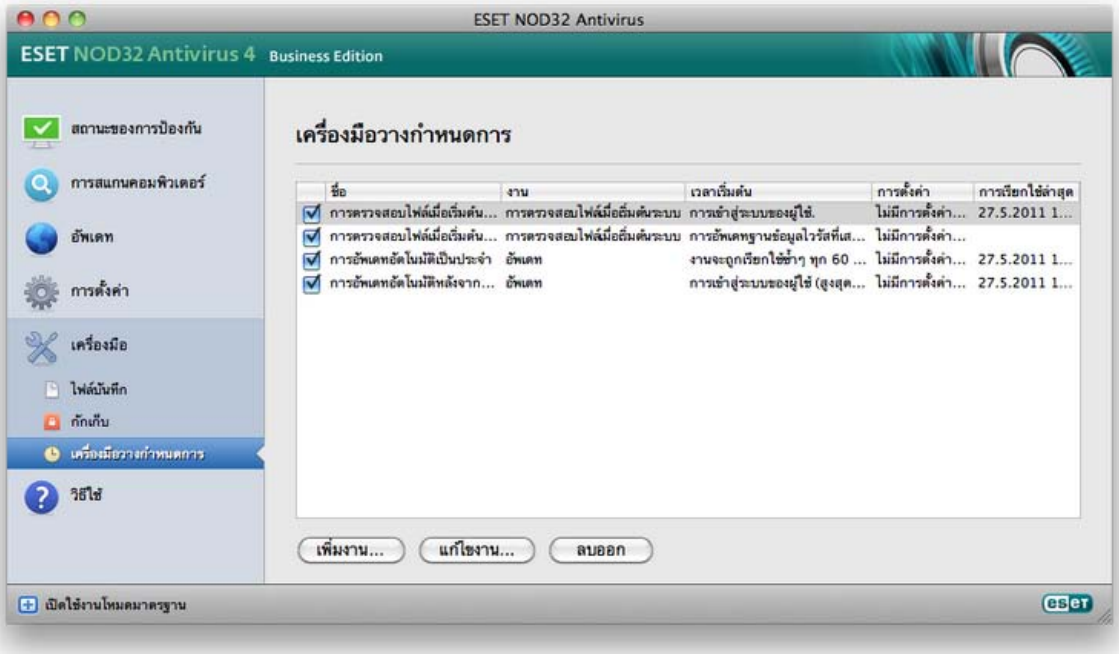
การอัพเดทสามารถเรียกใช้เป็นงานตามกำหนดการ เมื่อต้องการกำหนดค่างานตามกำหนดการ ให้คลิก **เครื่องมือ > เครื่องมือวางกำหนดการ** ตามค่าเริ่มต้น งานต่อไปนี้จะเปิดใช้ใน ESET NOD32 Antivirus:

- **การอัพเดทอัตโนมัติเป็นประจำ**
- **การอัพเดทอัตโนมัติหลังจากผู้ใช้เข้าสู่ระบบ**

งานการอัพเดทแต่ละงานจะสามารถแก้ไขได้เพื่อให้เหมาะกับความต้องการของคุณ นอกเหนือจากงานการอัพเดทเริ่มต้นแล้ว คุณสามารถสร้างงานการอัพเดทใหม่ด้วยการกำหนดค่าที่ผู้ใช้กำหนดได้ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการสร้างและการกำหนดค่างานการอัพเดท โปรดดูที่ส่วน เครื่องมือวางกำหนดการ

เครื่องมือวางกำหนดการ

เครื่องมือวางกำหนดการ จะสามารถใช้ได้ถ้ามีการเปิดใช้งานโหมดขั้นสูงใน ESET NOD32 Antivirus เครื่องมือวางกำหนดการสามารถพบได้ในเมนูหลักของ ESET NOD32 Antivirus ภายใต้ **เครื่องมือ เครื่องมือวางกำหนดการ** มีรายการงานตามกำหนดการทั้งหมด และคุณสมบัติของการกำหนดค่า เช่น วันที่ที่กำหนดไว้ล่วงหน้า เวลา และโปรไฟล์การสแกนที่ใช้



ตามค่าเริ่มต้น งานตามกำหนดการต่อไปนี้จะปรากฏในเครื่องมือวางกำหนดการ:

- การอัพเดทอัตโนมัติเป็นประจำ
- การอัพเดทอัตโนมัติหลังจากผู้ใช้เข้าสู่ระบบ
- การตรวจสอบไฟล์เมื่อเริ่มต้นอัตโนมัติหลังจากการเข้าสู่ระบบของผู้ใช้
- การตรวจสอบไฟล์เมื่อเริ่มต้นอัตโนมัติหลังจากการอัพเดทฐานข้อมูลไวรัสที่เสร็จสมบูรณ์
- การบำรุงรักษาบันทึก (หลังจากเปิดใช้งานตัวเลือก **แสดงงานของระบบ** ในการตั้งค่าเครื่องมือวางกำหนดการ)

เมื่อต้องการแก้ไขการกำหนดค่าของงานตามกำหนดการที่มีอยู่ (ทั้งค่าเริ่มต้นและที่ผู้ใช้กำหนด) ให้คลิกขวาที่งานและคลิก **แก้ไข...** หรือเลือกงานที่คุณต้องการแก้ไขและคลิกปุ่ม **แก้ไข...**

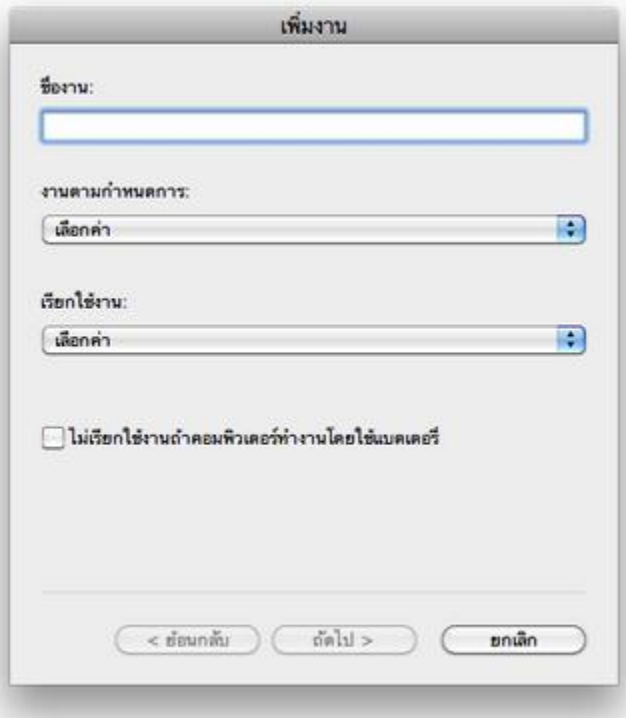
วัตถุประสงค์ของการวางกำหนดการงาน

เครื่องมือวางกำหนดการจะจัดการและเรียกใช้งานตามกำหนดการโดยใช้การกำหนดค่าและคุณสมบัติที่กำหนดไว้ล่วงหน้า การกำหนดค่าและคุณสมบัติจะมีข้อมูลต่างๆ เช่น วันที่และเวลา ตลอดจนโปรไฟล์ที่ระบุให้ใช้ระหว่างการเรียกใช้งาน

การสร้างงานใหม่

เมื่อต้องการสร้างงานใหม่ในเครื่องมือวางกำหนดการ ให้คลิกปุ่ม **เพิ่มงาน...** หรือคลิกขวาและเลือก **เพิ่ม...** จากเมนูบริบท งานตามกำหนดการที่ใช้ได้มีห้าประเภท:

- **เรียกใช้แอปพลิเคชัน**
- **อัพเดท**
- **การบำรุงรักษาการบันทึก**
- **การสแกนคอมพิวเตอร์ตามต้องการ**
- **การตรวจสอบไฟล์เมื่อเริ่มต้นระบบ**



เนื่องจากการอัพเดทเป็นงานตามกำหนดการที่ใช้บ่อยที่สุดงานหนึ่ง ดังนั้นเราจะอธิบายวิธีเพิ่มงานการอัพเดทใหม่

จากเมนูแบบเลื่อนลง **งานตามกำหนดการ** ให้เลือก **อัพเดท** ป้อนชื่อของงานลงในฟิลด์ **ชื่องาน** เลือกความถี่ของงานจากเมนูแบบเลื่อนลง **เรียกใช้งาน** ตัวเลือกที่ใช้ได้มีดังนี้: **ผู้ใช้กำหนด หนึ่งครั้ง ซ้ำ รายวัน รายสัปดาห์** และ **ตามเหตุการณ์** คุณจะได้รับพรอมต์ที่มีพารามิเตอร์การอัพเดทที่แตกต่างกัน ทั้งนี้จะขึ้นอยู่กับความถี่ที่เลือก ขั้นตอนถัดไป ให้กำหนดการทำงานที่ต้องการถ้าไม่สามารถดำเนินการกับงานหรือทำงานให้สำเร็จตามเวลาในกำหนดการ สามารถใช้ตัวเลือกสามตัวเลือกต่อไปนี้:

- **รอจนถึงเวลาตามกำหนดการครั้งถัดไป**
- **เรียกใช้งานเร็วที่สุดเท่าที่ทำได้**
- **เรียกใช้งานทันที ถ้าเวลานับจากการเรียกใช้ครั้งล่าสุดเกินจากช่วงเวลาที่ระบุ** (สามารถกำหนดระยะเวลาได้โดยใช้ตัวเลือก **ช่วงเวลาต่ำสุดของงาน**)

ในขั้นตอนถัดไป หน้าต่างข้อมูลสรุปพร้อมข้อมูลเกี่ยวกับงานตามกำหนดการในปัจจุบันจะปรากฏขึ้น คลิกที่ปุ่ม **สิ้นสุด**

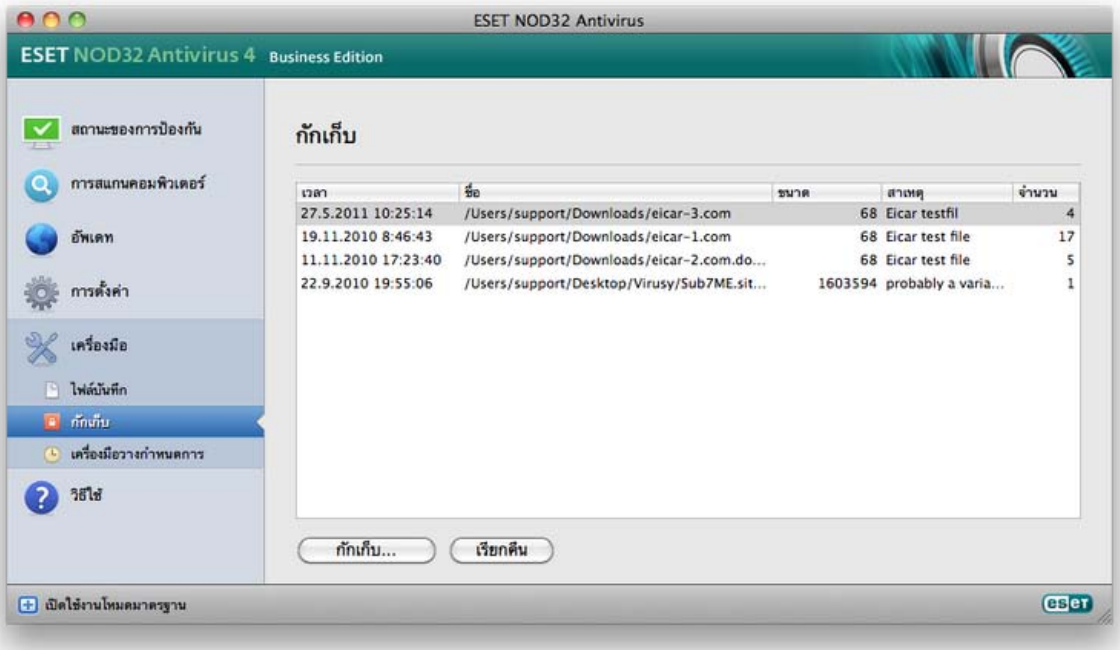
งานตามกำหนดการใหม่จะถูกเพิ่มในรายการของงานตามกำหนดการปัจจุบัน

ตามค่าเริ่มต้น ระบบจะมีงานตามกำหนดการที่มีความสำคัญ เพื่อให้มีการทำงานอย่างถูกต้อง งานเหล่านี้ไม่ควรมีการแก้ไขและจะถูกซ่อนตามค่าเริ่มต้น เมื่อต้องการเปลี่ยนตัวเลือกนี้และกำหนดให้มองเห็นงานได้ ให้เข้าสู่ **ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > เครื่องมือ > เครื่องมือวางกำหนดการ** และเลือกตัวเลือก **แสดงงานของระบบ**

กักเก็บ

หน้าที่หลักของการกักเก็บก็คือการเก็บไฟล์ที่ติดไวรัสไว้ในที่ปลอดภัย ไฟล์ควรมีการกักเก็บถ้าไม่สามารถล้างไวรัสได้ ถ้าไม่ปลอดภัยหรือไม่ควรลบไฟล์เหล่านี้ หรือถ้ามีการตรวจพบด้วยความผิดพลาดโดย ESET NOD32 Antivirus

คุณสามารถเลือกที่จะกักเก็บไฟล์ได้ ซึ่งเป็นตัวเลือกที่แนะนำ ถ้าไฟล์ทำงานน่าสงสัยแต่ไม่มีการตรวจพบโดยเครื่องมือสแกนป้องกันไวรัส ไฟล์ที่ถูกกักเก็บจะสามารถส่งเพื่อรับการวิเคราะห์ที่แล็บภัยคุกคามของ ESET



ไฟล์ที่เก็บไว้ในโฟลเดอร์การกักเก็บนั้นสามารถดูได้ในตารางที่แสดงวันที่และเวลาของการกักเก็บ พาธไปยังตำแหน่งดั้งเดิมของไฟล์ที่ติดไวรัส ขนาดเป็นไบต์ สาเหตุ (เช่น เพิ่มโดยผู้ใช้...) และจำนวนภัยคุกคาม (เช่น ถ้าเป็นอาร์ไคฟ์ที่มีการแฝงตัวหลายรายการ) โฟลเดอร์การกักเก็บที่มีไฟล์ที่กักเก็บ (*/Library/Application Support/Eset/cache/esets/quarantine*) จะอยู่ในระบบแม้ว่าจะถอนการติดตั้ง ESET NOD32 Antivirus แล้ว ไฟล์ที่กักเก็บจะถูกเก็บไว้ในรูปแบบที่เข้ารหัสที่ปลอดภัย และสามารถเรียกคืนได้อีกครั้งหลังจากติดตั้ง ESET NOD32 Antivirus

การกักเก็บไฟล์

ESET NOD32 Antivirus จะกักเก็บไฟล์ที่ถูกลบให้โดยอัตโนมัติ (ถ้าคุณไม่ยกเลิกตัวเลือกนี้ในหน้าต่างการเตือน) คุณสามารถกักเก็บไฟล์ที่น่าสงสัยได้ด้วยตนเอง ถ้าต้องการโดยคลิกปุ่ม **กักเก็บ...** เมนูบริบทสามารถใช้สำหรับวัตถุประสงค์นี้ได้เช่นกัน ให้คลิกขวาในหน้าต่าง **กักเก็บ** เลือกไฟล์ที่คุณต้องการกักเก็บและคลิกปุ่ม **เปิด**

การเรียกคืนจากการกักเก็บ

ไฟล์ที่กักเก็บสามารถเรียกคืนไปยังตำแหน่งเดิมได้ ใช้ปุ่ม **เรียกคืน** สำหรับวัตถุประสงค์นี้ การเรียกคืนจะสามารถใช้ได้จากเมนูบริบท โดยคลิกขวาที่ไฟล์ที่มีให้ในหน้าต่าง **กักเก็บ** แล้วคลิก **เรียกคืน** นอกจากนี้เมนูบริบทยังมีตัวเลือก **เรียกคืนไปที่...** ซึ่งช่วยให้คุณสามารถเรียกคืนไฟล์ไปยังตำแหน่งอื่นนอกเหนือจากตำแหน่งที่ถูกลบได้

การส่งไฟล์จากการกักเก็บ

ถ้าคุณได้กักเก็บไฟล์ที่น่าสงสัยที่ไม่ได้ตรวจพบโดยโปรแกรม หรือถ้าไฟล์ถูกประเมินว่าติดไวรัสโดยไม่ถูกต้อง (เช่น โดยการวิเคราะห์พฤติกรรมของรหัส) และมีการกักเก็บหลังจากนั้น โปรดส่งไฟล์ไปยังแล็บภัยคุกคามของ ESET ถ้าต้องการส่งไฟล์จากการกักเก็บ ให้คลิกขวาที่ไฟล์และเลือก **ส่งไฟล์เพื่อวิเคราะห์** จากเมนูบริบท

ไฟล์บันทึก

ไฟล์บันทึกประกอบด้วยข้อมูลเกี่ยวกับเหตุการณ์ของโปรแกรมที่สำคัญที่เกิดขึ้นทั้งหมด และให้ภาพรวมของภัยคุกคามที่พบ การบันทึกทำหน้าที่เป็นเครื่องมือที่จำเป็นในการวิเคราะห์ระบบ การตรวจหาภัยคุกคาม และการแก้ไขปัญหา การบันทึกนั้นดำเนินการในพื้นหลังโดยที่ผู้ใช้ไม่ต้องดำเนินการใดๆ ข้อมูลจะถูกบันทึกตามการตั้งค่าความละเอียดของการบันทึกปัจจุบัน ผู้ใช้สามารถดูข้อความและบันทึกได้โดยตรงจากระบบ ESET NOD32 Antivirus และสามารถอาร์ไคฟ์การบันทึกได้

ไฟล์บันทึกนั้นสามารถเข้าถึงได้จากเมนูหลักของ ESET NOD32 Antivirus โดยคลิก **เครื่องมือ > ไฟล์บันทึก** เลือกประเภทการบันทึกที่ต้องการโดยใช้เมนูแบบเลื่อนลง **บันทึก** ที่ด้านบนของหน้าต่าง มีบันทึกที่ใช้ได้ดังต่อไปนี้:

1. **ภัยคุกคามที่พบ** - ใช้ตัวเลือกนี้เพื่อดูข้อมูลทั้งหมดเกี่ยวกับเหตุการณ์ที่เกี่ยวข้องกับการตรวจหาการแฝงตัว
2. **เหตุการณ์** - ตัวเลือกนี้ได้รับการออกแบบมาสำหรับผู้ดูแลระบบและผู้ใช้เพื่อแก้ไขปัญหา การทำงานที่สำคัญทั้งหมด ซึ่งดำเนินการโดย ESET NOD32 Antivirus จะได้รับการบันทึกไว้ในบันทึกเหตุการณ์
3. **การสแกนคอมพิวเตอร์** - ผลลัพธ์ของการสแกนที่เสร็จสมบูรณ์ทั้งหมดจะปรากฏในหน้าต่างนี้ คลิกสองครั้งที่รายการใดก็ได้เพื่อดูรายละเอียดของการสแกนคอมพิวเตอร์ตามต้องการตามลำดับ

ในแต่ละส่วน ข้อมูลที่ปรากฏจะสามารถคัดลอกไปยังคลิปบอร์ดได้โดยตรง โดยเลือกรายการและคลิกที่ปุ่ม **คัดลอก**

การบำรุงรักษาการบันทึก

การกำหนดค่าการบันทึกสำหรับ ESET NOD32 Antivirus สามารถเข้าถึงได้จากหน้าต่างหลักของโปรแกรม คลิก **ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > เครื่องมือ > ไฟล์บันทึก** คุณสามารถระบุตัวเลือกต่อไปนี้สำหรับไฟล์บันทึก:

- **ลบบันทึกโดยอัตโนมัติ** - รายการบันทึกที่เก่ากว่าจำนวนวันที่ระบุจะถูกลบโดยอัตโนมัติ
- **ปรับปรุงประสิทธิภาพไฟล์บันทึกโดยอัตโนมัติ** - เปิดใช้งานการจัดระเบียบใหม่โดยอัตโนมัติสำหรับไฟล์บันทึก ถ้ามีบันทึกที่ไม่ได้ใช้เกินจำนวนเปอร์เซ็นต์ที่ระบุ

เมื่อต้องการกำหนดค่า **ตัวกรองเริ่มต้นของรายการบันทึก** ให้คลิกปุ่ม **แก้ไข...** และเลือก/ยกเลิกการเลือกประเภทการบันทึกตามต้องการ

การกรองบันทึก

บันทึกจะเก็บข้อมูลเกี่ยวกับเหตุการณ์ของระบบที่มีความสำคัญ คุณลักษณะการกรองบันทึกช่วยให้คุณแสดงบันทึกเกี่ยวกับเหตุการณ์ประเภทที่ระบุ

ประเภทของบันทึกที่ใช้บ่อยมีดังนี้

- **คำเตือนที่ร้ายแรง** - ข้อผิดพลาดของระบบที่ร้ายแรง (เช่น การป้องกันไวรัสไม่เริ่มต้นทำงาน)
- **ข้อผิดพลาด** - ข้อความแสดงข้อผิดพลาด เช่น "*เกิดข้อผิดพลาดขณะดาวน์โหลดไฟล์*" และข้อผิดพลาดร้ายแรง
- **คำเตือน** - ข้อความแสดงคำเตือน
- **บันทึกเพื่อแจ้งข้อมูล**- ข้อความแจ้งข้อมูล รวมถึงการอัพเดทที่เสร็จสมบูรณ์ การเตือน เป็นต้น
- **บันทึกเพื่อการวินิจฉัย** - ข้อมูลที่จำเป็นสำหรับการปรับแต่งโปรแกรมและการบันทึกทั้งหมดที่อธิบายไว้ที่ด้านบน

ส่วนติดต่อผู้ใช้

ตัวเลือกการกำหนดค่าส่วนติดต่อผู้ใช้ใน ESET NOD32 Antivirus จะช่วยให้คุณสามารถปรับระบบการทำงานเพื่อให้เหมาะกับความต้องการของคุณ
ตัวเลือกการกำหนดค่าเหล่านี้สามารถเข้าถึงได้จาก **ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > ผู้ใช้ > ส่วนติดต่อ**

ในส่วนนี้ ตัวเลือกโหมดขั้นสูงจะให้ผู้ใช้สามารถสลับไปยังโหมดขั้นสูงได้ โหมดขั้นสูงจะแสดงการตั้งค่าโดยละเอียดมากขึ้นและการควบคุมเพิ่มเติมสำหรับ ESET NOD32 Antivirus

เมื่อต้องการเปิดใช้งานฟังก์ชันหน้าจอเริ่มต้นเมื่อเริ่มระบบ ให้เลือก **แสดงหน้าจอเริ่มต้นเมื่อเริ่มระบบ**

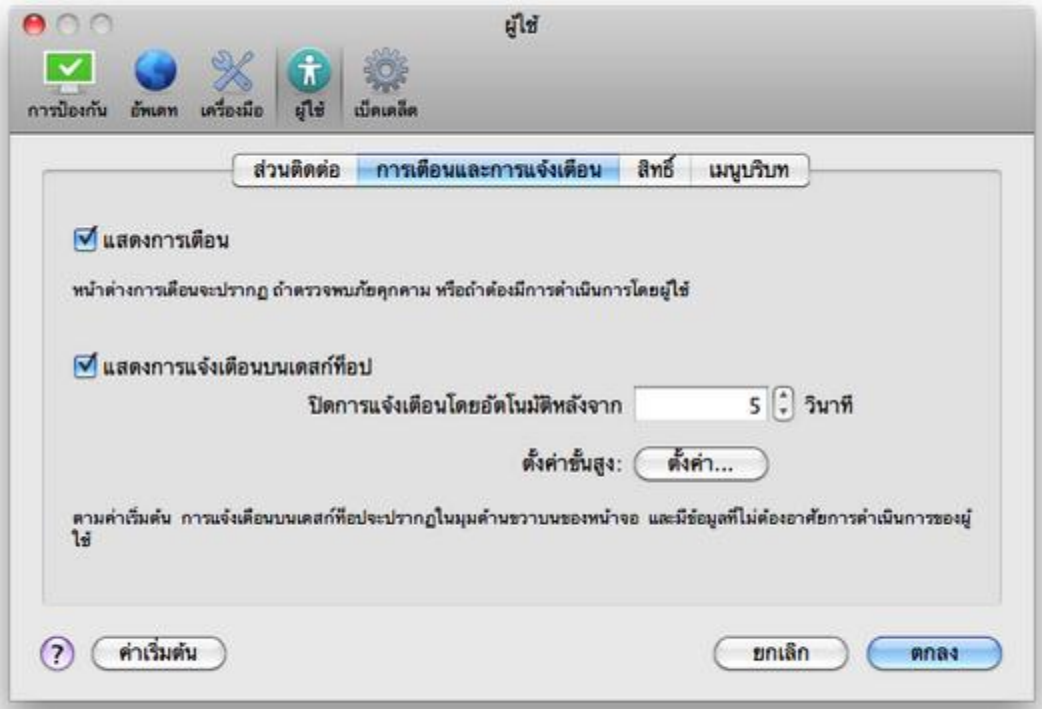
ในส่วน **ใช้เมนูมาตรฐาน** คุณสามารถเลือกตัวเลือก **ในโหมดมาตรฐาน/ในโหมดขั้นสูง** เพื่อเปิดใช้งานการใช้เมนูมาตรฐานในหน้าต่างหลักของโปรแกรมในโหมดการแสดงผลตามลำดับ

เมื่อต้องการเปิดใช้งานคำแนะนำเครื่องมือ ให้เลือกตัวเลือก **แสดงคำแนะนำเครื่องมือ** ตัวเลือก **แสดงไฟล์ที่ซ่อน** จะช่วยให้คุณมองเห็นและเลือกไฟล์ที่ซ่อนได้ในการตั้งค่า **เป้าหมายการสแกน** ของ **การสแกนคอมพิวเตอร์**

การเตือนและการแจ้งเตือน

ส่วน **การเตือนและการแจ้งเตือน** จะช่วยให้คุณสามารถกำหนดค่าวิธีจัดการการเตือนภัยคุกคามและการแจ้งเตือนของระบบใน ESET NOD32 Antivirus

การปิดใช้งานตัวเลือก **แสดงการเตือน** จะเป็นการยกเลิกหน้าต่างการเตือนทั้งหมด และเหมาะสำหรับในบางสถานการณ์เท่านั้น สำหรับผู้ใช้ส่วนใหญ่
เราขอแนะนำให้ใช้การตั้งค่าเริ่มต้นของตัวเลือกนี้ (เปิดใช้งานไว้แล้ว)



การเลือกตัวเลือก **แสดงการแจ้งเตือนบนเดสก์ท็อป** จะช่วยให้หน้าต่างการเตือนที่ไม่จำเป็นต้องมีการดำเนินการจากผู้ใช้สามารถปรากฏบนเดสก์ท็อปได้ (ตามค่าเริ่มต้นแล้วจะปรากฏที่มุมขวาบนของหน้าจอ) คุณสามารถกำหนดระยะเวลาที่จะให้การแจ้งเตือนปรากฏได้ โดยปรับค่า **ปิดการแจ้งเตือนโดยอัตโนมัติหลังจาก** X **วินาที**

การตั้งค่าขั้นสูงของการเตือนและการแจ้งเตือน

แสดงเฉพาะการแจ้งเตือนที่ต้องการการดำเนินการของผู้ใช้
ตัวเลือกนี้ช่วยให้คุณสามารถสลับการแสดงข้อความที่ต้องมีการดำเนินการของผู้ใช้

แสดงเฉพาะการแจ้งเตือนที่ต้องการการดำเนินการของผู้ใช้ เมื่อเรียกใช้แอพพลิเคชันในโหมดเต็มหน้าจอ
ตัวเลือกนี้จะมีประโยชน์เมื่อมีการนำเสนอผลงาน การเล่นเกม หรือทำกิจกรรมที่ต้องใช้ทั้งหน้าจอ

สิทธิ์

การตั้งค่า ESET NOD32 Antivirus เป็นส่วนสำคัญมากสำหรับนโยบายการรักษาความปลอดภัยขององค์กรของคุณ
การแก้ไขโดยไม่ได้รับอนุญาตอาจเป็นอันตรายต่อเสถียรภาพและการป้องกันระบบของคุณ ด้วยเหตุนี้ คุณจะสามารถเลือกได้ว่าจะให้การอนุญาตแก่ผู้ใช้รายใดเพื่อแก้ไขการกำหนดค่าโปรแกรม

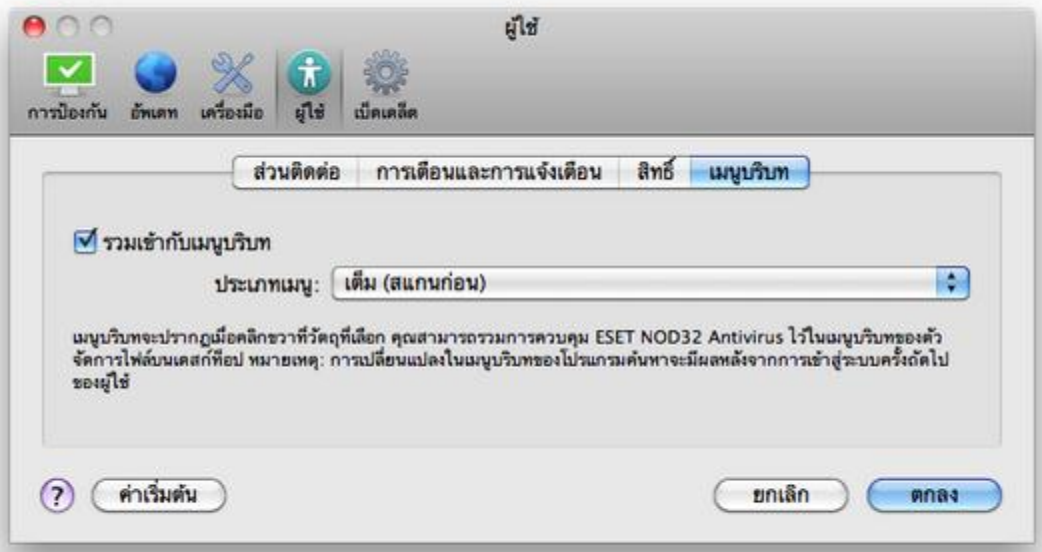
เมื่อต้องการระบุผู้ใช้ที่มีสิทธิ์ ให้เข้าสู่ **ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > ผู้ใช้ > สิทธิ์**

เพื่อให้ระบบของคุณมีความปลอดภัยสูงสุด จะต้องมีการกำหนดค่าโปรแกรมอย่างถูกต้อง การแก้ไขที่ไม่ได้รับอนุญาตอาจทำให้สูญเสียข้อมูลสำคัญ เมื่อต้องการตั้งค่ารายการผู้ใช้ที่มีสิทธิ์ ให้เลือกผู้ใช้จากรายการ **ผู้ใช้** ที่ด้านซ้าย และคลิกปุ่ม **เพิ่ม** เมื่อต้องการลบผู้ใช้ออก ให้เลือกชื่อผู้ใช้ดังกล่าวจากรายการ **ผู้ใช้ที่มีสิทธิ์** ที่ด้านขวา และคลิก **ลบออก**

หมายเหตุ: ถ้าไม่มีรายชื่อในรายการผู้ใช้ที่มีสิทธิ์ ผู้ใช้ทั้งหมดของระบบจะได้รับอนุญาตให้แก้ไขการตั้งค่าของโปรแกรม

เมนูบริบท

สามารถเปิดใช้งานการรวมเมนูบริบทได้ในส่วน **ตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > ผู้ใช้ > เมนูบริบท** โดยเลือกช่องทำเครื่องหมาย **รวมเข้ากับเมนูบริบท**



ThreatSense.Net

ระบบการเตือนล่วงหน้า ThreatSense.Net ทำให้ ESET ทราบถึงการแฝงตัวใหม่ๆ ได้ทันทีและต่อเนื่อง ระบบการเตือนล่วงหน้า ThreatSense.Net แบบสองทิศทางมีวัตถุประสงค์เดียว คือการปรับปรุงการป้องกันที่เรามีให้แก่คุณ วิธีที่ดีที่สุดที่จะทำให้มั่นใจว่าเราพบภัยคุกคามใหม่ๆ ทันทีที่ปรากฏก็คือการ "เชื่อมโยง" กับลูกค้าจำนวนมากที่สุดเท่าที่จะทำได้ และให้ลูกค้าของเราเป็นหน่วยลาดตระเวนภัยคุกคามของเรา คุณลักษณะนี้มีสองตัวเลือก:

1. คุณสามารถเลือกที่จะไม่เปิดใช้งานระบบการเตือนล่วงหน้า ThreatSense.Net คุณจะไม่สูญเสียการทำงานในซอฟต์แวร์ และคุณจะยังคงได้รับการป้องกันที่ดีที่สุดที่เรามีให้
2. คุณสามารถกำหนดค่าระบบการเตือนล่วงหน้า ThreatSense.Net ให้ส่งข้อมูลที่ไม่ระบุตัวบุคคลเกี่ยวกับภัยคุกคามใหม่ๆ และสถานที่ซึ่งรหัสที่เป็นภัยคุกคามนั้นมีอยู่ ไฟล์นี้สามารถส่งถึง ESET เพื่อการวิเคราะห์โดยละเอียด การศึกษาภัยคุกคามเหล่านี้จะช่วยให้ ESET ได้อัพเดทฐานข้อมูลภัยคุกคามและปรับปรุงความสามารถในการตรวจหาภัยคุกคามของโปรแกรม

เทคโนโลยีของระบบการเตือนล่วงหน้า ThreatSense.Net จะเก็บข้อมูลที่ไม่ระบุตัวบุคคลเกี่ยวกับคอมพิวเตอร์ของคุณ ซึ่งเกี่ยวข้องกับภัยคุกคามที่ตรวจพบใหม่ ข้อมูลนี้อาจรวมถึงตัวอย่างหรือสำเนาของไฟล์ที่ภัยคุกคามนั้นปรากฏ พาธไปยังไฟล์นั้น ชื่อไฟล์ วันที่และเวลา กระบวนการที่ภัยคุกคามปรากฏในคอมพิวเตอร์ของคุณ และข้อมูลเกี่ยวกับระบบปฏิบัติการของคอมพิวเตอร์

ถึงแม้จะเป็นไปได้ที่การดำเนินการนี้ในบางกรณีอาจเปิดเผยข้อมูลบางอย่างเกี่ยวกับตัวคุณหรือคอมพิวเตอร์ของคุณ (ชื่อผู้ใช้ในพาธไดเรกทอรี เป็นต้น) แก่แล็บภัยคุกคามของ ESET แต่ข้อมูลนี้จะไม่ถูกนำไปใช้เพื่อวัตถุประสงค์ใดๆ นอกเหนือจากที่จะช่วยให้เราสามารถตอบสนองต่อภัยคุกคามใหม่ๆ ได้ทันที

การตั้งค่า ThreatSense.Net นั้นสามารถเข้าถึงได้จากหน้าต่างการตั้งค่าขั้นสูง ภายใต้ **เครื่องมือ > ThreatSense.Net** เลือกตัวเลือก **เปิดใช้ระบบการเตือนล่วงหน้า ThreatSense.Net** เพื่อเปิดใช้งาน แล้วคลิกปุ่ม **ตั้งค่า...** ที่อยู่ด้านข้างส่วนหัวของตัวเลือกขั้นสูง

ไฟล์ที่น่าสงสัย

ตัวเลือกของไฟล์ที่น่าสงสัยช่วยให้คุณสามารถกำหนดค่าวิธีการส่งภัยคุกคามให้กับแล็บภัยคุกคามของ ESET เพื่อวิเคราะห์

ถ้าคุณพบไฟล์ที่น่าสงสัย คุณสามารถส่งไปยังแล็บภัยคุกคามของเราเพื่อวิเคราะห์ได้ ถ้าปรากฏเป็นแอพพลิเคชันที่เป็นอันตราย ระบบจะเพิ่มการตรวจหาไฟล์นี้ในการอัพเดทฐานข้อมูลไวรัสครั้งถัดไป

การส่งไฟล์ที่น่าสงสัย - คุณสามารถเลือกที่จะส่งไฟล์เหล่านี้ **ระหว่างการอัพเดท** ซึ่งหมายถึงว่าจะมีการส่งไฟล์ไปยังแล็บภัยคุกคามของ ESET ในระหว่างการอัพเดทฐานข้อมูลไวรัสตามปกติ หรืออีกวิธีหนึ่ง คุณสามารถเลือกที่จะส่งไฟล์ **เร็วที่สุดเท่าที่ทำได้** - การตั้งค่านี้จะเหมาะสมถ้ามีการเชื่อมต่ออินเทอร์เน็ตแบบถาวร

ถ้าคุณไม่ต้องการส่งไฟล์ใดๆ ให้เลือกตัวเลือก **ไม่ส่ง** การเลือกที่จะไม่ส่งไฟล์เพื่อวิเคราะห์จะไม่มีผลต่อการส่งข้อมูลสถิติ ซึ่งได้รับการกำหนดค่าไว้ในพื้นที่แยกต่างหาก

ระบบการเตือนล่วงหน้า ThreatSense.Net จะเก็บข้อมูลที่ไม่ระบุตัวบุคคลเกี่ยวกับคอมพิวเตอร์ของคุณ ซึ่งเกี่ยวข้องกับภัยคุกคามที่ตรวจพบใหม่ ข้อมูลนี้อาจรวมชื่อของการแฝงตัว วันที่และเวลาที่ตรวจพบ เวอร์ชันของผลิตภัณฑ์การรักษาความปลอดภัยของ ESET เวอร์ชันของระบบปฏิบัติการของคุณ และการตั้งค่าตำแหน่ง โดยทั่วไปแล้ว โปรแกรมจะส่งข้อมูลสถิติไปยังเซิร์ฟเวอร์ของ ESET วันละหนึ่งหรือสองครั้ง

ข้อมูลด้านล่างนี้คือตัวอย่างของแพ็คเกจสถิติที่ส่ง:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

การส่งข้อมูลสถิติโดยไม่ระบุชื่อ - คุณสามารถกำหนดได้ว่าจะส่งข้อมูลสถิติเมื่อใด ถ้าคุณเลือกส่ง **เร็วที่สุดเท่าที่ทำได้** ข้อมูลสถิติจะถูกส่งทันทีหลังจากที่มีการสร้างข้อมูลขึ้น การตั้งค่านี้เหมาะสมถ้ามีการเชื่อมต่ออินเทอร์เน็ตแบบถาวร ถ้าเลือกตัวเลือก **ระหว่างการอัพเดท** ข้อมูลสถิติทั้งหมดจะถูกส่งในระหว่างการอัพเดทหลังจากการรวบรวมข้อมูล

ถ้าคุณไม่ต้องการส่งข้อมูลสถิติโดยไม่ระบุชื่อ คุณสามารถเลือกตัวเลือก **ไม่ส่ง**

วิธีการส่ง - คุณสามารถเลือกวิธีการส่งไฟล์และข้อมูลสถิติไปยัง ESET ได้ เลือกตัวเลือก **เซิร์ฟเวอร์ Remote Administrator หรือ ESET** สำหรับการส่งไฟล์และสถิติด้วยทุกวิธีที่สามารถกระทำได้ เลือกตัวเลือก **เซิร์ฟเวอร์ Remote Administrator** เพื่อส่งไฟล์และสถิติไปยังเซิร์ฟเวอร์ Remote Administrator โดยที่หลังจากนี้จึงจะส่งไฟล์ไปยังแล็บภัยคุกคามของ ESET ถ้าเลือกตัวเลือก **ESET** ไฟล์ที่น่าสงสัยและข้อมูลสถิติทั้งหมดจะถูกส่งไปยังแล็บไวรัสของ ESET จากโปรแกรมโดยตรง

ตัวกรองการยกเว้น - ตัวเลือกนี้จะช่วยให้คุณสามารถยกเว้นบางไฟล์/โฟลเดอร์จากการส่ง ตัวอย่างเช่น ตัวเลือกนี้อาจมีประโยชน์สำหรับการยกเว้นไฟล์ที่อาจมีข้อมูลลับเฉพาะ เช่น เอกสารหรือสเปรดชีท ประเภทไฟล์ที่ใช้งานทั่วไปจะถูกยกเว้นตามค่าเริ่มต้น (*.doc* เป็นต้น) คุณสามารถเพิ่มประเภทไฟล์ไปยังรายการไฟล์ที่ยกเว้นได้

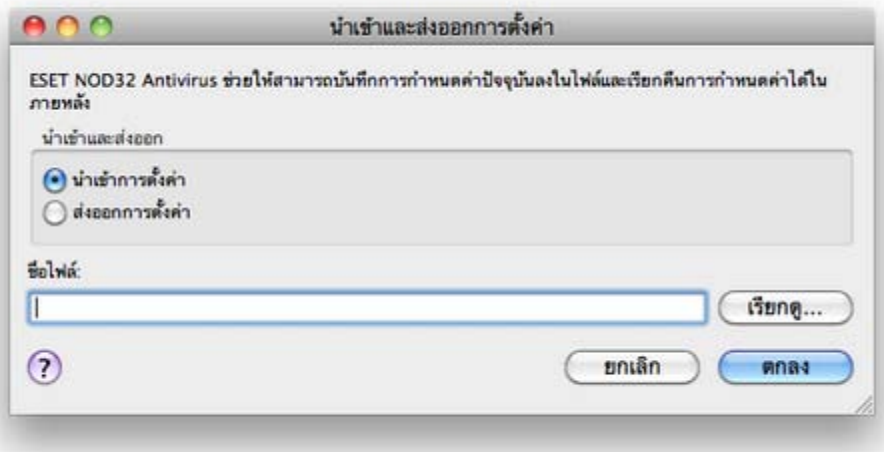
อีเมลที่ติดต่อได้ (ไม่จำเป็น) - อีเมลของคุณจะถูกส่งพร้อมกับไฟล์ที่น่าสงสัย และอาจใช้อีเมลดังกล่าวเพื่อติดต่อคุณถ้าต้องการข้อมูลเพิ่มเติมเพื่อการวิเคราะห์ โปรดทราบว่าคุณจะไม่ได้รับการตอบกลับจาก ESET ยกเว้นกรณีที่ต้องการข้อมูลเพิ่มเติม

ผู้ใช้ขั้นสูง

การตั้งค่าการนำเข้าและส่งออก

การกำหนดค่าการนำเข้าและส่งออกของ ESET NOD32 Antivirus สามารถใช้งานได้ในโหมดขั้นสูงภายใต้ **การตั้งค่า**

ทั้งการนำเข้าและส่งออกใช้ไฟล์อาร์ไคฟ์เพื่อเก็บการกำหนดค่า การนำเข้าและส่งออกจะมีประโยชน์ในกรณีที่คุณต้องสำรองการกำหนดค่าปัจจุบันของ ESET NOD32 Antivirus เพื่อให้สามารถใช้งานได้ในภายหลัง ตัวเลือกส่งออกการตั้งค่าสามารถใช้งานได้สะดวกสำหรับผู้ใช้ที่ต้องการใช้การกำหนดค่าที่ต้องการของ ESET NOD32 Antivirus ในระบบต่างๆ ผู้ใช้จะสามารถส่งออกไฟล์การกำหนดค่าเพื่อโอนการตั้งค่าที่ต้องการได้อย่างง่ายดาย



การตั้งค่าการนำเข้า

การนำเข้าการกำหนดค่าสามารถดำเนินการได้อย่างง่ายดาย จากเมนูหลัก ให้คลิก **การตั้งค่า > นำเข้าและส่งออกการตั้งค่า...** แล้วเลือกตัวเลือก **การตั้งค่าการนำเข้า** ป้อนชื่อของไฟล์การกำหนดค่า หรือคลิกปุ่ม **เรียกดู...** เพื่อเรียกดูไฟล์การกำหนดค่าที่คุณต้องการนำำเข้า

การตั้งค่าการส่งออก

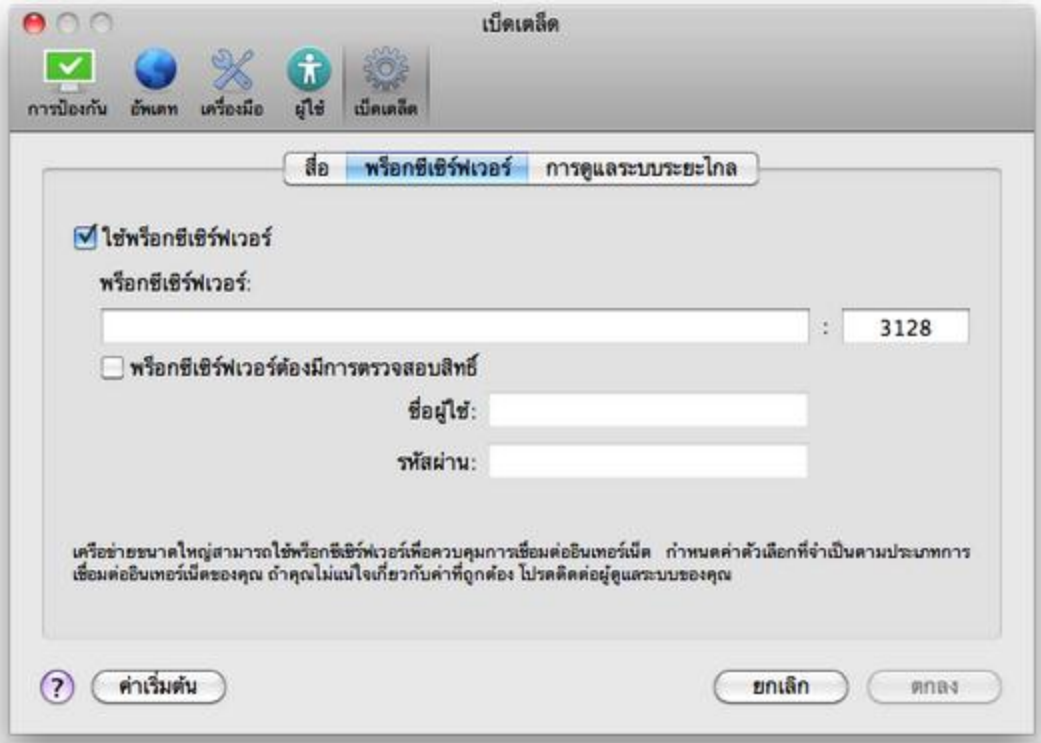
ขั้นตอนในการส่งออกการกำหนดค่าจะมีลักษณะคล้ายกันมาก จากเมนูหลัก ให้คลิก **การตั้งค่า > นำเข้าและส่งออกการตั้งค่า...** เลือกตัวเลือก **การตั้งค่าการส่งออก** และป้อนชื่อของไฟล์การกำหนดค่า ใช้เบราว์เซอร์เพื่อเลือกตำแหน่งในคอมพิวเตอร์เพื่อบันทึกไฟล์การกำหนดค่า

การตั้งค่าพร็อกซีเซิร์ฟเวอร์

การตั้งค่าพร็อกซีเซิร์ฟเวอร์สามารถกำหนดค่าได้ภายใต้ **เบ็ดเตล็ด > พร็อกซีเซิร์ฟเวอร์** การระบุพร็อกซีเซิร์ฟเวอร์ที่ระดับนี้จะกำหนดการตั้งค่าพร็อกซีเซิร์ฟเวอร์ร่วมสำหรับฟังก์ชันทั้งหมดของ ESET NOD32 Antivirus พารามิเตอร์ในที่นี้จะถูกนำมาใช้โดยโมดูลทั้งหมดที่ต้องการการเชื่อมต่ออินเทอร์เน็ต

เมื่อต้องการระบุการตั้งค่าพร็อกซีเซิร์ฟเวอร์สำหรับระดับนี้ ให้เลือกช่องทำเครื่องหมาย **ใช้พร็อกซีเซิร์ฟเวอร์** แล้วป้อนที่อยู่ของพร็อกซีเซิร์ฟเวอร์ในฟิลด์ **พร็อกซีเซิร์ฟเวอร์** พร้อมด้วยหมายเลขพอร์ตของพร็อกซีเซิร์ฟเวอร์

ถ้าการสื่อสารกับพร็อกซีเซิร์ฟเวอร์ต้องการการตรวจสอบสิทธิ์ ให้เลือกช่องทำเครื่องหมาย **พร็อกซีเซิร์ฟเวอร์ต้องการการตรวจสอบสิทธิ์** และป้อน **ชื่อผู้ใช้** และ **รหัสผ่าน** ที่ถูกต้องในฟิลด์ที่สอดคล้องกัน



การปิดกั้นสื่อที่ถอดเข้าออกได้

สื่อที่ถอดเข้าออกได้ (เช่น ซีดีหรือคีย์ USB) อาจมีรหัสที่เป็นอันตรายและทำให้คอมพิวเตอร์ของคุณได้รับความเสี่ยง เมื่อต้องการปิดกั้นสื่อที่ถอดเข้าออกได้ ให้ทำเครื่องหมายที่ตัวเลือก **เปิดใช้งานการปิดกั้นสื่อที่ถอดเข้าออกได้** เมื่อต้องการอนุญาตการเข้าถึงสื่อบางประเภท ให้ยกเลิกการเลือกไดรฟ์ข้อมูลของสื่อที่ต้องการ

การดูแลระบบระยะไกล

ESET Remote Administrator (ERA) เป็นเครื่องมือที่ใช้เพื่อจัดการนโยบายการรักษาความปลอดภัยและรับภาพรวมของการรักษาความปลอดภัยโดยรวมภายในเครือข่าย เครื่องมือนี้จะมีประโยชน์โดยเฉพาะเมื่อใช้กับเครือข่ายขนาดใหญ่ ERA เพิ่มระดับการรักษาความปลอดภัยของเครือข่ายของคุณ พร้อมทั้งให้ความสะดวกในการจัดการ ESET NOD32 Antivirus ในเวิร์กสเตชันของไคลเอ็นต์

ตัวเลือกการกำหนดค่าการดูแลระบบระยะไกลสามารถใช้งานได้จากหน้าต่างหลักของโปรแกรม ESET NOD32 Antivirus คลิก **การตั้งค่า > ป้อนการตั้งค่าแอพพลิเคชัน ... > เบ็ดเตล็ด > การดูแลระบบระยะไกล**

เปิดใช้งานการดูแลระบบระยะไกลโดยเลือกตัวเลือก **เชื่อมต่อกับเซิร์ฟเวอร์การดูแลระบบระยะไกล** จากนั้นคุณจะสามารถเข้าถึงตัวเลือกดังที่อธิบายด้านล่างนี้:

ช่วงเวลาการเชื่อมต่อเซิร์ฟเวอร์ - ตัวเลือกนี้จะกำหนดความถี่ที่ ESET NOD32 Antivirus จะเชื่อมต่อกับ ERA Server ถ้าตั้งค่าเป็น **0** ข้อมูลจะถูกส่งทุก 5 วินาที

เซิร์ฟเวอร์ Remote Administrator - ป้อนที่อยู่เครือข่ายของเซิร์ฟเวอร์ (ที่มีการติดตั้ง ERA Server) และหมายเลขพอร์ต ฟิลด์พอร์ตจะมีพอร์ตของเซิร์ฟเวอร์ที่กำหนดไว้ล่วงหน้า ซึ่งใช้สำหรับการเชื่อมต่อเครือข่าย เราขอแนะนำให้ใช้การตั้งค่าพอร์ตที่เป็นค่าเริ่มต้น คือ *2222*

ถ้าการเชื่อมต่อกับ ERA Server ถูกป้องกันด้วยรหัสผ่าน ให้เลือกช่องทำเครื่องหมาย **เซิร์ฟเวอร์ Remote Administrator ต้องการการตรวจสอบสิทธิ์** และพิมพ์รหัสผ่านในฟิลด์ **รหัสผ่าน**

โดยทั่วไปแล้ว เฉพาะเซิร์ฟเวอร์ **หลัก** เท่านั้นที่จะต้องกำหนดค่า หากคุณเรียกใช้เซิร์ฟเวอร์ ERA หลายเซิร์ฟเวอร์ในเครือข่าย คุณสามารถเลือกที่จะเพิ่มการเชื่อมต่อ **รอง** ERA Server อีกหนึ่งรายการได้ โดยเซิร์ฟเวอร์นี้จะทำหน้าที่เป็นโซลูชันสำรอง ถ้าไม่สามารถเข้าถึงเซิร์ฟเวอร์หลักได้ ESET NOD32 Antivirus จะติดต่อ ERA Server รอง และ ESET NOD32 Antivirus จะพยายามทำการเชื่อมต่อไปยังเซิร์ฟเวอร์หลักอีกครั้ง หลังจากการเชื่อมต่อนี้กลับมาใช้งานได้อีกครั้ง ESET NOD32 Antivirus จะสลับกลับไปที่เซิร์ฟเวอร์หลัก การกำหนดค่าโปรไฟล์ของเซิร์ฟเวอร์การดูแลระบบระยะไกลไว้สองโปรไฟล์นี้ เป็นวิธีที่เหมาะอย่างยิ่งสำหรับโมบายไคลเอ็นต์ที่มีโน้ตบุคเชื่อมต่อจากเครือข่ายในระบบและจากภายนอกเครือข่าย

ประมวลศัพท์

ประเภทของการแฝงตัว

การแฝงตัวเป็นชิ้นส่วนของซอฟต์แวร์ที่เป็นอันตรายซึ่งพยายามเข้าและ/หรือทำความเสียหายให้กับคอมพิวเตอร์ของผู้ใช้

ไวรัส

ไวรัสคอมพิวเตอร์เป็นการแฝงตัวที่ทำให้เกิดความเสียหายกับไฟล์ที่มีอยู่ในคอมพิวเตอร์ของคุณ ไวรัสถูกตั้งชื่อตามไวรัสทางชีววิทยา เนื่องจากใช้เทคนิคที่คล้ายกันในการแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปสู่เครื่องอื่น

ไวรัสคอมพิวเตอร์มักจะโจมตีไฟล์ที่เรียกใช้ได้ สคริปต์ และเอกสารเป็นหลัก ในการเพิ่มจำนวน ไวรัสจะแนบ "ตัว" เข้ากับส่วนท้ายของไฟล์เป้าหมาย กล่าวโดยย่อ ไวรัสมีการทำงานดังต่อไปนี้: หลังจากการเรียกใช้ไฟล์ที่ติดไวรัส ไวรัสจะเปิดใช้งานตนเอง (ก่อนแอพพลิเคชันดั้งเดิม) และดำเนินการกับงานที่กำหนดไว้ล่วงหน้า และหลังจากนั้น แอพพลิเคชันดั้งเดิมจะได้รับอนุญาตให้ทำงาน ไวรัสไม่สามารถติดในคอมพิวเตอร์ได้ จนกว่าผู้ใช้เรียกใช้หรือเปิดโปรแกรมที่เป็นอันตรายนั้นเอง ไม่ว่าจะโดยเจตนาหรือไม่ก็ตาม

ไวรัสคอมพิวเตอร์มีวัตถุประสงค์และความรุนแรงแตกต่างกัน บางชนิดมีอันตรายมาก เนื่องจากมีความสามารถในการลบไฟล์จากฮาร์ดไดรฟ์ ในทางกลับกัน ไวรัสบางชนิดไม่ทำให้เกิดความเสียหายใดๆ แต่ทำหน้าที่สร้างความรำคาญให้กับผู้ใช้ และแสดงความสามารถทางเทคนิคของผู้เขียนเท่านั้น

โปรดทราบว่าไวรัส (เมื่อเปรียบเทียบกับโทรจันหรือสปายแวร์) พบน้อยลงเรื่อยๆ เนื่องจากไม่มีประโยชน์ในเชิงพาณิชย์ต่อผู้เขียนซอฟต์แวร์ที่เป็นอันตราย นอกจากนี้ คำว่า "ไวรัส" นั้นมักจะถูกใช้ผิดๆ เพื่อรวมถึงการแฝงตัวทุกประเภท การใช้งานนี้มีการเปลี่ยนแปลงเกิดขึ้นช้าๆ และมีการใช้คำใหม่ที่ถูกต้องยิ่งกว่า คือ "มัลแวร์" (ซอฟต์แวร์ที่เป็นอันตราย)

ถ้าคอมพิวเตอร์ของคุณติดไวรัส คุณจำเป็นจะต้องเรียกคืนไฟล์ที่ติดไวรัสกลับสู่สภาวะเดิม กล่าวคือ ล้างไวรัสด้วยการใช้โปรแกรมป้องกันไวรัส

ตัวอย่างของไวรัสได้แก่: *OneHalf*, *Tenga* และ *Yankee Doodle*

เวิร์ม

เวิร์มคอมพิวเตอร์เป็นโปรแกรมที่มีรหัสที่เป็นอันตราย ซึ่งจะโจมตีคอมพิวเตอร์โฮสต์ และแพร่กระจายผ่านเครือข่าย ความแตกต่างขั้นพื้นฐานระหว่างไวรัสและเวิร์มคือ เวิร์มมีความสามารถในการจำลองและเดินทางด้วยตนเอง โดยไม่ขึ้นอยู่กับไฟล์ของโฮสต์ (หรือบูตเซคเตอร์) เวิร์มกระจายผ่านที่อยู่อีเมลในรายชื่อผู้ติดต่อของคุณหรือโจมตีจุดอ่อนของการรักษาความปลอดภัยในแอพพลิเคชันของเครือข่าย

ด้วยเหตุนี้ เวิร์มจึงสามารถทำงานได้มากกว่าไวรัสคอมพิวเตอร์ ด้วยความสามารถที่กว้างขวางของอินเทอร์เน็ต เวิร์มจึงสามารถแพร่กระจายไปทั่วโลกได้ภายในไม่กี่ชั่วโมงหลังจากมีการส่งเวิร์มนั้นออกมา ในบางกรณี อาจใช้เวลาเพียงไม่กี่นาที และความสามารถในการจำลองตนเองได้อย่างรวดเร็วโดยไม่ต้องอาศัยสิ่งอื่น จึงทำให้เวิร์มมีอันตรายมากกว่ามัลแวร์ประเภทอื่นๆ

เวิร์มที่ทำงานในระบบสามารถทำให้เกิดความขัดข้องได้หลายประการ: เวิร์มสามารถลบไฟล์ ลดประสิทธิภาพการทำงานของระบบ หรือแม้แต่ปิดการใช้งานโปรแกรม ลักษณะการทำงานของเวิร์มคอมพิวเตอร์ทำให้เวิร์มสามารถเป็น "ตัวนำ" การแฝงตัวประเภทอื่นๆ

ถ้าคอมพิวเตอร์ของคุณได้รับเวิร์ม ขอแนะนำให้คุณลบไฟล์ที่ได้รับเวิร์มออก เนื่องจากเป็นไปได้ว่าไฟล์ดังกล่าวจะมีรหัสที่เป็นอันตรายอยู่

ตัวอย่างของเวิร์มที่เป็นที่รู้จักคือ: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* และ *Netsky*

ม้าโทรจัน

ตามประวัติที่ผ่านมา ม้าโทรจันของคอมพิวเตอร์นั้นหมายถึงการแฝงตัวประเภทหนึ่ง ซึ่งพยายามเสนอตัวเป็นโปรแกรมที่มีประโยชน์ ซึ่งหลอกลวงให้ผู้ใช้อนุญาตให้ทำงานได้ ในปัจจุบัน ม้าโทรจันไม่จำเป็นต้องปิดบังซ่อนเร้นอีกต่อไป โปรแกรมเหล่านี้มีวัตถุประสงค์เพียงอย่างเดียวคือการแฝงตัวให้ง่ายที่สุดเท่าที่จะทำได้ และดำเนินการตามเป้าหมายที่เป็นอันตราย "ม้าโทรจัน" กลายเป็นคำที่มีความหมายกว้างมาก โดยหมายถึงการแฝงตัวที่ไม่อยู่ในหมวดหมู่ของการแฝงตัวประเภทใดโดยเจาะจง

เนื่องจากเป็นประเภทที่กว้างมาก จึงมักแบ่งออกเป็นประเภทย่อยหลายประเภท:

- โปรแกรมดาวน์โหลด - โปรแกรมที่เป็นอันตรายที่สามารถดาวน์โหลดการแฝงตัวประเภทอื่นจากอินเทอร์เน็ต
- ดรอปเปอร์ - ม้าโทรจันประเภทหนึ่งที่ออกแบบมาเพื่อวางมัลแวร์ประเภทอื่นในคอมพิวเตอร์ที่ถูกบุกรุก
- แบ็คดอร์ - แอพพลิเคชันที่สื่อสารกับผู้โจมตีระยะไกล เพื่อให้สามารถเข้าถึงระบบและควบคุมระบบได้
- โปรแกรมบันทึกการกดแป้นพิมพ์ - (คีย์ล็อกเกอร์) - โปรแกรมที่บันทึกการกดแป้นพิมพ์แต่ละครั้งที่ผู้ใช้พิมพ์ และส่งข้อมูลไปยังผู้โจมตีระยะไกล
- โปรแกรมหมุนหมายเลข - โปรแกรมประเภทนี้ได้รับการออกแบบให้เชื่อมต่อไปยังหมายเลขโทรศัพท์ที่มีค่าบริการสูง แทบเป็นไปไม่ได้ที่ผู้ใช้จะสังเกตพบว่ามีการสร้างการเชื่อมต่อใหม่ โปรแกรมหมุนหมายเลขอาจทำให้เกิดความเสียหายแก่ผู้ใช้ที่ใช้โมเด็มแบบหมุนหมายเลข ซึ่งเป็นแบบที่ไม่ได้ใช้งานอย่างแพร่หลายในปัจจุบัน
- ม้าโทรจันมักจะอยู่ในรูปแบบของไฟล์ที่เรียกใช้ได้ ถ้าไฟล์ในคอมพิวเตอร์ของคุณถูกตรวจพบว่าเป็นม้าโทรจัน ขอแนะนำให้ลบทิ้ง เนื่องจากไฟล์เหล่านี้มักจะมีรหัสที่เป็นอันตราย

ตัวอย่างของม้าโทรจันที่เป็นที่รู้จักได้แก่: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*

แอดแวร์

แอดแวร์เป็นคำศัพท์แบบสั้นสำหรับซอฟต์แวร์ที่มีโฆษณาสนับสนุน โปรแกรมที่แสดงเนื้อหาโฆษณาถือเป็นประเภทนี้ด้วยเช่นกัน แอพพลิเคชันแอดแวร์มักจะเปิดหน้าต่างป็อปอัปใหม่โดยอัตโนมัติ ซึ่งจะมีโฆษณาในเบราว์เซอร์อินเทอร์เน็ต หรือเปลี่ยนหน้าเริ่มต้นของเบราว์เซอร์ แอดแวร์มักจะมาพร้อมกับโปรแกรมฟรีแวร์ ซึ่งทำให้ผู้สร้างโปรแกรมฟรีแวร์มีรายได้เพื่อนำไปชดเชยต้นทุนการพัฒนาแอพพลิเคชัน (ที่มีประโยชน์โดยทั่วไป)

ลำพังตัวแอดแวร์เองนั้นไม่เป็นอันตรายแต่อย่างใด — ผู้ใช้อาจรู้สึกรำคาญโฆษณาเพียงเท่านั้น แต่อันตรายจะอยู่ตรงที่แอดแวร์นั้นสามารถทำหน้าที่ติดตามข้อมูล (เช่นเดียวกับที่สปายแวร์สามารถกระทำได้)

หากคุณตัดสินใจที่จะใช้ผลิตภัณฑ์ฟรีแวร์ โปรดให้ความสำคัญกับโปรแกรมการติดตั้งเป็นพิเศษ โปรแกรมติดตั้งจะแจ้งคุณเมื่อมีการติดตั้งโปรแกรมแอดแวร์เพิ่มเติม โดยส่วนมากคุณมีสิทธิ์ที่จะยกเลิก และติดตั้งโปรแกรมโดยที่ไม่มีแอดแวร์

บางโปรแกรมจะไม่ติดตั้งโดยที่ไม่มีแอดแวร์ หรือฟังก์ชันอาจถูกจำกัด ซึ่งหมายความว่า แอดแวร์สามารถเข้าถึงระบบในลักษณะที่ "ถูกกฎหมาย" เนื่องจากผู้ใช้ได้ยินยอมแล้ว ในกรณีนี้ควรกันไว้ดีกว่าแก้ หากมีการตรวจพบไฟล์ที่เป็นแอดแวร์ในคอมพิวเตอร์ของคุณ ขอแนะนำให้ลบไฟล์ดังกล่าว เนื่องจากเป็นไปได้มากว่าไฟล์นั้นอาจมีรหัสที่เป็นอันตราย

สปายแวร์

สปายแวร์จะรวมถึงแอพพลิเคชันทั้งหมดซึ่งส่งข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม/รับรู้จากผู้ใช้ สปายแวร์จะใช้ฟังก์ชันติดตามเพื่อส่งข้อมูลสถิติต่างๆ เช่น รายการเว็บไซต์ที่เยี่ยมชม ที่อยู่อีเมลจากรายชื่อผู้ติดต่อของผู้ใช้ หรือรายการกดแป้นพิมพ์ที่บันทึกไว้

ผู้สร้างสปายแวร์จะอ้างว่าเทคนิคเหล่านี้มีวัตถุประสงค์เพื่อศึกษาเกี่ยวกับความต้องการและความสนใจของผู้ใช้ เพื่อให้การโฆษณาตรงเป้าหมายมากยิ่งขึ้น ปัญหาที่เกิดคือ การขาดเส้นแบ่งที่ชัดเจนระหว่างแอพพลิเคชันที่มีประโยชน์กับแอพพลิเคชันที่มีอันตราย และไม่มีใครรับประกันได้ว่าข้อมูลที่ได้รับจะไม่ถูกนำไปใช้ในทางที่ผิด

ข้อมูลที่ได้รับจากแอพพลิเคชันสปายแวร์อาจมีรหัสการรักษาความปลอดภัย, PIN, หมายเลขบัญชีธนาคาร เป็นต้น ดังนั้น สปายแวร์จึงมักจะมาพร้อมกับโปรแกรมเวอร์ชันฟรีของผู้เขียน เพื่อสร้างรายได้หรือนำเสนอแรงจูงใจสำหรับการซื้อซอฟต์แวร์ ผู้ใช้มักจะทราบว่ามีสปายแวร์ระหว่างการติดตั้งโปรแกรม
เพื่อสร้างแรงจูงใจในการอัพเกรดเป็นเวอร์ชันที่ต้องชำระเงินหากไม่ต้องการให้มีสปายแวร์ดังกล่าว

ตัวอย่างของผลิตภัณฑ์ฟรีแวร์ที่เป็นที่รู้จัก ซึ่งมาพร้อมกับสปายแวร์คือแอพพลิเคชันไคลเอ็นต์ของเครือข่ายแบบ P2P (Peer-To-Peer) Spyfalcon หรือ Spy Sheriff (และอื่นๆ อีกมากมาย) จะอยู่ในชนิดย่อยของสปายแวร์บางประเภท - โดยจะปรากฏเป็นโปรแกรมป้องกันสปายแวร์ แต่จริงแล้วเป็นโปรแกรมสปายแวร์

หากมีการตรวจพบไฟล์ที่เป็นสปายแวร์ในคอมพิวเตอร์ของคุณ ขอแนะนำให้ลบไฟล์ดังกล่าว เนื่องจากเป็นไปได้มากว่าไฟล์นั้นอาจมีรหัสที่เป็นอันตราย

แอพพลิเคชันที่อาจไม่ปลอดภัย

มีโปรแกรมที่ถูกต้องจำนวนมากที่มีหน้าที่ลดความซับซ้อนของการดูแลระบบคอมพิวเตอร์ในเครือข่าย แต่โปรแกรมเหล่านี้อาจถูกใช้ในทางที่ผิดเพื่อวัตถุประสงค์ที่เป็นอันตราย เมื่ออยู่ในมือผู้ที่ไม่ประสงค์ดี ESET NOD32 Antivirus มีตัวเลือกเพื่อตรวจหาภัยคุกคามดังกล่าว

"แอพพลิเคชันที่อาจไม่ปลอดภัย" เป็นการจำแนกประเภทที่ใช้สำหรับซอฟต์แวร์เชิงพาณิชย์ที่ถูกต้อง โดยรวมถึงโปรแกรมอย่างเช่น เครื่องมือเข้าถึงระยะไกล แอพพลิเคชันที่พยายามค้นหารหัสผ่าน และเครื่องมือบันทึกการกดแป้นพิมพ์ (โปรแกรมที่บันทึกการใช้แป้นพิมพ์ของผู้ใช้)

ถ้าคุณพบว่ามีแอพพลิเคชันที่อาจไม่ปลอดภัยที่ทำงานอยู่ในคอมพิวเตอร์ของคุณ (และคุณไม่ได้เป็นผู้ติดตั้งไว้เอง) โปรดติดต่อผู้ดูแลระบบของคุณหรือลบแอพพลิเคชันนั้นออก

แอพพลิเคชันที่อาจไม่พึงประสงค์

แอพพลิเคชันที่อาจไม่พึงประสงค์ไม่จำเป็นจะต้องเป็นแอพพลิเคชันที่อันตราย แต่อาจมีผลเสียกับประสิทธิภาพการทำงานของคอมพิวเตอร์ แอพพลิเคชันดังกล่าวมักจะขอให้มีการยินยอมก่อนติดตั้ง หากแอพพลิเคชันเหล่านี้ปรากฏบนคอมพิวเตอร์ของคุณ ระบบจะทำงานแตกต่างไป (เมื่อเทียบกับวิธีการทำงานก่อนการติดตั้งแอพพลิเคชันเหล่านี้) การเปลี่ยนแปลงที่สำคัญที่สุดคือ:

- หน้าต่างใหม่ที่คุณไม่เคยเห็นก่อนหน้านี้จะเปิดขึ้น
- การเปิดใช้และการเรียกใช้กระบวนการที่ซ่อนอยู่
- การใช้ทรัพยากรของระบบเพิ่มมากขึ้น
- การเปลี่ยนแปลงผลลัพธ์การค้นหา
- แอพพลิเคชันจะสื่อสารกับเซิร์ฟเวอร์ระยะไกล