คู่มือการใช้งาน

คาร์ปาสกี้แอนตี้ไวรัส

2009

ถึง ผู้ใช้ คาร์ปาสกี้ แอนตี้ไวรัส 2009

ขอบพระคุณท่านที่เลือกใช้งานผลิตภัณฑ์ของเรา เราหวังว่า คู่มือการใช้งานนี้จะช่วยท่านในเรื่องของการใช้งาน รวมทั้งช่วยท่านในการตอบคำถามต่างๆเกี่ยวกับผลิตภัณฑ์

เอกสารคู่มือนี้อาจมีการกล่าวถึงรายละเอียดที่มีอยู่ก่อนหน้านี้โดยไม่จำเป็นต้องกล่าวล่วงหน้า สำหรับเวอร์ชั่นล่าสุดนี้ สามารถเข้าดูได้จากเว็บไซต์ http://www.thaikaspersky.com คาร์ปาสกี้แลปไม่อนุญาตให้มีการนำส่วนหนึ่งส่วนใดของเอกสาร

เอกสารนี้ประกอบไปด้วย ทั้งส่วนที่ได้รับการลงทะเบียนและไม่ได้รับการลงทะเบียน ทะเบียนการค้าทั้งหมดเป็นสมบัติของเจ้าของ

+7 (495) 645-7939, Tel., fax: +7 (495) 797-8700, +7 (495) 956-7000

http://www.kaspersky.com/ http://support.kaspersky.com/

วันที่ทำการปรับปรุง 29.04.2008

สารบัญ

เรื่อง **หน้า**

เรื่อง **หน้า**

เรื่อง **หน้า**

บริษัทไอคอมเทค จำกัด

33/4 The 9th Tower, **ชั้น** G (**ห้อง** G10,G11) **ถ.พระราม9 แขวงห้วยขวาง เขตห้วยขวาง**

กรุงเทพฯ 10310

โทร 662-6432150-1 Fax 662-6432152

www.thaikaspersky.com

บทนำ

ส่วนนี้ประกอบไปด้วย

ข้อมูลเพิ่มเติมเกี่ยวกับการใช้งาน

สิ่งเพิ่มเติมในคาร์ปาสกี้แอนตี้ไวรัส 2009

ภาพรวมการป้องกันในการใช้งาน

ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ

ข้อมูลเพิ่มเติมเกี่ยวกับการใช้งาน

หากท่านมีข้อสงสัยประการในเรื่องของการซื้อ การติดตั้ง หรือการใช้งานเรามีคำตอบในส่วนของปัญหาเหล่านั้นอยู่

คาร์ปาสกี้แลป มีแหล่งข้อมูลมากมาย สะดวกแก่การค้นหาของท่าน ขึ้นอยู่กับความสำคัญและความเร่งด่วนในการใช้งานข้อมูลเหล่านั้น

แหล่งข้อมูลที่สามารถค้นหาได้ด้วยตนเอง

ท่านสามารถใช้ระบบการช่วยเหลือ Help

ระบบการช่วยเหลือประกอบไปด้วยข้อมูลในการจัดการการป้องกันคอมพิวเตอร์ การดูสถานะของการป้องกัน การตรวจจับในพื้นที่ต่างกันของคอมพิวเตอร์และแสดงการทำงานอื่นๆ

เปิดการช่วยเหลือ คลิก Help เพื่อไปยังหน้าต่างโปรแกรมหลัก หรือกด F1

การติดต่อฝ่ายขาย

หากว่าท่านมีคำถามในเรื่องของการเลือกหรือซื้อโปรแกรม หรือการต่ออายุการใช้งาน สามารถติดต่อที่แผนกขาย

ท่านสามารถส่งคำถามมาที่แผนกขายได้ที่sales@thaikaspersky.com

การติดต่อส่วนบริการทางเทคนิค

หากท่านได้ซื้อโปรแกรมมาเป็นที่เรียบร้อยแล้ว ท่านสามารถได้รับการบริการข้อมูลจากฝ่ายบริการทางเทคนิคได้ทั้งทางโทรศัพท์หรือทางอินเทอร์เน็ต

เจ้าหน้าที่บริการทางด้านเทคนิค จะตอบคำถามของท่านในเรื่องของการติดตั้งและการใช้งานโปรแกรม หากว่าเครื่องคอมพิวเตอร์ของทานมีการติดสิ่งไม่พึงประสงค์ เราจะช่วยท่านในการกำจัดตามลำดับของมัลแวร์

การร้องขอความช่วยเหลือทางอีเมล์ต่อส่วนบริการทางด้านเทคนิค (สำหรับผู้ใช้งานที่ทำการลงทะเบียนแล้วเท่านั้น)

ท่านสามารถส่งคำถามของท่านไปยังผู้เชี่ยวชาญทางด้านเทคนิค โดยการเข้าไปยังแบบฟอร์มช่วยเหลือหน้าเว็บ

(http://support.kaspersky.com/helpdesk.html).

ท่านสามารถเขียนคำถามของท่านได้ทั้งภาษาไทยและภาษาอังกฤษ

ในการส่งข้อความคำถามทางอีเมล์ ท่านต้องส่งเลขที่ลูกค้า และรหัสผ่านที่ได้รับเมื่อทำการลงทะเบียนที่เว็บไซต์บริการทางด้านเทคนิค

หมายเหตุ

หากว่าท่านยังไม่ได้ลงทะเบียนเป็นผู้ใช้โปรแกรมของคาร์ปาสกีแลป ท่านสามารถกรอกแบบการลงทะเบียนได้ที่

http://www.thaikaspersky.com/kaspersky-thai/register_product_new.htm

ในการลงทะเบียน ท่านจะได้รับรหัสสำหรับการติดตั้ง หรือชื่อของไฟล์สำคัญ

ส่วนบริการทางด้านเทคนิค จะตอบคำถามท่านใน Personal Cabinet ที่ https://support.kaspersky.com/en/PersonalCabinet และส่งไปยังอีเมล์ของท่านตามคำขอ

ในการกรอกคำถามบนหน้าเว็บ ท่านควรอธิบายรายละเอียดต่างๆให้มากที่สุดเท่าที่เป็นไปได้ โดยเฉพาะข้อมูลสำคัญดังต่อไปนี้

- **ประเภทของคำถามที่กำหนดไว้** คำถามจากผู้ใช้ส่วนมากที่พบบ่อย จะนำมารวมเป็นกลุ่มหัวข้อพิเศษเดียวกัน ตัวอย่างเช่น “การติดตั้งผลิตภัณฑ์ ปัญหาในการถอนโปรแกรม” หรือ “การสแกนไวรัส/ ปัญหาในการถอนโปรแกรม” หากว่าไม่มีหัวข้อที่เหมาะสมกับคำถามของท่าน ให้เลือกหัวข้อ“คำถามทั่วไป”
- **ชื่อโปรแกรมและเวอร์ชั่นที่ใช้งาน**
- **เนื้อหาที่กำหนดไว้** อธิบายปัญหาของท่านให้มากที่สุดเท่าที่จะมากได้
- **หมายเลขลูกค้า และรหัสผ่าน** กรอกหมายเลขลูกค้าและรหัสผ่านซึ่งท่านจะได้รับเมื่อทำการลงทะเบียนผ่านหน้าเว็บไซต์บริการทางด้านเทคนิค
- **ที่อยู่อีเมล์** ฝ่ายสนับสนุนทางด้านเทคนิคจะส่งคำตอบไปยังอีเมล์นี้

การสนับสนุนทางเทคนิคทางโทรศัพท์

หากว่าท่านมีปัญหาที่ต้องการความช่วยเหลืออย่างเร่งด่วน ท่านสามารถโทรศัพท์เข้ามาแจ้งความต้องการได้กับสำนักงานที่ใกล้ที่สุด ท่านสามารถดูรายละเอียดได้จาก (http://support.kaspersky.com/support/details) สมัครใช้งานของรัสเซียที่ (http://www.thaikaspersky.com/kaspersky-thai/service.htm) หรือผู้ใช้งานประเทศไทย (http://support.kaspersky.com/support/international) ส่วนการสนับสนุนทางเทคนิค จะช่วยเหลือท่านตามคำร้องขออย่างรวดเร็วที่สุดเท่าที่เป็นไปได้

พูดคุยเรื่องการใช้งานกับคาร์ปาสกี้แลปบนเว็บแสดงความคิดเห็น

หากว่าคำถามของท่านไม่ได้เป็นเรื่องเร่งด่วย ท่านสามารถพูดคุยเรื่องราวที่ท่านต้องการทราบกับผู้เชี่ยวชาญของคาร์ปาสกี้แลป รวมทั้งผู้ใช้งานคาร์ปาสกี้ท่านอื่นๆ ได้บนเว็บแสดงความคิดเห็นที่ http://forum.kaspersky.com/

ในการแสดงความคิดเห็น ท่านสามารถอ่านหัวข้อที่มีอยู่ ตอบคำถาม สร้างหัวข้อและการใช้งานค้นคว้า

สิ่งเพิ่มเติมในคาร์ปาสกี้แอนตี้ไวรัส 2009

คาร์ปาสกี้แอนตี้ไวรัส 2009 (หรือที่จะกล่าวถึงต่อไปว่า “คาร์ปาสกี้แอนตี้ไวรัส” หรือ”โปรแกรม”) เป็นสิ่งที่รวบรวมกลยุทธ์ใหม่ล่าสุดในการป้องกันข้อมูล โดยพื้นฐานของการเข้าถึงข้อมูลอย่างถูกต้อง กลยุทธ์นี้จะช่วยในการป้องกันการกระทำอันไม่พึงประสงค์โดยโปรแกรมที่น่าสงสัย หรือเป็นอันตราย ความสามารถของโปรแกรมจะทำการปกป้องข้อมูลที่เป็นความลับของผู้ใช้ โดยเพิ่มพูนความสามารถจากเพิ่มมากมาย โปรแกรมนี้ประกอบไปด้วยเครื่องมือ และวิซาร์ดเพื่อให้การปกป้องคอมพิวเตอร์เป็นเรื่องง่ายดายขึ้น

คุณลักษณะใหม่ในคาร์ปาสกี้แอนตี้ไวรัส 2009

<u>คุณลักษณะของการปกป้องแบบใหม่</u>

- การตรวจสอบระบบการปฏิบัติการและซอฟต์แวร์ที่ได้รับการติดตั้ง เพื่อตรวจจับและกำจัดช่องโหว่หรือจุดอ่อน รักษาระดับของความปลอดภัยในระดับสูง และป้องกันโปรแกรมที่เป็นอันตรายต่อระบบของท่าน
- ตัววิเคราะห์ความปลอดภัยแบบใหม่ และวิซาร์ดกำหนดค่าการใช้งานต่างๆ ที่สะดวกต่อการตรวจสอบ และกำจัดภัยคุกคามความปลอดภัย ช่องโหว่ หรือจุดอ่อน ในโปรแกรมที่ติดตั้ง รวมทั้งการกำหนดค่าของระบบปฏิบัติการและการใช้งาน
- คาร์ปาสกี้แลปตอบสนองต่อภัยคุกคามใหม่ๆ ที่เกิดขึ้นอย่างรวดเร็ว ผ่านเครือข่ายความปลอดภัยคาร์ปาสกี้ ที่ทำงานร่วมกันในการรับข้อมูลภัยคุกคามจากเครื่องคอมพิวเตอร์ของผู้ใช้ และส่งต่อไปยังเซิร์ฟเวอร์ของคาร์ปาสกี้แลป
- วิซาร์ดการกู้ระบบแบบใหม่ ช่วยในการซ่อมแซมความเสียหายที่เกิดขึ้นต่อระบบของท่านเมื่อมีผู้เข้ามาทำลายระบบ

<u>คุณลักษณะการปกป้องแบบใหม่สำหรับผู้ใช้งานอินเทอร์เน็ต</u>

- ปรับปรุงส่วนของการปกป้องจากผู้บุกรุกทางอินเทอร์เน็ต รวมทั้งฐานข้อมูลของโปรแกรมในส่วนของเว็บไซต์ปลอมต่างๆ
- ความปลอดภัยในการใช้งานการส่งข้อความแบบทันที ด้วยเครื่องมือที่ทำการตรวจสอบการใช้งานโปรแกรม MSN และ ICQ

คุณลักษณะตัวประสานการใช้งานของผู้ใช้งานกับโปรแกรมแบบใหม่

- ตัวประสานการใช้งานแบบใหม่นี้ครอบคลุมการปกป้องข้อมูลมากขึ้น
- กล่องข้อความที่มีความสามารถสูง ช่วยให้ผู้ใช้ทำการตัดสินใจได้รวดเร็วขึ้น
- ขยายความสามารถในการทำงาน สำหรับการบันทึกสถิติ และการทำรายงาน สามารถเลือกตัวกรองจากรายงาน และเครื่องมืออันทางพลังที่มีความยืดหยุ่นมากขึ้น

ภาพรวมการป้องกันในการใช้งาน

คาร์ปาสกี้แอนตี้ไวรัส ปกป้องเครื่องคอมพิวเตอร์ของท่านจากภัยคุกคามทั้งที่รู้จักและไม่รู้จัก รวมไปถึงข้อมูลอันไม่พึงประสงค์ภัยคุกคามแต่ละประเภทที่แยกตามองค์ประกอบของโปรแกรม การติดตั้งที่มีความยืดหยุ่น ด้วยตัวเลือกการกำหนดค่าการใช้งานที่ง่ายดาย ตามความต้องการของผู้ใช้

คาร์ปาสกี้แอนตี้ไวรัสประกอบไปด้วยคุณลักษณะด้านการป้องกันดังต่อไปนี้

- ระบบการเฝ้าระวังพฤติกรรมการใช้งานโปรแกรมของผู้ใช้ การป้องกันการกระทำที่เป็นอันตรายใดๆ
- การปกป้องแบบเรียลไทม์ของการรับส่งข้อมูลทั้งหมด ที่ผ่านเข้าออกเครื่องคอมพิวเตอร์ของท่าน
- ความปลอดภัยออนไลน์ ที่ให้การป้องกันการจู่โจมแบบฟิชชิ่ง
- การมอบหมายงานตรวจสอบไวรัส เพื่อการตรวจสอบไฟล์ส่วนบุคคล ไดร์ฟ พื้นที่เฉพาะ หรือตรวจหาไวรัสในทุกส่วนของคอมพิวเตอร์ งานในการตรวจสอบจะมีการกำหนดค่าเพื่อให้ตรวจจับช่องโหว่ หรือจุดอ่อน ที่อยู่ในโปรแกรมที่ผู้ใช้ติดตั้ง
- การอัพเดทเพื่อให้โปรแกรมอยู่ในสถานะทันต่อเหตุการณ์ที่เกิดขึ้นใหม่อยู่เสมอ ทั้งโมดูลของโปรแกรมและฐานข้อมูลที่ใช้ในการตรวจจับโปรแกรมอันไม่พึงประสงค์ การจู่โจมของแฮกเกอร์ และข้อความสแปม
- วิซาร์ดและเครื่องมือสะดวกต่อการจัดการงานตรวจสอบที่เกิดขึ้นในระหว่างการทำงานของคาร์ปาสกี้แอนตี้ไวรัส

- คุณลักษณะที่สนับสนุนการทำงาน โดยมีข้อมูลและตัวช่วยที่ทำงานกับโปรแกรมเพื่อเพิ่มประสิทธิภาพการทำงาน

วิซาร์ดและเครื่องมือ

การทำให้เกิดความมั่นใจในความปลอดภัยของเครื่องคอมพิวเตอร์ เป็นการทำงานที่ซับซ้อนต้องอาศัยความรู้ของคุณลักษณะในระบบปฏิบัติการ และวิธีการเข้าเอาชนะจุดอ่อนของมัน นอกจากนี้ ปริมาณและความหนาแน่นของข้อมูลเกี่ยวกับความปลอดภัยของระบบ ทำให้การวิเคราะห์และการดำเนินการยากขึ้น

เพื่อช่วยในการแก้ไขปัญหาการทำงานแบบเฉพาะในการทำให้เกิดความปลอดภัยต่อคอมพิวเตอร์ คาร์ปาสกี้แอนตี้ไวรัสจึงมีวิซาร์ดและเครื่องมือดังต่อไปนี้

- วิซาร์ดวิเคราะห์ความปลอดภัย ใช้ในการวินิจฉัยข้อบกพร่องของเครื่องคอมพิวเตอร์หรือส่วนประกอบใด ๆ ของเครื่องเพื่อค้นหาช่องโหว่ หรือจุดอ่อนของโปรแกรมที่ผู้ใช้งานติดตั้ง
- วิซาร์ดการตั้งค่าใช้งานต่างๆ วิเคราะห์การตั้งค่าโปรแกรมที่ช่วยค้นหาไมโครซอฟต์อินเทอร์เน็ตเอ็กซ์พลอเรอร์ ประเมินเบื้องต้นจากด้านความปลอดภัย
- วิซาร์ดการกู้คืนระบบ กำจัดการจู่โจมของโปรแกรมอันไม่พึงประสงค์ออกจากระบบ
- วิซาร์ดการกู้คืนหน่วยบันทึก มีประโยชน์ต่อระบบหลังจากระบบถูกจู่โจมให้เกิดความเสียหายต่อไฟล์ของระบบปฏิบัติการ เพื่อไม่ให้เครื่องคอมพิวเตอร์ตั้งต้นใหม่อีกครั้ง

ตัวช่วยสนับสนุน

โปรแกรมรวมคุณลักษณะการสนับสนุน ที่ทำให้โปรแกรมมีความทันสมัยอยู่เสมอ เพื่อเพิ่มความสามารถในการทำงานของโปรแกรม และช่วยในการใช้งานของท่าน

เครือข่ายความปลอดภัยของคาร์ปาสกี้

เครือข่ายความปลอดภัยของคาร์ปาสกี้ คือ ระบบการโอนถ่ายข้อมูลอย่างอัตโนมัติในการตรวจจับภัยคุกคามที่เกิดขึ้นแล้วส่งไปยังฐานข้อมูลส่วนกลางของคาร์ปาส้กีแลป ฐานข้อมูล้นีทำให้คาร์ปาส้กี มีความรวดเร็วต่อภัยคุกคามที่แพร่ขยายอย่างรวดเร็ว และแจ้งกลับผู้ใช้ได้ในทันที

ลิขสิทธิ์

เมื่อท่านซื้อคาร์ปาสกี้แอนตี้ไวรัส แล้วได้เข้าสู่ข้อตกลงทางลิขสิทธิ์ ซึ่งควบคุมการใช้งานของโปรแกรม การเข้าถึงการอัพเดทฐานข้อมูลโปรแกรม และการสนับสนุนทางด้านเทคนิค้นันเป็นไปตามอายุของลิขสิทธิ์ การใช้งานเต็มประสิทธิภาพการทำงานตามลิขสิทธิ์

ในส่วนของ “ลิขสิทธิ์” สามารถบอกในส่วนที่เกี่ยวกับลิขสิทธิ์ปัจจุบันของท่าน การซื้อ และการต่ออายุ

การสนับสนุน

ผู้ใช้งานคาร์ปาสกี้แอนตี้ไวรัสที่ลงทะเบียนแล้วทั้งหมด สามารถรับประโยชน์ในการบริการสนับสนุนทางด้านเทคนิค โดยดูข้อมูลเกี่ยวกับวิธีการรับความช่วยเหลือทางด้านเทคนิคในส่วน"Support"

เมื่อลิงค์ไปที่ส่วนสนับสนุน จะพบว่ามีส่วนแสดงความคิดเห็นของผู้ใช้คาร์ปาสกี้ เพื่อส่งรายงานข้อผิดพลาดไปยังส่วนสนับสนุนทางเทคนิค เรามีความยินดีในการบริการท่านผ่านทางโทรศัพท์ในเรื่องเกี่ยวกับโปรแกรม

การวิเคราะห์พฤติกรรมของไวรัสแบบฮิวริสติก

พฤติกรรมของไวรัสแบบฮิวริสติก ใช้ในส่วนของการปกป้องแบบเรียลไทม์ เช่น การป้องกันไฟล์จากไวรัส การป้องกันเมล์จากไวรัส การป้องกันเว็บจากไวรัส และในการตรวจสอบไวรัส

การตรวจสอบวัตถุโดยการใช้ลายเซ็นต์ ซึ่งใช้ฐานข้อมูลที่ใช้คำอธิบายครอบคลุมภัยคุกคามทั้งหมดที่ระบุไว้เพื่อการตรวจสอบโปรแกรมที่ไม่พึงประสงค์ และอันตราย เป็นโปรแกรมวิเคราะห์รหัสของวัตถุและเป็นวิธีการตัดสินใจว่าเป็นอันตรายหรือไม่ทางอ้อม ที่สามารถตรวจจับได้ทั้งไวรัสที่รู้จักและไม่รู้จักซึ่งไม่เหมือนกับวิธีการแบบลายเซ็นต์

ประโยชน์ของการวิเคราะห์แบบฮิวริสติก นั่นเพื่อการตรวจจับโปรแกรมอันไม่พึงประสงค์ ที่ไม่ได้มีการลงทะเบียนไว้ในฐานข้อมูล เพราะภัยคุกคามและการจู่โจมมีการสร้างขึ้นใหม่ทุกวัน อันเป็นการตรวจจับก่อนการวิเคราะห์ไวรัส

อย่างไรก็ตาม วิธีการฮิวริสติก อาจทำให้การทำงานของระบบหยุดชะงักลงเนื่องเพราะการตรวจจับพบว่ามีรหัสไม่พึงประสงค์ที่ได้จากการตรวจสอบแบบฮิวริสติก

<u>หมายเหตุ</u>

การใช้งานร่วมกันของวิธีการในการตรวจสอบจะทำให้มีความปลอดภัยมากกว่า

เมื่อมีการตรวจสอบวัตถุ การวิเคราะห์แบบฮิวริสติก จะเหนือกว่าในด้านความปลอดภัยในการตรวจจับวัตถุโดยโปรแกรมในสภาพแวดล้อมเสมือน หากว่าการกระทำที่น่าสงสัยที่ค้นเหมือนเป็นวัตถุดำเนินการ ทำให้วัตถุนั้นได้รับการปฏิเสธในการฝังลงเครื่องแม่ และจะมีข้อความเตือนแนะนำผู้ใช้ในการดำเนินการต่อไป

- การแยกวัตถุทำการตรวจสอบภัยคุกคามตัวใหม่และดำเนินการในการอัพเดทฐานข้อมูล
- ลบวัตถุ
- ข้ามไป(หากท่านมั่นใจว่าวัตถุนั้นไม่ใช่สิ่งไม่พึงประสงค์)

ในการเลือกใช้การวิเคราะห์แบบฮิวริสติก ให้เลือกที่ Use heuristic analyzer และเลื่อนรายละเอียดการตรวจสอบในตำแหน่งเหล่านี้ น้อย (Shallow), ปานกลาง (Medium) หรือ ทุกรายละเอียด (Detailed) ระดับของรายละเอียดในการตรวจสอบควรให้มีความสมดุลกับปริมาณข้อมูลที่เข้ามา และคุณภาพของการตรวจสอบภัยคุกคามใหม่ รวมทั้งการโหลดของทรัพยากรในระบบปฏิบัติการ และระยะเวลาของการตรวจสอบ ระดับของฮิวริสติกที่มีค่าสูงมาก จะมีความต้องการทรัพยากรในระบบปฏิบัติการมาก และใช้เวลาในการดำเนินการนานกว่า

<u>คำเตือน!</u>

การสกัดกั้นภัยคุกคามใหม่ๆ โดยการใช้การวิเคราะห์แบบฮิวริสติกของคาร์ปาสกี้แลป และวิธีการในการกำจัดนั้นมีการอัพเดทฐานข้อมูลในทุกชั่วโมง

ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ

เพื่อให้การทำงานของซอฟต์แวร์เต็มประสิทธิภาพ คอมพิวเตอร์จะต้องมีความต้องการระบบอย่างน้อยดังต่อไปนี้

- พื้นที่ว่างของฮาร์ดดิสก์ 75 MB
- CD-ROM (สำหรับการติดตั้งโปรแกรมโดยการใช้ CD)
- เมาส์
- IE 5.5 ขึ้นไป (สำหรับการอัพเดทฐานข้อมูลของโปรแกรม และโมดูลซอฟต์แวร์ผ่านทางอินเทอร์เน็ต)
- Microsoft Window Installer 2.0

Microsoft Windows XP Home Edition (SP2 หรือสูงกว่า), Microsoft Windows XP Professional (SP2 หรือสูงกว่า), Microsoft Windows XP Professional x64 Edition:

- Intel Pentium 300 MHZ Processor หรือสูงกว่า (หรือเทียบเท่ากัน)
- 256 MB RAM

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor หรือสูงกว่า(หรือเทียบเท่ากัน)
- 512 MB RAM

ภัยคุกคามต่อความปลอดภัยของคอมพิวเตอร์

ความปลอดภัยของคอมพิวเตอร์ที่เป็นอันตรายจาก โปรแกรมคุกคาม สแปม ฟิชชิ่ง การจู่โจมของแฮกเกอร์ ซอฟต์แวร์โฆษณาและแบนเนอร์ ซึ่งตัวการหลักของภัยคุกคามเหล่านี้มาจากอินเทอร์เน็ต

<u>เนื้อหาในส่วนนี้ประกอบไปด้วย</u>

โปรแกรมภัยคุกคาม

โปรแกรมภัยคุกคาม

คาร์ปาสกี้แอนตี้ไวรัส สามารถสกัดกั้นโปรแกรมอันไม่พึงประสงค์กว่าพันโปรแกรม ที่เข้ามาแฝงอยู่ในเครื่องคอมพิวเตอร์ของท่าน บางส่วนของโปรแกรมเหล่านี้ทำการคุกคามการทำงานของเครื่องคอมพิวเตอร์ท่าน และตัวอื่นๆที่จัดว่าอันตราย หลังจากที่โปรแกรมทำการสืบค้นโปรแกรมอันไม่พึงประสงค์ และจัดแยกหมวดหมู่ให้อยู่ในระดับอันตราย(สูง หรือกลาง)

การวิเคราะห์ไวรัสของคาร์ปาสกี้แลป จำแนกความแตกต่างออกเป็นสองหมวดหมู่หลักของโปรแกรมภัยคุกคาม คือ โปรแกรมแอบแฝงมุ่งร้าย และโปรแกรมอันไม่พึงประสงค์

โปรแกรมแอบแฝงมุ่งร้าย (Malware) สร้างความเสียหายให้แก่คอมพิวเตอร์ของผู้ใช้ เช่น การขโมยข้อมูล การสกัดกั้น เปลี่ยนแปลงหรือลบข้อมูล รวมทั้งการขัดขวางการทำงานของระบบปฏิบัติการของเครื่องคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

โปรแกรมที่ไม่พึงประสงค์ (PUPs) แตกต่างจากโปรแกรมแอบแฝงมุ่งร้าย ที่ไม่ได้เข้าไปทำลายแต่จะเข้าไปแทรกซึมอยู่ในระบบปฏิบัติการของคอมพิวเตอร์

สารานุกรมไวรัส (http://www.viruslist.com/en/viruses/encyclopedia) จะมีคำอธิบายเรื่องของรายละเอียดของโปรแกรมเหล่านี้

โปรแกรมมุ่งร้าย

โปรแกรมมุ่งร้าย (Malware) เป็นการสร้างตัวเองขึ้นมาเฉพาะเพื่อทำให้เกิดความเสียหายแก่เครื่องคอมพิวเตอร์และผู้ใช้งานเครื่องคอมพิวเตอร์ อันได้แก่ การขโมย การสกัดกั้น เปลี่ยนแปลงหรือลบข้อมูล รวมทั้งการขัดขวางการทำงานของระบบปฏิบัติการของเครื่องคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

โปรแกรมมุ่งร้ายแบ่งออกได้เป็น 3 ประเภท คือ ไวรัสและหนอนอินเทอร์เน็ต โทรจัน และโปรแกรมอเนกประสงค์มุ่งร้าย

ไวรัสและหนอนอินเทอร์เน็ต สามารถสร้างสำเนาของตัวเอง แพร่กระจายและขยายออกไปซ้ำแล้วซ้ำอีก ทำกระบวนการโดยที่ผู้ใช้งานไม่ทราบการกระทำดังกล่าว หรือดำเนินการที่ผู้ใช้มองเห็นการกระทำโปรแกรมเหล่านี้จะแสดงอาการมุ่งร้ายเมื่อตัวมันดำเนินการ

โปรแกรมโทรจัน (Trojan) จะไม่มีการสร้างสำเนาซึ่งไม่เหมือนกับไวรัส หรือหนอนอินเทอร์เน็ต โทรจันมีผลต่อคอมพิวเตอร์ อย่างเช่นจากการที่ผู้ใช้งานส่งอีเมล์ หรือการเข้าเว็บไซต์เมื่อเข้าไปยังเว็บไซต์ที่มีเชื้ออยู่ โปรแกรมจะแสดงอาการมุ่งร้ายเมื่อมีการใช้งาน

โปรแกรมอเนกประสงค์มุ่งร้าย *(Malicious tools)* สร้างขึ้นเพื่อให้มีผลต่อคอมพิวเตอร์ ทำลายคอมพิวเตอร์ อย่างไรก็ตาม มีความแตกต่างจากโปรแกรมมุ่งร้ายอื่นๆ ที่ไม่ได้มีพฤติกรรมในการมุ่งร้ายเมื่อมีการดำเนินการโปรแกรม และยังคงมีความปลอดภัยเมื่ออยู่บนเครื่องคอมพิวเตอร์ของผู้ใช้ การกระทำที่แฮก

เกอร์ใช้เพื่อการสร้างไวรัส หนอนอินเทอร์เน็ตและโทรจัน จัดการจู่โจมเครือข่ายโดยการรีโมตเซิร์ฟเวอร์ ดัดแปลงแก้ไขโปรแกรมการกระทำมุ่งร้ายอื่นๆ

ไวรัส (Virus)

หมวดหมู่ย่อย: ไวรัสและหนอนอินเทอร์เน็ต

ระดับความรุนแรง: สูง

ไวรัสแบบดั้งเดิม และหนอนอินเทอร์เน็ตที่มีการดำเนินการบนเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตบนเครื่องคอมพิวเตอร์ที่ติดรวมทั้งสามารถสำเนาตัวเอง และแพร่กระจายทั่วคอมพิวเตอร์

ไวรัสแบบดั้งเดิม

หลังจากไวรัสเข้าแทรกซึมไปยังระบบ จะทำการติดฝังไปยังไฟล์ กระตุ้นตัวเอง และแสดงพฤติกรรมมุ่งร้าย รวมทั้งเพิ่มสำเนาตัวเองไปยังไฟล์อื่น

ไวรัสแบบดั้งเดิม ทำสำเนาแค่เพียงทรัพยากรภายในของเครื่องพิวเตอร์ที่ติดเชื่อ แต่ไม่สามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่น การแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ เกิดขึ้นได้หากว่าไวรัสทำการเพิ่มตัวเองลงไปยังไฟล์แล้วไฟล์นั้นเก็บไว้ยังโฟลเดอร์ที่มีการใช้งานร่วมกัน หรือCD หรือการส่งไฟล์ที่แนบไวรัสไปทางอีเมล์

รหัสของไวรัสแบบดั้งเดิม ออกมาเพื่อการแทรกซึมยังส่วนเฉพาะของเครื่องคอมพิวเตอร์ ระบบปฏิบัติการหรือโปรแกรมขึ้นอยู่กับสิ่งแวดล้อม ระยะทางระหว่างไฟล์ บูท สคริปต์และไวรัสมหภาค

ไวรัสสามารถติดไปกับไฟล์โดยวิธีต่างๆมากมาย การเขียนทับไวรัสที่เขียนโดยรหัสจองตัวมันเองแทนที่รหัสของไฟล์ที่มีการติดไวรัส เข้าทำลายเนื้อหาเดิมของไฟล์ ไฟล์ที่ติดไวรัสจะหยุดการทำงานและไม่สามารถกำจัดได้ ไวรัสปาราสิตที่เป็นตัวทำลายจะทำการเปลี่ยนแปลงไฟล์ระบบการทำงานบางส่วนหรือเต็มส่วน ไวรัสร่วมมือจะไม่ทำการเปลี่ยนแปลงไฟล์ แต่จะทำการสำเนา และเมื่อมีการเปิดไฟล์ที่ติดไวรัส ก็จะดำเนินการไวรัสที่ทำสำเนา ประเภทอื่นๆของไวรัสเช่น ไวรัสลิงค์ ไวรัส OBJ ที่แปลว่า โมดูลวัตถุติดเชื้อ ไวรัส VIB ที่แปลว่า ห้องสมุดรวบรวมการติดไวรัสและไวรัสที่เป็นเนื้อหาต้นฉบับที่ติดไวรัสของโปรแกรม

หนอนอินเทอร์เน็ต (Worm)

หลังจากที่มีการเข้าสู่ระบบ หนอนอินเทอร์เน็ต จะมีความคล้ายคลึงกับไวรัส ที่กระตุ้นตัวเองและกระทำการมุ่งร้าย หนอนอินเทอร์เน็ตสามารถไปตามช่องทางจากเครื่องหนึ่งสู่อีกเครื่องหนึ่ง แพร่พันธุ์ตัวเองและกระจายไปยังช่องทางข้อมูลต่างๆ

การจัดหมวดหมู่ของหนอนอินเทอร์เน็ต โดยการเพิ่มจำนวนอย่างรวดเร็วดังรายการแสดงตารางข่างล้างนี้

ตารางที่ 1 หมวดหมู่ของหนอนอินเทอร์เน็ตแบ่งตามการเพิ่มจำนวน

ประเภท	ชื่อ	คำอธิบาย
หนอนอีเมล์	หนอนอีเมล์ (E-mail worms)	หนอนอีเมล์ เป็นหนอนที่มาจากการรับส่งอีเมล์ ข้อความที่มีการติดเชื้อ จะมาจากการแนบไฟล์รวมทั้งมีการสำเนาหนอนอินเทอร์เน็ต หรือการลิงค์ไปให้อัพโหลดข้อมูลที่มีหนอนอินเทอร์เน็ต เว็บไซต์เหล่านั้นมีการปรับเปลี่ยน หรือเป็นของแฮกเกอร์ เมื่อมีการเปิดไฟล์ที่แนบไป หนอนอินเทอร์เน็ตก็จะเป็นการกระตุ้นหนอนอินเทอร์เน็ต หรืออีกวิธีหนึ่งคือ เมื่อคลิกที่ลิงค์ ดาวน์โหลดและเปิดไฟล์ หลังจากนั้นก็จะทำการแพร่ตัวเองโดยการหาอีเมล์ของคนอื่นและส่งข้อความที่ติดเชื้อนี้ออกไปอีก
หนอนที่มากับระบบการส่งข้อความทันที	IM Worms	หนอนจะทำการแพร่ไปยังระบบการส่งข้อความทันที (Instant messaging) เช่น ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager and Skype หนอนเหล่านี้จะทำการติดต่อกับรายชื่อผู้ติดต่อที่อยู่รายการชื่อและทำการส่งไฟล์และลิงค์ที่มีการติดเชื้อ เมื่อ

		ผู้ใช้ทำการดาวน์โหลดไฟล์และเปิดไฟล์ หนอนก็จะทำงาน
หนอนที่มากับโปรแกรม IRC	IRC Worms	หนอนอินเทอร์เน็ตประเภทนี้จะทำการแพร่เข้าสู่เครื่องคอมพิวเตอร์ของท่านโดยผ่านทางโปรแกรมสนทยา IRC ซึ่งอาศัยช่องทางการสื่อสารแบบเรียลไทม์บนอินเทอร์เน็ต หนอนอินเทอร์เน็ตนี้อยู่บนช่องทางการสนทนาบนอินเทอร์เน็ต ทั้งการทำสำเนาไฟล์ หรือการลิงค์ไปยังเว็บอื่น เมื่อผู้ใช้ทำการดาวน์โหลดไฟล์และเปิดไฟล์ หนอนก็จะทำงาน
หนอนที่มากับเครือข่าย	Net Worms	หนอนชนิดนี้ ทำการกระจายผ่านเครือข่ายของคอมพิวเตอร์ หนอนประเภทนี้มีความแตกต่างจากหนอนอินเทอร์เน็ต หนอนเครือข่ายมีการแพร่พันธุ์โดยไม่จำเป็นต้องการมีส่วนร่วมของผู้ใช้ หนอนจะทำการค้นหาเครือข่ายภายในสำหรับคอมพิวเตอร์ซึ่งมีช่องโหว่และอ่อนแอ และทำการกระจายออกไปยังเครือข่าย ด้วยรหัสหรือส่วนของรหัสไปยังแต่ละเครื่องคอมพิวเตอร์ หากเครื่องคอมพิวเตอร์มีความเสี่ยงในเครือข่ายก็จะทำการแทรกซึมโดยการส่งแพ็กเก็ต และเมื่อมีหนอนอยู่เต็มระบบหนอนก็จะปฏิบัติงานทันที
หนอนที่มากับโปรแกรม P2P	File exchange Worms	หนอนจากการแลกเปลี่ยนไฟล์ (File exchange worms) แพร่พันธุ์ผ่านทางเครือข่ายแบบ Peer to Peer เช่น Kazaa, Grokster, EDonkey, FastTrack หรือ Gnutella ในการใช้งานเครือข่ายเพื่อการแลกเปลี่ยนไฟล์ หนอนจะทำการสำเนาตัวเองเข้าสู่โฟลเดอร์ของไฟล์ที่ทำการแลกเปลี่ยน ซึ่งจะตั้งอยู่บนครื่องคอมพิวเตอร์

		หนอนอินเทอร์เน็ตที่มีความซับซ้อนมากกว่า ทำการเลียนแบบเน็ตเวิร์กโปรโตคอลของเน็ตเวิร์กที่มีการแลกเปลี่ยนไฟล์ และเสนอการสำเนาตัวเองเข้าไปแทนที่ไฟล์ที่ทำการแลกเปลี่ยนเพื่อให้ดาวน์โหลด
หนอนอินเทอร์เน็ต	หนอนอินเทอร์เน็ตอื่นๆ	หนอนอินเทอร์เน็ตอื่นๆ ประกอบไปด้วย • หนอนที่แพร่กระจายโดยการสำเนาตัวเองผ่านทางทรัพยากรเครือข่าย ใช้ความสามารถในการทำหน้าที่ของระบบปฏิบัติการ เข้าไปสู่โฟลเดอร์เน็ตเวิร์กที่กำลังทำงานอยู่ เชื่อมต่อไปยังเครื่องคอมพิวเตอร์ในเครือข่ายทั่วโลก และเข้าไปยังไดร์ฟ แตกต่างจากหนอนเครือข่ายคอมพิวเตอร์ ที่ผู้ใช้ต้องเปิดไฟล์จึงจะได้รับและทำการสำเนาจากนั้นหนอนจึงทำงาน

โปรแกรมโทรจัน (Trojan)

หมวดหมู่ย่อย: โทรจัน (โปรแกรมโทรจัน)

ระดับความรุนแรง: สูง

แตกต่างจากหนอนและไวรัส โปรแกรมโทรจันจะไม่มีการสร้างสำเนาซึ่งไม่เหมือนกับไวรัส หรือหนอนอินเทอร์เน็ต โทรจันมีผลต่อคอมพิวเตอร์ อย่างเช่นจากการที่ผู้ใช้งานส่งอีเมล์ หรือการเข้าเว็บไซต์เมื่อเข้าไปยังเว็บไซต์ที่มีเชื้ออยู่ โปรแกรมจะแสดงอาการมุ่งร้ายเมื่อมีการใช้งาน

โปรแกรมโทรจันมีการทำงานที่เป็นการกระทำมุ่งร้าย หน้าที่หลักของโทรจันคือ การหยุดชะงัดแปลงและการลบข้อมูล การขัดขวางการทำงานของระบบคอมพิวเตอร์หรือ เครือข่ายคอมพิวเตอร์ โปรแกรมโทรจันยังสามารถรับและส่งไฟล์ ดำเนินการ แสดงข้อความ การเข้าถึงเว็บเพจดาวน์โหลดและติดตั้งโปรแกรม รวมทั้งการเริ่มต้นคอมพิวเตอร์ที่ติดเชื้อ โทรจันเข้าในคอมพิวเตอร์ของเหยื่อโดยปราศจากการตรวจจับ

โดยทั่วไปจะอยู่ในรูปของไฟล์แนบอีเมล์ที่น่าเชื่อถือ เมื่อใดที่โทรจันถูกเปิดโดยผู้รับเมล์โดยปราศจากความสงสัย นักโจมตีระบบก็จะสามารถเข้าถึงข้อมูลที่เก็บอยู่ในเครื่องที่ไม่ได้จำกัดสิทธ์ผู้ใช้โทรจันสามารถอยู่ในรูปโปรแกรมที่ทำงานซ่อนอยู่ในคอมพิวเตอร์ หรือซ่อนตัวอยู่ในโปรแกรมที่ถูกต้องปลอดภัยหมายความว่าเป็นโปรแกรมที่ยูสเซอร์ไว้ใจการทำงานของฟังก์ชันต่างๆที่มี

ผู้บุกรุกมักใช้การติดตั้ง โปรแกรมโทรจันเข้าเป็นส่วนประกอบ

โปรแกรมโทรจันมีความแตกต่างกันไปตามลักษณะการคุกคามดังอธิบายได้ตามตารางข้างล่างต่อไปนี้

ตารางที่ 2 ประเภทของโทรจันที่แบ่งตามลักษณะการคุกคามบนเครื่องคอมพิวเตอร์

ประเภท	ชื่อ	คำอธิบาย
Trojan- ArcBomb	โปรแกรมโทรจัน- ระเบิดไฟล์สำรองข้อมูล(Archive Bomb)	ไฟล์สำรองข้อมูลเมื่อมีการขยายออกก็จะเพิ่มขนาดทำให้ขัดขวางการทำงานของเครื่องคอมพิวเตอร์ เมื่อท่านทำการขยายไฟล์สำรองข้อมูล คอมพิวเตอร์อาจทำงานช้าลงจนกระทั่งหยุดการทำงาน จานเก็บข้อมูลอาจเต็มไปด้วยข้อมูลว่างเปล่า ระเบิดไฟล์สำรองข้อมูล (Archive Bomb) เป็นอันตรายต่อเมล์เซิร์ฟเวอร์ หากว่ามีข้อมูลเข้ามาในระบบโดยอัตโนมัติ จนกลายเป็นระเบิดไฟล์สำรองข้อมูล (Archive Bomb) อาจทำให้หยุดการทำงานของเซิร์ฟเวอร์
ประตูหลัง (Backdoor)	โปรแกรมโทรจันในการควบคุมระบบจากระยะไกล (Remote administration Trojan programs)	โปรแกรมเหล่านี้ถือว่าเป็นโปรแกรมที่อันตรายที่สุดในบรรดาโปรแกรมโทรจันทั้งหมด หลักการทำงานอันชาญฉลาดที่มีความคล้ายคลึงกับโปรแกรมในการควบคุมระบบจากระยะไกล โปรแกรมทำการติดตั้งเองโดยที่ผู้ใช้งานไม่ทราบและให้ผู้บุกรุกเข้ามาทำการควบคุมระบบจากระยะไกล
โทรจัน (Trojans)	โทรจัน (Trojans)	โทรจันประกอบไปด้วย โปรแกรมมุ่งร้าย

		ดังต่อไปนี้ • **โปรแกรมโทรจันแบบดั้งเดิม** ทำหน้าที่หลักแบบโทรจัน ได้แก่ การขโมยข้อมูล การสกัดกั้น เปลี่ยนแปลงหรือลบข้อมูล รวมทั้งการขัดขวางการทำงานของระบบปฏิบัติการของเครื่องคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ จะไม่มีการทำลักษณะอื่นเพิ่มเติมเหมือนโปรแกรมโทรจันประเภทอื่นๆ ดังอธิบายไว้ในตาราง • **วัตถุประสงค์หลากหลาย** โปรแกรมโทรจัน ที่ทำหน้าที่อื่นๆเพิ่มเติม หลายประเภท
โทรจันข่มขู่เรียกค่าไถ่ (Trojan-Ransoms)	โปรแกรมโทรจันที่ต้องการข่มขู่ผู้ใช้เพื่อการเรียกค่าไถ่	โทรจันประเภทนี้ จะทำการจับเอาข้อมูลของเครื่องคอมพิวเตอร์เป็นตัวประกัน ดัดแปลงหรือหยุดการทำงาน หรือขัดขวางการทำงานของระบบปฏิบัติการคอมพิวเตอร์ หลังจากนั้นผู้บุกรุกทำการข่มขู่ผู้ใช้ให้ได้ตามต้องการเพื่อให้เกิดการแลกเปลี่ยนกับการทำลายข้อมูลของเครื่องที่เป็นตัวประกัน
Trojan- clickers	Trojan- clickers	โปรแกรมนี้เข้าถึงเครื่องคอมพิวเตอร์ของผู้ใช้จากการที่ผู้ใช้ทำการส่งคำสั่งไปยังเว็บบราวเซอร์หรือการแทนที่เว็บที่เก็บสะสมในไฟล์ระบบ การใช้โปรแกรมเหล่านี้ ผู้บุกรุกจะทำการจู่โจมเครือข่าย หรือเพิ่มการจราจรไปสู่บางส่วนของไซต์เพื่อให้ทำการแสดงแบนเนอร์โฆษณา
Trojan-Downloaders	โปรแกรม Trojan-Downloaders	โปรแกรมเหล่านี้ มีการเข้าถึงเว็บเพจของผู้บุกรุก การดาวน์โหลดโปรแกรมมุ่งร้ายตัวอื่น และติดตั้งลงบนเครื่องคอมพิวเตอร์ของผู้ใช้ ทั้งมีการเก็บชื่อไฟล์ของโปรแกรมที่เป็นโปรแกรมมุ่งร้ายด้วยรหัสของตัวเอง หรือการรับมาจากการเข้าหน้าเว็บที่มีโปรแกรมเหล่านี้

Trojan-Droppers	โปรแกรม Trojan-Droppers	โปรแกรมเหล่านี้เป็นการเก็บโปรแกรมโทรจันตัวอื่นๆ บนจานข้อมูลของเครื่องคอมพิวเตอร์และติดตั้งลงไป ผู้บุกรุกสามารถใช้ Trojan-Droppers ในการกระทำดังต่อไปนี้ • ติดตั้งโปรแกรมมุ่งร้ายโดยที่ผู้ใช้ไม่ทราบ เนื่องจาก Trojan-Droppers ไม่มีข้อความใดปรากฏในการติดตั้ง หรือการแสดงข้อความเท็จ ตัวอย่างเช่น การแจ้งให้ทราบเครื่องคอมพิวเตอร์เกิดปัญหา หรือการใช้งานระบบปฏิบัติการผิดเวอร์ชั่น • เพื่อไม่ให้โปรแกรมมุ่งร้ายสามารถสืบค้นได้ เพราะว่าโปรแกรมแอนตี้ไวรัสบางตัวก็ไม่สามารถตรวจจับโปรแกรมมุ่งร้ายที่แฝงอยู่ใน Trojan-Droppers
Trojan- Notifies	โปรแกรม Trojan- Notifies	โปรแกรมจะทำการแจ้งแก่ผู้บุกรุกว่า สามารถเชื่อมต่อเครื่องคอมพิวเตอร์ได้แล้ว และทำการโอนถ่ายข้อมูลจากเครื่องคอมพิวเตอร์ไปยังผู้บุกรุก ได้แก่ หมายเลข IP จำนวนพอร์ทที่เปิด หรือที่อยู่อีเมล์ โปรแกรมมีการสื่อสารกับผู้บุกรุก ผ่านทาง FTP อีเมล์ หรือทางหน้าเว็บของผู้บุกรุก Trojan- Notifies พบมากในโปรแกรมโทรจันที่ติดตั้งแบบสมบูรณ์ โปรแกรมจะทำการแจ้งว่าโปรแกรมโทรจันตัวอื่นมีการติดตั้งเสร็จสิ้นแล้วบนเครื่องคอมพิวเตอร์ของผู้ใช้
Trojan-Proxies	Trojan-Proxies	โปรแกรมนี้จะปล่อยให้ผู้บุกรุกเข้ามายังหน้าเว็บแบบไม่เปิดเผย โดยการใช้การระบุตัวตนของคอมพิวเตอร์ของผู้ใช้ และทำการส่งสแปมออกไป
Trojan-PSWs	โทรจันขโมยรหัสผ่าน	โทรจันขโมยรหัสผ่าน (Password Stealing

		Ware) เป็นโปรแกรมที่เข้ามาขโมยเอาบัญชีผู้ใช้ ตัวอย่างเช่น ข้อมูลการลงทะเบียน โปรแกรมจะทำการค้นหาข้อมูลที่เป็นความลับในไฟล์ระบบ และทำการลงทะเบียนส่งไปยังผู้คิดค้นโปรแกรม โดยการส่งอีเมล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก โทรจันบางโปรแกรมก็สามารถจำแนกได้ในหัวข้อนี้ รวมไปถึง Trojan-Bankers, Trojans-IMs และ Trojans-GameThieves
Trojan-Spies	โปรแกรมสายลับโทรจัน	โปรแกรมนี้ใช้สำหรับการสอดแนมผู้ใช้ โดยทำการสะสมข้อมูลเกี่ยวกับการกระทำของผู้ใช้คอมพิวเตอร์ ตัวอย่างเช่น เข้าไปดักข้อมูลการเข้าถึงยังแป้นพิมพ์ของผู้ใช้ การยิงสุ่มภาพแล้วจับเอารายการของโปรแกรมที่กำลังทำงาน หลังจากนั้นโปรแกรมได้รับข้อมูล ก็จะโอนถ่ายข้อมูลไปโดยการส่งอีเมล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก
Trojan-DoS	โปรแกรมโทรจันจู่โจมเครือข่าย	การโจมตีจู่โจมไม่ให้สามารถบริการได้ (DoS-Denial of Service) โทรจันจะทำการส่งการร้องขอจากเครื่องคอมพิวเตอร์ของผู้ใช้เป็นจำนวนมากไปยังเซิร์ฟเวอร์ทางไกล เมื่อเซิร์ฟเวอร์ได้รับการร้องขอจำนวนมากก็จะหยุดการทำงาน โปรแกรมนี้มักจะทำงานที่มาจากเครื่องคอมพิวเตอร์หลายเครื่อง เพื่อทำการโจมตีเซิร์ฟเวอร์
Trojan-IMs	โปรแกรมโทรจันขโมยข้อมูลส่วนบุคคลของผู้ใช้งานระบบส่งข้อความทันที	โปรแกรมนี้จะทำการขโมยเอาหมายเลขและรหัสผ่านของผู้ใช้บริการระบบส่งข้อความทันที (Instant messaging programs) ตัวอย่างเช่น ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager หรือ Skype โดยการส่งอีเมล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุก

		รุก
รูทคิทส์ (Rootkits)	รูทคิทส์ (Rootkits)	โปรแกรมเหล่านี้ จะซ่อนเร้นอยู่ในโปรแกรมมุ่งร้ายอื่นๆ การกระทำของโปรแกรมนี้คือการขยายบางโปรแกรมออกไปในระบบ ซ่อนไฟล์ กระบวนการในหน่วยความจำของเครื่องคอมพิวเตอร์ที่ติดเชื้อ หรือซ่อนการโอนถ่ายข้อมูลระหว่างโปรแกรมที่ติดตั้งลงในเครื่องคอมพิวเตอร์ของผู้ใช้ และเครื่องคอมพิวเตอร์อื่นๆ ในเครือข่าย
Trojan-SMS	โปรแกรมโทรจันข้อความบริการส่งข้อความ	โปรแกรมนี้เป็นโปรแกรมที่เกิดปัญหาในโทรศัพท์เคลื่อนที่ และทำการส่งข้อความจำนวนมากออกจากเครื่องโทรศัพท์ของผู้ใช้
Trojan-GameThieves	โปรแกรมโทรจันขโมยข้อมูลส่วนบุคคลของผู้ใช้งานเครือข่ายเกมส์	โปรแกรมนี้จะทำการขโมยข้อมูลบัญชีของผู้ใช้เกมส์เครือข่าย และทำการโอนถ่ายข้อมูลเหล่านี้ไปยังผู้บุกรุกโดยการส่งอีเมล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก
Trojan-Bankers	โปรแกรมโทรจันขโมยข้อมูลบัญชีธนาคาร	โปรแกรมนี้จะทำการขโมยข้อมูลบัญชีทางธนาคาร หรือข้อมูลบัญชีการเงินดิจิตอล หรืออิเล็กทรอนิกส์ และทำการโอนถ่ายข้อมูลเหล่านี้ไปยังผู้บุกรุก โดยการส่งอีเมล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก
Trojan-Mailfinders	โปรแกรมโทรจันสะสมที่อยู่อีเมล์	โปรแกรมนี้จะทำการสะสมที่อยู่อีเมล์บนเครื่องคอมพิวเตอร์ และทำการโอนถ่ายข้อมูลเหล่านี้ไปยังผู้บุกรุกโดยการส่งอีเมล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก ผู้บุกรุกจะใช้ที่อยู่อีเมล์เหล่านี้ในการส่งสแปมต่อไป

โปรแกรมอเนกประสงค์มุ่งร้าย *(Malicious tools)*

หมวดหมู่ย่อย: โปรแกรมอเนกประสงค์มุ่งร้าย

ระดับความรุนแรง: ปานกลาง

โปรแกรมอเนกประสงค์เหล่านี้ สร้างขึ้นเพื่อให้มีผลต่อคอมพิวเตอร์ ทำลายคอมพิวเตอร์ อย่างไรก็ตาม มีความแตกต่างจากโปรแกรมมุ่งร้ายอื่นๆ ที่ไม่ได้มีพฤติกรรมในการมุ่งร้ายเมื่อมีการดำเนินการโปรแกรม และยังคงมีความปลอดภัยเมื่ออยู่บนเครื่องคอมพิวเตอร์ของผู้ใช้ การกระทำที่แฮกเกอร์ใช้เพื่อการสร้างไวรัส หนอนอินเทอร์เน็ตและโทรจัน จัดการจู่โจมเครือข่ายโดยการรีโมตเซิร์ฟเวอร์ ดัดแปลงแก้ไขโปรแกรมการกระทำมุ่งร้ายอื่นๆ

ประเภทของโปรแกรมอเนกประสงค์มุ่งร้ายมีอยู่มากมายตามลักษณะของการทำงาน ดังอธิบายไว้ในตารางด้านล่างต่อไปนี้

ตารางที่ 3 ประเภทของโปรแกรมอเนกประสงค์มุ่งร้ายตามลักษณะการทำงาน

ประเภท	ชื่อ	คำอธิบาย
Constructor	ผู้สร้าง(Constructors)	ผู้สร้าง (Constructors) ใช้ในการสร้างไวรัส หนอนอินเทอร์เน็ต และโปรแกรมโทรจันตัวใหม่ๆ โปรแกรมผู้สร้างบางตัวมีหน้าตาเป็นวินโดว์ ที่ให้แฮกเกอร์สามารถเลือกสร้างประเภทของโปรแกรมมุ่งร้ายได้หลากหลาย วิธีการของโปรแกรมนี้ จะใช้การต้านการแก้ไขข้อบกพร่อง และคุณสมบัติอื่นๆที่คล้ายคลึงกัน
DoS	การจู่โจมเครือข่าย	การโจมตีจู่โจมไม่ให้สามารถบริการได้ (DoS-Denial of Service) การส่งการร้องขอจากเครื่องคอมพิวเตอร์ของผู้ใช้เป็นจำนวนมากไปยังเซิร์ฟเวอร์ทางไกล เมื่อเซิร์ฟเวอร์ได้รับการร้องขอจำนวนมากก็จะหยุดการทำงาน
Exploit	Exploit	Exploit เป็นโปรแกรมที่ได้รับการออกแบบมาเพื่อให้ทำการเจาะระบบโดยอาศัย ช่องโหว่ของ

		โปรแกรม หรือช่องโหว่ต่างๆเพื่อที่จะเข้ามาทำการครอบครอง หรือควบคุมคอมพิวเตอร์ เพื่อที่จะให้กระทำการบางอย่าง ตัวอย่างเช่น Exploit สามารถเขียน หรืออ่านไฟล์ หรือพาไปยังเว็บที่ติดเชื้อ Exploit ที่แตกต่างกันจะใช้ช่องโหว่ของโปรแกรมที่แตกต่างกัน หรือบริการเครือข่ายที่ต่างกัน Exploit ที่ส่งผ่านไปทางเครือข่ายจะไปยังเครื่องคอมพิวเตอร์ต่างๆ ตามรูปแบบของแพ็กเก็ตของเครือข่าย การค้นหาเครื่องคอมพิวเตอร์ในเครือข่ายที่อ่อนแอ ตัวอย่างเช่น Exploit เข้ามาในไฟล์เอกสาร เพื่อหาช่องโหว่ของเนื้อหาในไฟล์เอกสาร (DOC) เมื่อผู้ใช้เปิดใช้งานไฟล์เอกสารที่ติดเชื้อ ก็จะปฏิบัติการตามคำสั่งของผู้บุกรุก สามารถเข้ามามาในระบบได้แล้วก็จะเริ่มทำการเปลี่ยนแปลงข้อมูลในระบบ ข้อมูลของระบบ หรือว่าโปรแกรมของเซิร์ฟเวอร์ เพื่อให้ส่งข้อมูลไปหาตัวเอง หรือว่าเพื่อให้ Exploit สามารถเข้ามาสู่ระบบได้อีก ครั้งหนึ่งถึงแม้ว่าช่องโหว่เดิมได้ถูกปิดไปแล้ว Exploit สามารถเข้าอยู่ในเนื้อความของอีเมล์เพื่อหาช่องโหว่ที่อยู่ในโปรแกรมอีเมล์ และเริ่มการกระทำมุ่งร้ายตราบเท่าที่ผู้ใช้งานเปิดไฟล์ที่ติดเชื้อนี้ Exploit สามารถใช้การแพร่กระจายผ่านทางหนอนเครือข่าย Exploit-Nukers เป็นแพ็กเก็ตเครือข่ายที่ทำให้เครื่องคอมพิวเตอร์ทำงานไม่ได้
FileCryptors	ตัวเข้ารหัสไฟล์(File Cryptors)	ตัวเข้ารหัสไฟล์ (File Cryptors) ทำการสร้างรหัสลับโปรแกรมมุ่งร้ายอื่น เพื่อซ่อนไม่ให้แอนตี้ไวรัสมองเห็น
Flooders	โปรแกรมทำให้เครือข่ายท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากผ่านยังช่องทางเครือข่าย รวมไปถึงช่องทางการ

		สนทนา IRC อย่างไรก็ตาม หมวดหมู่ของโปรแกรมมุ่งร้ายนี้ไม่ได้รวมถึงการทำให้ อีเมล์ การส่งข้อความทันที หรือการส่งข้อความท่วมท้น ซึ่งแยกหมวดหมู่เอาไว้ดังตารางข้างล่าง (Email-Flooder, IM-Flooder และ SMS-Flooder).
HackTools	เครื่องมือเจาะโปรแกรม (Hacking Tools)	เครื่องมือเจาะโปรแกรม (Hacking Tools) จะให้เพื่อการเจาะเครื่องคอมพิวเตอร์ที่มีโปรแกรมนี้อยู่ หรือเพื่อการเตรียมการเจาะเครื่องคอมพิวเตอร์เครื่องอื่น เช่น การสร้างบัญชีผู้ใช้ระบบใหม่ที่ไม่ได้รับอนุญาต หรือการล้างข้อมูลบันทึกเพื่อปิดบังว่ามีผู้ใช้ใหม่ขึ้นมาในระบบ บางครั้งก็มีการแสดงการทำงานที่มุ่งร้าย ตัวอย่างเช่น การระงับรหัสผ่าน โปรแกรมสนิฟเฟอร์ (Sniffers) เป็นโปรแกรมซึ่งทำหน้าที่ดักจับแพ็กเกตในเครือข่าย
not-virus: Hoax	โปรแกรม Hoax	โปรแกรมเหล่านี้ทำให้ผู้ใช้หวาดกลัวด้วยข้อความเหมือนไวรัส โปรแกรมทำการตรวจค้นไวรัสในไฟล์ หรือแสดงข้อความเกี่ยวกับการฟอร์แมตจานข้อมูลทั้งที่ไม่ได้มีเกิดขึ้น
Spoofers	การปลอมแปลง (Spoofers)	โปรแกรมเหล่านี้จะทำการส่งข้อความการร้องขอของเครือข่าย ด้วยที่อยู่ของผู้ส่งที่ปลอมแปลงขึ้น ผู้บุกรุกใช้การปลอมแปลงนี้เป็นคำสั่ง ตัวอย่างเช่น การทำเหมือนว่าเป็นผู้ส่งจริง
VirTools	เครื่องมือที่ใช้ในการสร้างปรับเปลี่ยนโปรมแกรมมุ่งร้าย	โปรแกรมนี้ทำให้มีโอกาสในการเปลี่ยนแปลงโปรแกรมมุ่งร้ายอื่นๆ เพื่อซ่อนโปรแกรมมุ่งร้ายจากโปรแกรมต่อต้านไวรัส
Email-Flooders	โปรแกรมทำให้อีเมล์ท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากไปยังที่อยู่อีเมล์ ทำให้เกิดการไหลของข้อมูลจำนวนมาก ทำให้ผู้ใช้ ไม่สามารถรับอีเมล์ที่เข้ามาแล้วไม่ใช่สแปมได้

IM-Flooders	โปรแกรมทำให้ระบบส่งข้อความทันทีท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากไปยังระบบส่งข้อความทันที(Instant messaging) เช่น ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager and Skype ทำให้ผู้ใช้ไม่สามารถรับข้อความที่เข้ามาแล้วไม่ใช่สแปมได้
SMS-Flooders	โปรแกรมทำให้ข้อความบริการส่งข้อความท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากไปยังบริการส่งข้อความบนโทรศัพท์เคลื่อนที่

โปรแกรมซึ่งอาจไม่พึงประสงค์

โปรแกรมซึ่งอาจไม่พึงประสงค์ แตกต่างจากโปรแกรมมุ่งร้าย และไม่ได้ต้องการทำให้เกิดความเสียหาย อย่างไรก็ตาม ก็เป็นการผิดต่อความปลอดภัยของคอมพิวเตอร์

โปรแกรมซึ่งอาจไม่พึงประสงค์ ประกอบไปด้วย ซอฟต์แวร์โฆษณา โปรแกรมเกี่ยวข้องกับเรื่องเพศ โปรแกรมที่มีความเสี่ยงอื่นๆ

ซอฟต์แวร์โฆษณา เป็นการแสดงข้อความโฆษณาส่งถึงผู้ใช้

โปรแกรมเกี่ยวข้องกับเรื่องเพศ แสดงข้อมูลทางเพศส่งถึงผู้ใช้

โปรแกรมที่มีความเสี่ยงอื่นๆ เป็นโปรแกรมที่เป็นประโยชน์ต่อผู้ใช้คอมพิวเตอร์ อย่างไรก็ตาม หากผู้บุกรุกเข้ามาล่วงล้ำด้วยโปรแกรมเหล่านี้ หรือเข้ามาติดตั้งลงในเครื่องคอมพิวเตอร์ของผู้ใช้ ก็จะเป็นการผิดต่อความปลอดภัยของคอมพิวเตอร์

โปรแกรมซึ่งอาจไม่พึงประสงค์จะมีวิธีการในการติดตั้งลงเครื่องคอมพิวเตอร์อยู่สองวิธีดังต่อไปนี้

- ติดตั้งเองโดยผู้ใช้ ร่วมกับการติดตั้งโปรแกรมอื่น หรือติดตั้งโปรแกรมเดียวตัวอย่างเช่น นักพัฒนาซอฟต์แวร์ร่วมกับโปรแกรมโฆษณาที่ติดมากับซอฟต์แวร์ฟรี และแชร์แวร์
- การติดตั้งโดยผู้บุกรุก ตัวอย่างเช่น รวมมาในโปรแกรมที่เป็นโปรแกรมมุ่งร้ายอื่นๆ โดยการอาศัยช่องโหว่ของเว็บบราวเซอร์ หรือตัวดาวน์โหลดโทรจันหรือดรอปเปอร์ เมื่อผู้ใช้เข้ามายังเว็บไซต์ที่มีการติดเชื้อ

ซอฟต์แวร์โฆษณา (Adware)

หมวดหมู่ย่อย: ซอฟต์แวร์โฆษณา (Adware)

ระดับความรุนแรง: ปานกลาง

ซอฟต์แวร์โฆษณา (Adware) เป็นการแสดงข้อมูลโฆษณาแก่ผู้ใช้ โดยการแสดงแบนเนอร์ของตนเองบนหน้าต่างการใช้งานของโปรแกรมอื่น แล้วเปลี่ยนไปยังเว็บไซต์โฆษณาที่ทำการค้นหาตามคำขอ บางซอฟต์แวร์โฆษณา (Adware) ก็ทำการสะสมข้อมูลทางการตลาดเกี่ยวกับผู้ใช้ส่งไปยังผู้พัฒนาซอฟต์แวร์โฆษณา (Adware) ซึ่งเว็บไซต์ที่เข้าไป หรือจากการค้นหาตามคำขอ แตกต่างจากสายลับโทรจันที่ข้อมูลเหล่านี้ส่งออกมาจากการได้รับความยินยอมของผู้ใช้

โปรแกรมเกี่ยวข้องกับเรื่องเพศ (Pornware)

หมวดหมู่ย่อย: โปรแกรมเกี่ยวข้องกับเรื่องเพศ(Pornware)

ระดับความรุนแรง: ปานกลาง

โดยทั่วไปแล้ว ผู้ใช้งานมักติดตั้งโปรแกรมเหล่านี้ด้วยตัวเองจากการค้นหา หรือดาวน์โหลดข้อมูลที่เกี่ยวกับเรื่องเพศ

ผู้บุกรุกก็สามารถทำการติดตั้งโปรแกรมเหล่านี้ที่เครื่องคอมพิวเตอร์ของผู้ใช้ เพื่อแสดงการโฆษณารูปแบบการค้าและการบริการเรื่องเพศแก่ผู้ใช้ โดยปราศจากการยินยอมของผู้ใช้ ในการติดตั้งผู้บุกรุกจะ

อาศัยช่องโหว่ของระบบปฏิบัติการหรือเว็บบราวเซอร์ แล้วทำการแพร่กระจายตัวดาวน์โหลดโทรจัน หรือ ดรอปเปอร์

โปรแกรมเกี่ยวข้องกับเรื่องเพศ(Pornware) มีอยู่ 3 ประเภทตามตารางแสดงด้านล่างนี้

ตารางที่ 4 ประเภทของโปรแกรมเกี่ยวกับเรื่องเพศ (Pornware)

ประเภท	ชื่อ	คำอธิบาย
Porn-Dialers	การโทรออกเองอัตโนมัติ	โปรแกรมนี้ประกอบไปด้วย เบอร์โทรศัพท์ของบริการทางด้านเรื่องเพศ และจะทำการโทรออกเองโดยอัตโนมัติแตกต่างจาก Trojan dialers ที่จะมีการแจ้งให้ผู้ใช้ทราบก่อน
Porn-Downloaders	โปรแกรมสำหรับการดาวน์โหลดผ่านทางอินเทอร์เน็ต	โปรแกรมดาวน์โหลดข้อมูลในเรื่องเพศเข้าสู่เครื่องคอมพิวเตอร์ของผู้ใช้ แตกต่างจาก Trojan Downloaders ที่จะมีการแจ้งให้ผู้ใช้ทราบก่อน
Porn-tools	เครื่องมือ	ใช้เพื่อการค้นหา และแสดงภาพทางเพศ อันประกอบไปด้วย แถบเครื่องมือบราวเซอร์ และเครื่องเล่นวีดีโอแบบพิเศษ

โปรแกรมที่มีความเสี่ยงอื่นๆ

หมวดหมู่ย่อย: โปรแกรมทีมีความเสี่ยงอื่นๆ

ระดับความรุนแรง: ระดับกลาง

ส่วนมากแล้วโปรแกรมเหล่านี้ มีใช้กันด้วยความคุ้นเคย มีรวมไปถึง โปรแกรมสนทนา IRC ตัวหมุนโทรออก โปรแกรมการจัดการดาวน์โหลดไฟล์ ตัวเฝ้าดูการทำงานของระบบคอมพิวเตอร์ โปรแกรมอเนกประสงค์ในการจัดการรหัสผ่าน FTP HTTP หรือเซิร์ฟเวอร์เทลเน็ท

อย่างไรก็ตาม หากว่าผู้บุกรุกเข้ามาล่วงล้ำผ่านทางโปรแกรมเหล่านี้ หรือติดตั้งลงบนคอมพิวเตอร ผู้ใช้ก็จะเป็นการฝ่าฝืนต่อความปลอดภัยของคอมพิวเตอร์

ตารางแสดงโปรแกรมที่มีความเสี่ยง แบ่งกลุ่มตามหน้าที่

ตารางที่ 5 ประเภทของโปรแกรมที่มีความเสี่ยงแบ่งกลุ่มตามหน้าที่

ประเภท	ชื่อ	คำอธิบาย
Client-IRC	โปรแกรมการสนทนากับลูกข่าย	ผู้ใช้งานทำการติดตั้งโปรแกรมเพื่อการสื่อสารผ่านทาง IRC ผู้บุกรุกอาศัยช่องทางนี้ในการแพร่กระจายโปรแกรมมุ่งร้าย
Dialers	โปรแกรมหมุนโทรออกอัตโนมัติ	โปรแกรมนี้จะทำการซ่อนตัวติดตั้งการเชื่อมต่อผ่านทางโมเด็ม
Downloaders	Downloaders	โปรแกรมเหล่านี้สามารถดาวน์โหลดไฟล์จากเว็บไซต์
Monitors	Monitors	โปรแกรมเหล่านี้ทำการเฝ้าดูการกระทำของคอมพิวเตอร์ที่มีการติดตั้ง รวมไปถึงการเฝ้าดูการทำงานของโปรแกรม และการแลกเปลี่ยนข้อมูลกับโปรแกรมบนเครื่องคอมพิวเตอร์เครื่องอื่น
PSWTools	เครื่องมือกู้คืนรหัสผ่าน	โปรแกรมเหล่าใช้เพื่อทำการดูและกู้คืนรหัสผ่านที่จำไม่ได้ ผู้บุกรุกจะใช้ในวิธีการเดียวกันเมื่อทำการติดตั้งโปรแกรมบนคอมพิวเตอร์ของผู้ใช้

RemoteAdmin	โปรแกรมในการควบคุมระบบจากระยะไกล	โปรแกรมนี้มีการใช้งานอย่างมากจากผู้ดูแลระบบ ที่ทำการเข้าถึงคอมพิวเตอร์ด้วยการควบคุมระยะไกล เพื่อการเฝ้าดูและจัดการ ผู้บุกรุกใช้โปรแกรมนี้ในวิธีการเดียวกันเมื่อทำการติดตั้งโปรแกรมบนคอมพิวเตอร์ของผู้ใช้ โปรแกรมที่มีความเสี่ยงในการควบคุมระบบจากระยะไกล มีความแตกต่างจากโทรจัน (หรือว่าประตูหลัง) โปรแกรมโทรจันสามารถแทรกเข้ามาได้อย่างเป็นอิสระภายในระบบ และทำการติดตั้งตัวเอง โปรแกรมที่ถูกต้องตามกฎหมายไม่มีการทำงานนี้
Server-FTP	FTP Servers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น FTP servers ผู้บุกรุกจะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้เพื่อทำการควบคุมระยะไกลผ่านทางโปรโตคอล FTP
Server-Proxy	Proxy servers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น Proxy servers ผู้บุกรุกจะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้เพื่อทำการควบคุมระยะไกลผ่านทางโปรโตคอล Proxy
Server-Telnet	Telnet servers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น Telnet servers ผู้บุกรุกจะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้เพื่อทำการควบคุมระยะไกลผ่านทางโปรโตคอล Telnet
Server-Web	Web servers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น Web servers ผู้บุกรุกจะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้เพื่อทำการควบคุมระยะไกลผ่านทางโปรโตคอล HTTP
RiskTool	เครื่องมือคอมพิวเตอร์ภายใน	เครื่องมือเหล่านี้ทำให้ผู้ใช้มีความสามารถเพิ่มเติมในการทำงานภายในเครื่องคอมพิวเตอร์ของผู้ใช้ โปรแกรมนี้ยอมให้แฮกเกอร์แอบแฝงไฟล์เข้ามา แอบแฝงหน้าต่างโปรแกรม หรือการปิดการดำเนินการที่กำลังทำอยู่
NetTool	เครื่องมือเครือข่าย	เครื่องมือเหล่านี้ยอมให้ผู้ใช้จัดการเครื่องคอมพิวเตอร์เครื่องอื่นๆในเครือข่าย ตัวอย่าง กธรีสตาร์ทตัวเอง การค้นหาพอร์ทที่เปิด หรือการดำเนินการโปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์เหล่านี้
Client-P2P	โปรแกรมลูกข่ายแบบ Peer to peer	โปรแกรมเหล่านี้ใช้สำหรับการจัดการระบบเครือข่ายแบบ Peer to Peer ผู้บุกรุกสามารถใช้เพื่อปล่อยโปรแกรม

		มุ่งร้าย
Client-SMTP	SMTP clients	โปรแกรมเหล่านี้ ทำการส่งข้อความทางอีเมล์ และซ่อนการกระทำเอาไว้ในอีเมล์ เพื่อส่งสแปมไปยังผู้ใช้ที่มีการระบุ
WebToolbar	แถบเครื่องมือเว็บ	โปรแกรมเหล่านี้มีการเพิ่มเติมแถบเครื่องมือการค้นหาเพื่อไปยังแถบเครื่องมือบราวเซอร์อื่น
FraudTool	โปรแกรมการหลอกลวง	โปรแกรมเหล่านี้มีการอำพรางโปรแกรมจริงตัวอื่น ตัวอย่างเช่น โปรแกรมป้องกันไวรัสแบบปลอม มีการแฝงการตรวจสอบซอฟต์แวร์มุ่งร้าย แต่ไม่ได้ค้นหาหรือไม่ได้ทำการกำจัดแต่อย่างใด

วิธีการป้องกันการติดโปรแกรมที่น่าสงสัยเป็นอันตรายโดยโปรแกรม

คาร์ปาสกี้แอนตี้ไวรัส ทำการค้นหาโปรแกรมมุ่งร้ายโดยใช้วิธีการ 2 วิธี คือ การค้นหาแบบตอบสนอง (โดยการใช้ฐานข้อมูล) และการค้นหาแบบเชิงรุก (ใช้การวิเคราะห์แบบฮิวริสติก)

ฐานข้อมูลของโปรแกรมประกอบไปด้วยการรายงานที่ระบุภุยคุกคามกว่าพัน ที่ได้รับจากการตรวจสอบ รายงานนี้ประกอบไปด้วยข้อมูลที่มาจากทั้งส่วนของการควบคุม และอัลกอริทึมสำหรับการกำจัดโปรแกรมเหล่านี้ ตัววิเคราะห์แอนตี้ไวรัสของคาร์ปาสกี้แลปทำการวิเคราะห์โปรแกรมมุ่งร้ายใหม่ๆ เป็นร้อยๆโปรแกรมประจำทุกวัน สร้างการรายงานผลและระบุตัวตน รวมทั้งมีการอัพเดทในไฟล์ฐานข้อมูล

การติดตั้งโปรแกรม

โปรแกรมนี้เป็นโปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์แบบมีการโต้ตอบกับเครื่องคอมพิวเตอร์โดยการใช้วิซาร์ดการติดตั้งโปรแกรม

<u>คำเตือน!</u>

ขอแนะนำให้ท่านทำการปิดโปรแกรมที่กำลังทำงานก่อนเริ่มต้นการติดตั้ง

ติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์โดยการดำเนินการกับไฟล์ที่มีชื่อ .exe

<u>หมายเหตุ</u>

การติดตั้งโปรแกรมจากการดาวน์โหลดไฟล์ผ่านทางอินเทอร์เน็ต นั้นเหมือนกับการดาวน์โหลดไฟล์บน CD

โปรแกรมการติดตั้งจะดำเนินการบนหน้าต่างวิซาร์ดมาตรฐาน แต่ละหน้าต่างจะประกอบไปด้วยปุ่มควบคุมกระบวนการติดตั้ง ต่อไปนี้จะเป็นการอธิบายความหมายของปุ่มควบคุมเหล่านี้

- Next หมายถึง การยอมรับการกระทำนั้น และดำเนินการต่อไปยังขั้นตอนต่อไปในกระบวนการติดตั้ง
- Previous หมายถึง การย้อนกลับไปยังขั้นตอนก่อนหน้านี้
- Cancel หมายถึง การยกเลิกการติดตั้ง
- Finish หมายถึง กระบวนการติดตั้งเสร็จสมบูรณ์

รายละเอียดเพิ่มเติมของแต่ละขั้นตอนมีดังต่อไปนี้

เนื้อหาในส่วนนี้ประกอบไปด้วย

ขั้นตอนที่1 ค้นหาโปรแกรมเวอร์ชั่นล่าสุด

ขั้นตอนที่2 ตรวจสอบความต้องการของระบบ

ขั้นตอนที่3 หน้าต่างการเริ่มต้นวิซาร์ด

ขั้นตอนที่4 ข้อตกลงทางด้านลิขสิทธิ์

ขั้นตอนที่5 เลือกประเภทของการติดตั้ง

ขั้นตอนที่6 เลือกโฟลเดอร์การติดตั้ง

ขั้นตอนที่7 เลือกส่วนประกอบโปรแกรมเพื่อทำการติดตั้ง

ขั้นตอนที่8 ค้นหาซอฟต์แวร์แอนตี้ไวรัสตัวอื่น

ขั้นตอนที่9 ขั้นตอนสุดท้ายของการตรียมติดตั้ง

ขั้นตอนที่10 เสร็จสิ้นการติดตั้ง

ขั้นตอนที่ 1 ค้นหาโปรแกรมเวอร์ชั่นล่าสุด

ก่อนทำการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ของท่าน วิซาร์ดการติดตั้งของคาร์ปาสกี้แลป จะเข้าทำการตรวจสอบค้นหาโปรแกรมเวอร์ชั่นล่าสุดบนเซิร์ฟเวอร์ของคาร์ปาสกี้แลป

หากไม่พบว่ามีโปรแกรมเวอร์ชั่นที่ใหม่กว่า วิซาร์ดจะเริ่มดำเนินการติดตั้งเวอร์ชั่นปัจจุบันที่มีอยู่

หากพบว่ามีเวอร์ชั่นที่ใหม่กว่าบนเซิร์ฟเวอร์ของคาร์ปาสกี้แลป ระบบจะขอให้ท่านทำการดาวน์โหลดและติดตั้ง หากท่านยกเลิกการดาวน์โหลด วิซาร์ดจะเริ่มดำเนินการติดตั้งเวอร์ชั่นปัจจุบันที่มีอยู่หากท่านทำการดาวน์โหลดเวอร์ชั่นที่ใหม่กว่า ก็จะทำการดาวน์โหลดไฟล์การติดตั้งลงบนเครื่องคอมพิวเตอร์ของท่าน และวิซาร์ดการติดตั้งก็จะเป็นของเวอร์ชั่นใหม่อย่างอัตโนมัติ สำหรับรายละเอียดการติดตั้งของเวอร์ชั่นใหม่ กรุณาดูที่เอกสารของเวอร์ชั่นใหม่

ขั้นตอนที่ 2 ตรวจสอบความต้องการของระบบ

ก่อนการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ วิซาร์ดจะทำการยืนยันความต้องการขั้นต่ำของระบบ (ดูได้จากส่วนของ **ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ**) เพื่อทำการยืนยันความต้องการของระบบที่ถูกต้องในการติดตั้งซอฟต์แวร์

หากว่าไม่มีตามความต้องการของระบบ จะมีการแสดงข้อความขึ้น แนะนำให้ท่านทำการอัพเดทโดยการใช้ Window Update และลงโปรแกรมที่ตรงตามความต้องการของระบบ ก่อนการติดตั้งคาร์ปาสกี้แอนตี้ไวรัสอีกครั้ง

ขั้นตอนที่ 3 หน้าต่างการเริ่มต้นวิซาร์ด

หากระบบของท่านตรงตามความต้องการของระบบ (ดูได้จากส่วนของ **ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ**) และไม่มีโปรแกรมเวอร์ชั่นที่ใหม่กว่า จากการตรวจสอบค้นหาโปรแกรมเวอร์ชั่นล่าสุดบนเซิร์ฟเวอร์ของคาร์ปาสกี้แลป หรือท่านได้ยกเลิกการดาวน์โหลด วิซาร์ดจะเริ่มดำเนินการติดตั้งเวอร์ชั่นปัจจุบันที่มีอยู่

เมื่อปรากฏกรอบสนทนาแรกของวิซาร์ดการติดตั้งบนหน้าจอ แสดงว่ากำลังเข้าสู่ขั้นตอนการติดตั้ง

เริ่มกระบวนการติดตั้งโดยการกดปุ่ม Next ยกเลิกการติดตั้งกดปุ่ม Cancel

ขั้นตอนที่ 4 ข้อตกลงทางด้านลิขสิทธิ์

กรอบสนทนาต่อไปของวิซาร์ดแสดงข้อตกลงทางด้านลิขสิทธิ์ ระหว่างท่านและคาร์ปาสกี้แลป อ่านโดยระเอียดและหากท่านยอมรับข้อตกลงและเงื่อนไขแล้วให้เลือกที่ I accept the terms of the license agreement และกดปุ่ม Next เพื่อดำเนินการติดตั้งต่อไป

ยกเลิกการติดตั้งกดปุ่ม Cancel

ขั้นตอนที่ 5 เลือกประเภทของการติดตั้ง

ระหว่างขั้นตอนนี้จะมีคำถามให้ท่านเลือกประเภทของการติดตั้งที่เหมาะสมสำหรับท่านดังนี้

- **การติดตั้งด่วน** (Express installation) หากท่านเลือกการติดตั้งนี้ จะทำการติดตั้งโปรแกรมทั้งหมดลงบนเครื่องคอมพิวเตอร์ของท่าน รวมทั้งการตั้งค่าป้องกันเริ่มต้นที่ทางคาร์ปาสกี้แลปแนะนำ เมื่อการติดตั้งเสร็จสิ้น จะเริ่มต้นวิซาร์ดการตั้งค่าโปรแกรมขึ้น
- **การติดตั้งแบบเลือกเอง** (Custom installation) หากท่านเลือกการติดตั้งนี้ ระบบจะถามให้ท่านเลือกส่วนที่ท่านต้องการเลือกลง เพื่อระบุไฟล์ของโปรแกรมที่ท่านต้องการ (ดูที่ขั้นตอนที่ 6 เลือกโฟลเดอร์การติดตั้ง) เพื่อเริ่มการทำงานของโปรแกรม และการตั้งค่าการใช้งานโดยซาร์ดการตั้งค่าโปรแกรม

หากท่านเลือกการติดตั้งแบบแรก วิซาร์ดการติดตั้งโปรแกรมจะข้ามไปยังขั้นตอนที่ 8 (ดูที่ ขั้นตอนที่ 8 ค้นหาซอฟต์แวร์แอนตี้ไวรัสตัวอื่น) ถ้าเป็นอีกแบบการติดตั้ง ท่านสามารถทำตามขั้นตอนตามแต่ละขั้นตอนของการติดตั้ง

ขั้นตอนที่ 6 เลือกโฟลเดอร์การติดตั้ง

<u>หมายเหตุ</u>

ขั้นตอนของวิซาร์ดการติดตั้งนี้ แสดงให้เห็นหากท่านเลือกการติดตั้งแบบเลือกเอง (Custom installation) (ดูที่ ขั้นตอนที่ 5 เลือกประเภทของการติดตั้ง)

ในขั้นตอนนี้จะมีคำถามให้ท่านระบุโฟลเดอร์ของการติดตั้งบนเครื่องคอมพิวเตอร์ที่ต้องการติดตั้ง เส้นทางคำสั่งเริ่มต้นคือ

- <Drive> \ Program Files \ Kaspersky Lab \ Kaspersky Anti-Virus 2009 – for 32-bit systems.
- <Drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2009 – for 64-bit systems.

ท่านสามารถระบุโฟลเดอร์ที่แตกต่างจากนี้โดยการเลือกปุ่ม Browse และเลือกโฟลเดอร์ในกล่องสนทนาโฟลเดอร์มาตรฐาน หรือเข้าไปยังทางผ่านของโฟลเดอร์

<u>คำเตือน!</u>

โปรดสังเกตว่า หากว่าท่านเลือกการเข้าเส้นทางคำสั่งด้วยมือสู่โฟลเดอร์การติดตั้ง ความยาวของอักขระจะต้องไปเกิน 200 อักขระ และต้องไม่มีเส้นทางเป็นคำสั่งที่มีอักขระพิเศษ

กดปุ่ม Next เพื่อการติดตั้งต่อไป

ขั้นตอนที่ 7 เลือกส่วนประกอบโปรแกรมเพื่อทำการติดตั้ง

<u>หมายเหตุ</u>

ขั้นตอนของวิซาร์ดการติดตั้งนี้ แสดงให้เห็นหากท่านเลือกการติดตั้งแบบเลือกเอง (Custom installation) (ดูที่ ขั้นตอนที่ 5 เลือกประเภทของการติดตั้ง)

ในการติดตั้งแบบเลือกเอง ท่านจะต้องทำการเลือกส่วนประกอบโปรแกรมเพื่อทำการติดตั้งตามที่ท่านต้องการลงบนเครื่องคอมพิวเตอร์ โดยค่าเริ่มต้น ทุกส่วนประกอบของโปรแกรมจะตั้งเอาไว้ที่ การปกป้อง การตรวจสอบและการอัพเดทไฟล์โปรแกรมที่ท่านต้องการ

ข้อมูลที่มีอยู่เกี่ยวกับแต่ละส่วนประกอบของโปรแกรม จะมีส่วนช่วยท่านในการเลือกตัดสินใจลงตามที่ท่านต้องการ เลือกส่วนประกอบจากรายการและอ่านรายละเอียดข้อมูลจากกรอบด้านล่าง ข้อมูลจะเป็นการอธิบายคร่าวๆ เกี่ยวกับส่วนประกอบรวมทั้งข้อมูลพื้นที่ของหน่วยเก็บข้อมูลที่ต้องการหากทำการติดตั้ง

ก่อนทำการติดตั้งส่วนประกอบใดๆ ให้ทำการเปิดเมนูลัด โดยการคลิกที่สัญลักษณ์หน้าชื่อของส่วนประกอบ และเลือกที่รายการ Component will not be available พึงระวัง หากท่านเลือกยกเลิกการติดตั้งส่วนประกอบใดๆ รายการนั้นจะไม่มีการป้องกันจากโปรแกรมที่เป็นอันตราย

การเลือกส่วนประกอบของการติดตั้งโปรแกรม เปิดที่เมนูลัดโดยการคลิกที่สัญลักษณ์ถัดไปต่อจากชื่อของส่วนประกอบ และเลือกที่ Component will be installed on local hard drive

เมื่อเสร็จสิ้นการเลือกไฟล์ที่ต้องการติดตั้ง กดที่ปุ่ม Next หากต้องการย้อนกลับเลือกรายการของส่วนประกอบตามค่าเริ่มต้น ให้กดปุ่ม Clear

ขั้นตอนที่ 8 ค้นหาซอฟต์แวร์แอนตี้ไวรัสตัวอื่น

ในขั้นตอนนี้ วิซาร์ดจะทำการค้นหาโปรแกรมแอนตี้ไวรัสตัวอื่น รวมทั้งโปรแกรมอื่นของคาร์ปาสกี้แลป ที่จะเป็นการทำงานขัดกับโปรแกรม

หากพบว่ามีโปรแกรมใดๆ บนเครื่องคอมพิวเตอร์ของท่าน จะมีการแสดงรายการให้เห็นบนจอ และจะมีการถามให้ท่านเลือกลบโปรแกรมเหล่านั้นทิ้ง ก่อนการดำเนินการติดตั้ง

หากว่ารายการของโปรแกรมแอนตี้ไวรัสที่ตรวจพบได้ รวมไปถึงโปรแกรม 7.0 ของคาร์ปาสกี้แลป มีการบันทึกไฟล์คีย์ในตอนที่ทำการลบทิ้งไป ท่านสามารถใช้คีย์นี้สำหรับเวอร์ชันปัจจุบัน เราขอแนะนำให้ท่านเก็บรักษาแยกเอาไว้และในที่เก็บหน่วยเก็บสำรอง วัตถุเหล่านี้จะเคลื่อนย้ายอัตโนมัติเมื่อมีการแยกออกจากเวอร์ชั่นปัจจุบัน และสามารถทำการตรวจสอบซ้ำหลังการติดตั้ง

หากเลือกการลบทิ้งคาร์ปาสกี้เวอร์ชั่น 7.0 แบบอัตโนมัติ จะมีการบันทึกข้อมูลการเริ่มต้นโปรแกรม และการนำกลับมาใช้ใหม่ในระหว่างการติดตั้งเวอร์ชัน 2009

<u>คำเตือน!</u>

โปรแกรมนี้ยอมรับไฟล์คีย์สำหรับเวอร์ชั่น 6.0 หรือ 7.0 เท่านั้น ไม่สนับสนุนการทำงานสำหรับเวอร์ชั่น 5.0 หรือเวอร์ชั่นก่อนหน้านี้

ขั้นตอนที่ 9 ขั้นตอนสุดท้ายของเตรียมการติดตั้ง

ขั้นตอนนี้เป็นการเสร็จสิ้นการเตรียมการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ของท่าน

ครั้งแรกที่ท่านใช้งานโปรแกรมแบบเลือกเอง (ดูที่ ขั้นตอนที่ 5 เลือกประเภทของการติดตั้ง) ขอแนะนำให้ท่านไม่ทำการไม่ยกเลิกการตรวจสอบที่ Enable Self-Defense before installation ให้ทำขั้นตอนนี้เพื่อกลับไปตรวจสอบกระบวนการติดตั้ง เพื่อดูความผิดพลาดที่อาจเกิดขึ้นระหว่างการติดตั้ง

<u>หมายเหตุ</u>

หากการติดตั้งโปรแกรมเป็นการติดตั้งระยะไกลจากการใช้ Remote Desktop ท่านสามารถเลือกไม่เลือก Enable Self-Defense before installation หากมีการตรวจสอบการติดตั้งอาจไม่สามารถทำงานได้หรืออาจมีการทำงานผิดพลาด

กดปุ่ม Next เพื่อดำเนินการติดตั้ง ไฟล์การติดตั้งจะเริ่มต้นสำเนาลงบนเครื่องคอมพิวเตอร์ของท่าน

<u>คำเตือน!</u>

ในช่วงของการติดตั้ง การเชื่อมต่อเครือข่ายที่มีอยู่อาจมีความหน่วง ถ้าแพ็กเก็ตของโปรแกรมมีการแทรกเข้ามาในทราฟฟิกของเครือข่าย การเชื่อมต่อจะกลับมาเป็นปกติเมื่อการติดตั้งสิ้นสุดลง

ขั้นตอนที่ 10 เสร็จสิ้นการติดตั้ง

หน้าต่าง Installation complete การติดตั้งเสร็จสิ้น จะแสดงข้อมูลการติดตั้งที่เสร็จสิ้นของโปรแกรมบนคอมพิวเตอร์ของท่าน

ตัวอย่างเช่น วินโดว์จะแสดงความจำเป็นในการเปิดเครื่องใหม่เพื่อความสมบูรณ์ของการติดตั้ง หลังจากระบบได้เริ่มใหม่อีกครั้ง วิซาร์ดการติดตั้งก็จะเสร็จสมบูรณ์

หากไม่ต้องการเริ่มระบบใหม่ ให้เลือกปุ่ม Next เพื่อเริ่มวิซาร์ดการตั้งค่าการใช้งาน

ตัวประสานการใช้งานของผู้ใช้กับโปรแกรม

โปรแกรมออกแบบมาเพื่อให้มีความง่ายต่อการใช้งาน ในบทนี้จะอธิบายถึงรายละเอียดคุณลักษณะต่างๆ

นอกจากนี้ตัวประสานการใช้งานของผู้ใช้กับโปรแกรมหลัก ยังมีการเชื่อมไปยังโปรแกรม Microsoft Outlook, the Bat! และ Microsoft Windows Explorer การเชื่อมโยงขยายไปยังโปรแกรมเหล่านี้ ทำให้คาร์ปาสกี้แอนตี้ไวรัส สามารถจัดการ และทำงานได้จากตัวประสานของโปรแกรมเหล่านี้

<u>เนื้อหาในส่วนนี้ประกอบไปด้วย</u>

รูปสัญลักษณ์แสดงการแจ้งเตือน

เมนูลัด

หน้าต่างโปรแกรมหลัก

การแจ้งเตือน

หน้าต่างการตั้งค่าโปรแกรม

รูปสัญลักษณ์แสดงการแจ้งเตือน

ทันทีหลังจากการติดตั้งโปรแกรม รูปสัญลักษณ์ของโปรแกรมจะปรากฏบนบริเวณแถบงานของไมโครซอฟต์วินโดว์(Microsoft Windows taskbar) ตรงมุมขวาด้านล่าง

รูปสัญลักษณ์แสดงถึงการทำงานในตอนนั้นของโปรแกรม บอกถึงสถานะการป้องกัน แสดงจำนวนพื้นฐานการทำงานของโปรแกรม

ถ้ารูปสัญลักษณ์ เป็นสีแสดงว่ากำลังทำงาน มีการดำเนินการในบางส่วนหรือทั้งหมดของโปรแกรม แต่หากว่ารูปสัญลักษณ์ เป็นขาวดำแสดงว่าไม่มีการทำงาน

รูปสัญลักษณ์ของโปรแกรมมีการเปลี่ยนแปลงไปตามการดำเนินการต่อไปนี้

- กำลังทำการตรวจสอบอีเมล์
- กำลังอัพเดทฐานข้อมูลและโมดูลโปรแกรม
- จำเป็นต้องมีการปิดและเปิดเครื่องคอมพิวเตอร์ใหม่เพื่อการอัพเดท
- เกิดข้อผิดพลาดในบางส่วนของโปรแกรม

รูปสัญลักษณ์เหล่านี้ เป็นพื้นฐานตัวประสานการใช้งานระหว่างผู้ใช้กับโปรแกรม ประกอบด้วยเมนูลัด (Short cut) (ดูที่ เรื่องของเมนูลัด ในเรื่องถัดไป) และ หน้าต่างโปรแกรมหลัก (ดูที่ เรื่องของหน้าต่างโปรแกรมหลัก)

การเปิดเมนูลัด ให้ทำการคลิกขวาบนสัญลักษณ์ของโปรแกรม

การเปิดหน้าต่างโปรแกรมหลัก ให้คลิกสองครั้งที่สัญลักษณ์ของโปรแกรม หน้าต่างหลักเมื่อเปิดจะแสดงส่วนของ Protection เสมอ

หากมีข่าวสารจากคาร์ปาสกี้ รูปสัญลักษณ์ข่าวสารจะปรากฏในแถบงาน ที่บริเวณมุมขวาด้านล่างเมื่อทำการคลิกสองครั้งบนรูปสัญลักษณ์จะมีหน้าต่างแสดงข่าวขึ้นมา

เมนูลัด

ท่านสามารถกำหนดการดำเนินการเพื่อการปกป้องพื้นฐาน ได้จากรายการดังต่อไปนี้

- Update เริ่มต้นโมดูลโปรแกรม และการอัพเดทฐานข้อมูล รวมทั้งการติดตั้งการอัพเดทลงบนเครื่องคอมพิวเตอร์
- Full Computer Scan เริ่มการตรวจสอบอย่างเต็มรูปแบบให้แก่คอมพิวเตอร์ฟ้นจากวัตถุอันตราย โดยทำการตรวจสอบทุกไดร์ฟรวมไปถึงสื่อเก็บข้อมูลที่เคลื่อนย้ายได้
- Virus Scan เลือกวัตถุแล้วทำการตรวจสอบไวรัส รายการเริ่มต้นสำหรับการตรวจสอบมีไม่กี่รายการ เช่น โฟลเดอร์ My documents และตัวเก็บอีเมล์ ท่านสามารถเพิ่มเติมให้ทำการตรวจสอบได้ตามความต้องการ
- Kaspersky Anti-Virus เปิดหน้าต่างโปรแกรมหลัก (ดูที่ เรื่องของ หน้าต่างโปรแกรมหลัก)
- Setting ดูและปรับเปลี่ยนการตั้งค่าโปรแกรม
- Activate การเริ่มต้นโปรแกรม เพื่อเป็นผู้ใช้ที่จดทะเบียนแล้ว ท่านจะต้องทำการเริ่มต้นโปรแกรมของท่าน รายการเมนูนี้จะคงอยู่หากว่าท่านยังไม่ได้ทำการเริ่มต้นโปรแกรม
- About ข้อมูลแสดงผลเกี่ยวกับโปรแกรม
- Pause protection/ Resume protection การหยุดการทำงานชั่วคราว หรือการเปิดให้ใช้งานป้องกันแบบเรียลไทม์ ตัวเลือกเมนูนี้จะไม่ส่งผลต่อการอัพเดทโปรแกรม หรือการดำเนินการตรวจสอบไวรัส
- Exit ปิดโปรแกรมและปลดโปรแกรมออกจากความจำของเครื่อง

รูปที่ 1 เมนูลัด

หากกำลังมีการทำงานตรวจสอบไวรัส เมื่อท่านเปิดเมนูลัด จะขึ้นเป็นสถานะการดำเนินการ(อัตราร้อยละที่เสร็จสมบูรณ์) ไว้ที่เมนูลัด ในการเลือกงานท่านจะเปิดจากหน้าต่างโปรแกรมหลัก ซึ่งมีรายงานผลการดำเนินการของงานตรวจสอบอยู่

หน้าต่างโปรแกรมหลัก

หน้าต่างโปรแกรมหลักประกอบไปด้วย3 ส่วนคือ

- ส่วนบนสุดของหน้าต่างแสดงให้เห็นถึงสถานะของการป้องกันขณะนั้นของคอมพิวเตอร์

ภาพที่ 2 สถานะของการป้องกันปัจจุบันของคอมพิวเตอร์

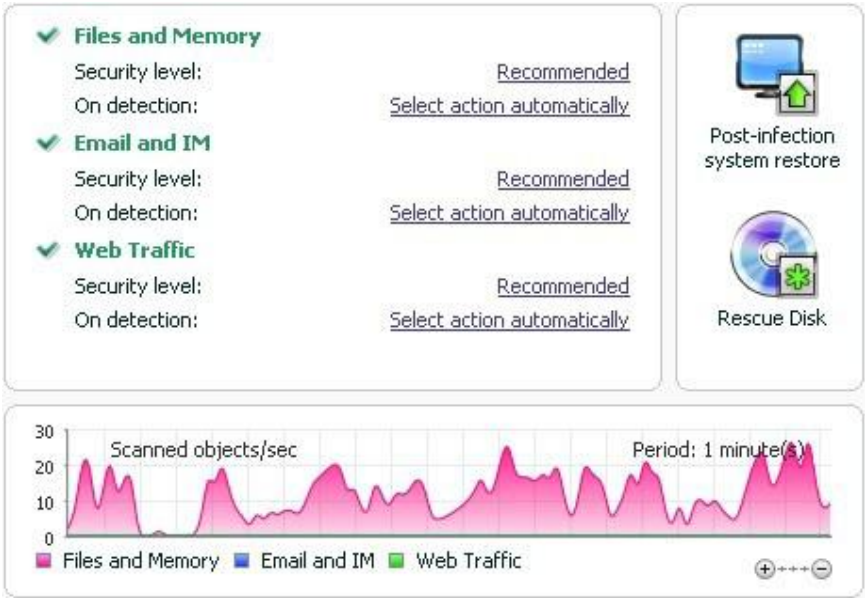
สถานะของการป้องกันปัจจุบันของคอมพิวเตอร์แบ่งออกเป็น 3 ค่า โดยที่แต่ละค่าจะมีสีประจำคล้ายกับสีของไฟจราจร สีเขียวหมายถึง สถานะของการป้องกันปัจจุบันของคอมพิวเตอร์อยู่ในระดับที่ถูกต้อง ขณะที่สีเหลืองและสีแดงนั้น อยู่ในสถานะที่มีภัยคุกคามต่อความปลอดภัยในการตั้งค่าระบบ หรือการดำเนินการโปรแกรม เนื่องมาจากฐานข้อมูลโปรแกรมมุ่งร้าย และภัยคุกคามไม่ทันสมัย การปิดส่วนการทำงานของการป้องกัน และการเลือกการติดตั้งการป้องกันที่ในระดับน้อย

ภัยคุกคามความปลอดภัย จำกัดออกไปได้ทันทีที่ปรากฏ เลือกลิงค์Fix it now เพื่อรับทราบข้อมูลเกี่ยวกับมันแล้วกำจัดมันอย่างรวดเร็ว(ดูที่ภาพข้างล่าง)

- ส่วนด้านซ้ายมือของหน้าต่าง แถบนำทาง (Navigation bar) จะนำเข้าสู่ส่วนการทำงานของโปรแกรมอย่างรวดเร็ว รวมทั้งการตรวจสอบไวรัสและการอัพเดทงาน

ภาพที่ 3 ส่วนทางซ้ายของหน้าต่าง

- ส่วนทางด้านขวาของหน้าต่างประกอบไปด้วยขข้อมูลเกี่ยวกับการทำงานของโปรแกรม ที่ได้เลือกไปในส่วนทางด้านซ้ายมือ และใช้เพื่อการตั้งค่าตัวเลือกการทำงานและเครื่องมือแสดงการทำงานด้านการตรวจสอบไวรัส การดาวน์โหลดตัวอัพเดทเป็นต้น



ท่านสามารถใช้ปุ่มดังต่อไปนี้ได้ด้วย

- Setting เพื่อเปิดหน้าต่างการตั้งค่าโปรแกรม
- Help เพื่อเปิดระบบการช่วยเหลือของโปรแกรม
- Detected เพื่อเปิดรายการของวัตถุที่เป็นอันตรายโดยส่วนประกอบหรือการตรวจสอบใดๆ และแสดงสถิติอย่างละเอียดของการดำเนินการของโปรแกรม
- Reports เพื่อเปิดรายการเหตุการณ์ที่เกิดขึ้นระหว่างการดำเนินการของโปรแกรม
- Support เพื่อแสดงข้อมูลเกี่ยวกับระบบ และลิงค์ไปยังแหล่งทรัพยากรข้อมูลของคาร์ปาส้กีแลป รวมทั้งการบริการสนับสนุนทางเทคนิคและฟอรั่ม

หมายเหตุ

ท่านสามารถเปลี่ยนแปลงหน้าตาการแสดงของโปรแกรมโดยการสร้าง และใช้ภาพกราฟฟิกและสีของท่านเองได้

การแจ้งเตือน

เมื่อเกิดเหตุการณ์ขึ้นระหว่างการดำเนินการ การแจ้งเตือนพิเศษจะปรากฏขึ้นบนหน้าจอ แสดงเป็นข้อความขึ้นทันทีเหนือรูปสัญลักษณ์ของโปรแกรมในแถบล่างด้านขวา

การแจ้งเตือนจะแตกต่างกันไป ขึ้นอยู่กับความร้ายแรงต่อความปลอดภัยของเครื่องคอมพิวเตอร์ ที่มีดังต่อไปนี้

- Alert เกิดเหตุการณ์ที่มีความร้ายแรงขึ้น ตัวอย่างเช่น ไวรัส มีกิจกรรมอันตรายต่อระบบของท่าน ท่านต้องทำการตัดสินใจในทันทีว่าจะดำเนินการสิ่งใด การเตือนประเภทนี้จะเป็นสีแดง
- Warning! เหตุการณ์ที่มีโอกาสเป็นอันตราย ตัวอย่างเช่น ไฟล์มีการติดเชื้อ หรือการกระทำต้องสงสัยบนระบบของท่าน ท่านจะได้รับคำแนะนำให้กระทำการอย่างหนึ่งอย่างใดกับเหตุการณ์ที่เป็นอันตรายนี้ ประเภทของการเตือนนี้จะเป็นสีเหลือง
- Note การเตือนนี้จะเป็นการบอกข้อมูลถึงเหตุการณ์ที่ไม่ได้เป็นอันตราย ได้แก่ การเตือนเกี่ยวกับการทำงานของส่วนประกอบ**ตัวกรองเนื้อหา** การเตือนประเภทนี้จะเป็นสีเขียว

หน้าต่างการตั้งค่าโปรแกรม

หน้าต่างการตั้งค่าโปรแกรม สามารถเปิดได้จากหน้าต่างโปรแกรมหลัก (ดูที่ เรื่องของ หน้าต่างโปรแกรมหลัก) หรือเมนูลัด (ดูที่เรื่องของเมนูลัด) เพื่อการเรียกหน้าต่างนี้ขึ้นมาให้คลิกที่ Setting เพื่อลิงค์ไปยังส่วนบนสุดของหน้าต่างโปรแกรมหลัก หรือเลือกตัวเลือกที่เหมาะสมบนเมนูลัดของโปรแกรม

หน้าต่างการตั้งค่าโปรแกรมประกอบไปด้วยสองส่วนคือ

- ส่วนทางด้านซ้ายมือของหน้าต่าง ประกอบไปด้วยการเข้าถึงส่วนประกอบของโปรแกรม เช่นงานการตรวจสอบไวรัส และการอัพเดทงาน
- ส่วนทางด้านขวาของหน้าต่างประกอบด้วยรายการการตั้งค่าสำหรับส่วนประกอบ หรืองานที่ได้เลือกไว้ทางด้านซ้ายของหน้าต่าง

การเริ่มต้น

หนึ่งในวัตถุประสงค์หลักของการที่คาร์ปาส้กีแลป สร้างคาร์ปาสกีแอนตี้ไวรัสคือการสร้างโปรแกรมที่ดีที่สุดสำหรับเป็นทางเลือกของโปรแกรมทั้งหมด เพื่อให้ผู้ใช้งานคอมพิวเตอร์ไม่เกิดความยุ่งยาก สามารถทำงานได้ทันทีหลังจากการติดตั้ง โดยไม่ต้องใช้เวลานานในการเปลี่ยนแปลงการติดตั้ง

เพื่อความสะดวกสบายแก่ผู้ใช้ เราจึงรวมเอาขั้นตอนในกรตั้งค่าเบื้องต้น เข้าไว้ในวิซาร์ดการติดตั้งเริ่มแรกในตอนที่เริ่มต้นการทำงานของโปรแกรม โดยการตามคำแนะนำของวิซาร์ด ท่านสามารถทำการเริ่มต้นโปรแกรม ตั้งค่าสำหรับการอัพเดทการจำกัดการเข้าถึงโปรแกรมโดยการใช้รหัสผ่านและการทำการติดตั้งอื่นๆ

เครื่องคอมพิวเตอร์ของท่านอาจมีการติดโปรแกรมมุ่งร้ายก่อนมีการติดตั้งโปรแกรม เพื่อการตรวจจับโปรแกรมมุ่งร้ายที่มีอยู่ ต้องทำการตรวจสอบคอมพิวเตอร์ (ดูที่ การตรวจสอบไวรัสในเครื่องคอมพิวเตอร์)

อันเนื่องมาจากการติดโปรแกรมมุ่งร้าย หรือความล้มเหลวของระบบ การตั้งค่าของเครื่องคอมพิวเตอร์อาจมีการผิดเพี้ยน ให้ดำเนินการวิซาร์ดการวิเคราะห์ความปลอดภัย เพื่อค้นหาช่องโหว่หรือจุดอ่อนใดๆ ในซอฟต์แวร์ที่มีการติดตั้งและความผิดปกติของการตั้งค่าระบบ

ฐานข้อมูลโปรแกรมที่มากับชุดการติดตั้งอาจเป็นรุ่นเก่า ให้เริ่มต้นการอัพเดทโปรแกรม หากไม่ได้มีการดำเนินในวิซาร์ดการตั้งค่า หรือกระทำอย่างอัตโนมัติหลังจากมีการติดตั้งโปรแกรม

หลังจากดำเนินการเสร็จสมบูรณ์ในส่วนนี้ โปรแกรมก็พร้อมปกป้องเครื่องคอมพิวเตอร์ของท่าน เพื่อประเมินการดำเนินการของเครื่องคอมพิวเตอร์ท่าน ให้ใช้วิซาร์ดการจัดการความปลอดภัย (ดูที่ส่วนของการจัดการความปลอดภัย)

<u>เนื้อหาในส่วนนี้ประกอบไปด้วย</u>

การตรวจสอบไวรัสในเครื่องคอมพิวเตอร์

การมีส่วนร่วมในเครือข่ายความปลอดภัยคาร์ปาสกี้

การจัดการความปลอดภัย

การหยุดปกป้องชั่วคราว

การอัพเดทโปรแกรม

<u>คำเตือน!</u>

คุณต้องทำการเชื่อมต่ออินเทอร์เน็ตเพื่อการอัพเดทคาร์ปาสกี้แอนตี้ไวรัส

ฐานข้อมูลประกอบไปด้วยลายเซ็นต์ภัยคุกคามที่อยู่ในชุดการกระจายโปรแกรม อย่างไรก็ตาม เมื่อโปรแกรมได้ทำการติดตั้งเป็นที่เรียบร้อยอาจยังไม่ใหม่เพียงพอ เมื่อคาร์ปาสกี้แลปทำการอัพเดทแล้ว ฐานข้อมูลและโมดูลก็จะอยู่ในสภาพปกติ

ท่านสามารถระบุการอัพเดทงานเมื่อวิซาร์ดการติดตั้งดำเนินการ คาร์ปาสกี้แอนตี้ไวรัสจะทำการตรวจสอบการอัพเดทจากเซิร์ฟเวอร์ของคาร์ปาสกี้แลปให้อย่างอัตโนมัติตามค่าการเริ่มต้นหากว่าเซิร์ฟเวอร์พบว่ามีการอัพเดทใหม่ก็จะทำการดาวน์โหลดและติดตั้งต่อไป

เพื่อให้เครื่องคอมพิวเตอร์ของคุณทันต่อฐานข้อมูล ขอแนะนำให้ทำการอัพเดทคาร์ปาสกีแอนตี้ไวรัสทันทีหลังจากการติดตั้ง

- สำหรับการอัพเดทคาร์ปาสกี้แอนตี้ไวรัสด้วยมือ

1. เปิดหน้าต่างโปรแกรมหลัก
2. เลือกส่วน Update ในทางด้านซ้ายมือ
3. เลือกปุ่ม Start update

เนื่องมาจากว่า คาร์ปาสกี้แอนตี้ไวรัส จะเริ่มทำการอัพเดท รายละเอียดของกระบวนการจะแสดงผลให้เห็นทางหน้าต่างพิเศษ

การวิเคราะห์ความปลอดภัย

ระบบปฏิบัติการของเครื่องคอมพิวเตอร์อาจโดนทำลายจากความล้มเหลวของระบบ และกิจกรรมของโปรแกรมมุ่งร้าย นอกจากนี้โปรแกรมผู้ใช้งานที่ติดตั้งลงไปบนเครื่องคอมพิวเตอร์ของท่าน ก็อาจเป็นช่องโหว่ให้ผู้บุกรุกสามารถเข้ามาทำลายเครื่องคอมพิวเตอร์ของท่าน

เพื่อการค้นหาและการกำจัดปัญหาทางด้านความปลอดภัย แนะนำให้ดำเนินการ วิซาร์ดวิเคราะห์ความปลอดภัย *Security Analyzer Wizard* ทันทีหลังจากที่คุณทำการติดตั้งโปรแกรมเรียบร้อยแล้ว สำหรับความเสียหายของระบบปฏิบัติการ และการติดตั้ง

- <u>เริ่มต้นการทำงาน</u>

1. เปิดหน้าต่างโปรแกรมหลัก
2. ทางด้านซ้ายของหน้าต่าง เลือก System Security
3. เริ่มต้นการทำงานที่ Security Analyzer

การตรวจสอบไวรัสในเครื่องคอมพิวเตอร์

นักพัฒนาโปรแกรมมุ่งร้ายจะทำทุกวิถีทางเพื่อการเข้าถึงเครื่องคอมพิวเตอร์ และไท่อาจทราบได้ว่าโปรแกรมมุ่งร้ายเหล่านั้นเข้ามาเครื่องคอมพิวเตอร์ของเราได้อย่างไร

เมื่อท่านติดตั้งคาร์ปาสกี้แอนตี้ไวรัสลงบนเครื่องคอมพิวเตอร์ของท่าน โปรแกรมจะดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ของท่านอย่างอัตโนมัติ ด้วยการทำ Quick scan งานนี้จะทำการค้นหาเพื่อการทำลายโปรแกรมที่เป็นอันตรายภายในเครื่อง ซึ่งจะทำให้ระบบปฏิบัติการของเครื่องทำงานหนัก

ผู้เชี่ยวชาญของคาร์ปาสกี้แลป แนะนำให้ท่านทำการตรวจสอบเครื่องแบบเต็มรูปแบบดังต่อไปนี้

- เริ่มต้น/ หยุดการตรวจสอบไวรัส

1. เปิดหน้าต่างโปรแกรมหลัก
2. ทางด้านซ้ายมือของหน้าต่างเลือก Scan (Full scan, Quick scan)
3. คลิกที่ปุ่ม Start scan เพื่อเลือกการเริ่มต้นตรวจสอบ หากต้องการหยุดให้เลือกปุ่ม Stop scan ในขณะที่กำลังดำเนินการ

การมีส่วนร่วมในเครือข่ายความปลอดภัยคาร์ปาสกี้

ภัยคุกคามใหม่ๆ เกิดขึ้นมากมายทุกวัน เพื่อให้ท่านได้ชัดความสะดวกสบายในการรับทราบข้อมูลทางสถิติ ข่าวสารเกี่ยวกับการเกิดภัยคุกคาม รับทราบที่มาของภัยคุกคามและวิธีในการกำจัด คาร์ปาสกี้แลปเชิญท่านใช้บริการเครือข่ายความปลอดภัยคาร์ปาสกี้

การใช้งานเครือข่ายความปลอดภัยคาร์ปาสกี้ รวมถึงการส่งข้อมูลเข้าสู่คาร์ปาสกี้แลปมีดังต่อไปนี้

- การตั้งชื่อที่มีความเป็นหนึ่งเดียวบนเครื่องคอมพิวเตอร์ของท่าน ชื่อนี้จะมีลักษณะอยู่บนการตั้งค่าเครื่องคอมพิวเตอร์ของท่าน และไม่มีข้อมูลอื่นใด
- ข้อมูลเหล่านี้เป็นข้อมูลเกี่ยวกับภัยคุกคามที่จับได้จากโปรแกรม โครงสร้างและเนื้อหาของข้อมูลขึ้นอยู่กับประเภทของภัยคุกคาม
- ข้อมูลระบบ ประกอบไปด้วย เวอร์ชั่นของระบบปฏิบัติการรวบรวมการบริการ ไดร์ฟเวอร์และการบริการที่สามารถดาวน์โหลดได้ บราวเซอร์ เวอร์โปรแกรมอีเมล์ การขยายบราวเซอร์ จำนวนเวอร์ชั่นของคาร์ปาสกี้แอนตี้ไวรัสที่ทำการติดตั้ง

เครือข่ายความปลอดภัยของคาร์ปาสกี้ รวมไปถึงสถิติที่ขยายอันมีข้อมูลเกี่ยวกับ

- แฟ้มการกระทำในระบบ และโปรแกรมที่มีการลงชื่อที่ได้ดาวน์โหลดลงบนเครื่องคอมพิวเตอร์
- โปรแกรมที่ทำงานอยู่บนเครื่องคอมพิวเตอร์ของท่าน

ข้อมูลเกี่ยวกับทางสถิตินี้ ส่งออกไปเมื่อโปรแกรมได้ทำการอัพเดทเป็นที่เรียบร้อยแล้ว

<u>คำเตือน!</u>

คาร์ปาสกี้แลปให้การรับประกันว่าจะไม่มีการเก็บรวบรวมชื่อและข้อมูลส่วนบุคคลของผู้ใช้ หรือทำการแจกจ่ายข้อมูลส่วนบุคคลของผู้ใช้ ในการดำเนินการเกี่ยวกับเครือข่ายความปลอดภัยคาร์ปาส้กี

- การตั้งค่าการส่งสถิติ

1. เปิดหน้าต่างการตั้งค่าโปรแกรม
2. เลือก Feedback ที่อยู่ทางด้านซ้ายของหน้าต่าง
3. เลือกช่อง I agree to participate in Kaspersky Security Network เพื่อยืนยันในการเข้าร่วมเครือข่ายความปลอดภัยคาร์ปาสกี้ เลือกช่อง I agree to send extended statistics within the framework of Kaspersky Security Network เพื่อยืนยันการยินยอมในการส่งข้อมูลทางสถิติ

การจัดการความปลอดภัย

ปัญหาด้านการป้องกันความปลอดภัยบนเครื่องคอมพิวเตอร์ แสดงให้เห็นที่หน้าต่างโปรแกรมหลัก โดยมีการเปลี่ยนสีของรูปสัญลักษณ์สถานะการป้องกัน เมื่อการป้องกันเกิดปัญหา เราขอแนะนำให้รีบดำเนินการในทันที

ภาพที่ 5: สถานะปัจจุบันของการป้องกันเครื่องคอมพิวเตอร์

ท่านสามารถดูรายการของสถานะปัจจุบัน คำอธิบายและการแก้ปัญหาที่เป็นไปได้บนแถบสถานะ Status (ดูที่ภาพด้านล่าง) ที่เปิดขึ้นเมื่อท่านคลิกลิงค์ Fix it now (ดูที่ภาพข้างบน)

ภาพที่ 6 การแก้ปัญหาความปลอดภัย

แถบแสดงรายการของปัญหาที่เกิดขึ้น รายการปัญหาจะลำดับตามความสำคัญ ประการแรกเป็นปัญหาที่มีความรุนแรงมากที่สุด มีรูปสัญลักษณ์ที่เป็นสีแดง ประการที่สอง จะเป็นปัญหาที่มีความสำคัญน้อยรองลงมา จะเป็นรูปสัญลักษณ์สีเขียว คำอธิบายอย่างละเอียดแยกไปตามแต่ละปัญหา และกรกระทำที่มีอยู่ตามมา

- **กำจัดทันที** (Eliminate immediately) ใช้ปุ่มเพื่อการตอบสนอง ท่านสามารถเริ่มทำการแก้ไขปัญหา อันเป็นการกระทำแนะนำ

- **เลื่อนการกำจัด** (Postpone elimination) ไม่ว่าเหตุผลใดก็ตามที่ท่านไม่สามารถกำจัดปัญหาได้ในทันที ท่านสามารถชะลอการกระทำและย้อนกลับมาภายหลังโดยการเลือกการกำจัด โดยใช้ปุ่ม Hide message

ตัวเลือกนี้จะต้องใช้กับเฉพาะปัญหาที่ไม่ได้ร้ายแรง ตัวอย่างเช่น ตรวจเจอวัตถุมุ่งร้ายแต่ไม่ได้มีผลต่อเครื่องคอมพิวเตอร์ มีปัญหาที่ส่วนประกอบบางตัว หรือเกิดความไม่ถูกต้องของไฟล์โปรแกรม

การซ่อนข้อความไม่ให้ปรากฏอีกครั้ง ให้เลือกที่ช่อง Show hidden messages

การหยุดปกป้องชั่วคราว

การหยุดปกป้องชั่วคราว หมายถึง การไม่ทำงานด้านการปกป้องของโปรแกรมเป็นการชั่วคราวในบางช่วงเวลา

- วิธีการหยุดปกป้องชั่วคราว

1. เลือกที่ Pausing protection จากเมนูลัดของโปรแกรม(ดูที่ส่วนของเมนูลัด)
2. เมื่อเปิดหน้าต่างขึ้นมา ให้เลือกคาบเวลาที่ต้องการหยุดการปกป้อง
    - ในช่วงเวลา (In <time interval>) การป้องกันจะเกิดขึ้นเมื่อเวลาผ่านไป
    - หลังการเริ่มต้นทำงานใหม่ (After restart) การป้องกันจะเกิดหลังจากการเริ่มต้นทำงานใหม่ของระบบ
    - โดยมือ Manually การป้องกันที่เกิดขึ้นจากการที่ผู้ใช้ตั้งค่าการป้องกันด้วยตัวเอง โดยการเลือก Resume protection จากเมนูลัดของโปรแกรม

ด้วยเหตุที่ว่า มีการหยุดการป้องกันชั่วคราวการป้องกันในส่วนประกอบต่างๆ ก็หยุดลง โดยมีการแสดงให้เห็นดังต่อไปนี้

- ชื่อไม่มีการทำงาน (เป็นสีเทา) สำหรับส่วนประกอบที่ปิดการทำงานในส่วนของ Protection ของหน้าต่างหลัก
- รูปสัญลักษณ์ของโปรแกรมไม่มีการทำงาน (เป็นสีเทา) (**ดูที่ส่วนของ รูปสัญลักษณ์แสดงการแจ้งเตือน**) ในรายชื่อระบบ
- สีแดงเป็นรูปสัญลักษณ์แสดงสถานะ และสำหรับรายชื่อของหน้าต่างโปรแกรมหลัก

ถ้ามีการเชื่อมต่อเครือข่ายใหม่ ในเวลาเดียวกับการหยุดการป้องกัน การแจ้งเตือนจะมีข้อความแสดงเกี่ยวกับการหยุดการเชื่อมต่อ

การตั้งค่าโปรแกรมให้สมบูรณ์

หลังจากการติดตั้งและตั้งค่าโปรแกรมเป็นที่เรียบร้อยแล้ว ท่านควรทำการยืนยันการติดตั้งโปรแกรมที่ถูกต้อง โดยการทดสอบไวรัสและการปรับเปลี่ยนค่า

เนื้อหาในส่วนนี้มีดังต่อไปนี้

ทดสอบไวรัส EICAR และการปรับเปลี่ยน

การทดสอบไวรัสออกแบบโดย EICAR (สถาบันการค้นคว้าแอนตี้ไวรัสคอมพิวเตอร์แห่งยุโรป) สำหรับใช้การทดสอบผลิตภัณฑ์แอนตี้ไวรัส

ทดสอบไวรัสที่ไม่ใช่ไวรัส เพราะว่าไม่มีรหัสที่ทำอันตรายต่อเครื่องคอมพิวเตอร์ของท่าน อย่างไรก็ตาม ผู้ผลิตส่วนมากของผลิตภัณฑ์แอนตี้ไวรัสระบุว่าไฟล์เหล่านี้เป็นไวรัส

คำเตือน!

ไม่มีการใช้ไวรัสจริงในการทดสอบระบบการทำงานของผลิตภัณฑ์แอนตี้ไวรัส

ท่านสามารถดาวน์โหลดการทดสอบไวรัสได้จากเว็บไซต์ขององค์กร EICAR http://www.eicar.org/anti_virus_test_file.htm

หมายเหตุ

ก่อนทำการดาวน์โหลดไฟล์ ต้องทำการปิดการทำงานของการป้องกันอนตี้ไวรัสของคอมพิวเตอร์ไม่เช่นนั้นแล้ว โปรแกรมอื่นๆ จะทำการระบุว่าไฟล์ Anti_virus_test_file.htm เป็นการติดเชื้อผ่านทางโปรโตคอล HTTP

อย่าลืม เปิดการใช้งานแอนตี้ไวรัสทันทีหลังจากการดาวน์โหลดทดสอบไวรัส

โปรแกรมจะระบุไฟล์ที่ทำการดาวน์โหลดจาก EICAR ว่าเป็นไฟล์ที่มีการติดไวรัส ที่ไม่สามารถกำจัดได้ และให้ทำการดำเนินการต่อวัตถุนั้น

ท่านสามารถทำการเปลี่ยนแปลงการทดสอบไวรัสเบื้องต้น เพื่อยืนยันการดำเนินการของโปรแกรมที่แตกต่างจากประเภทของไฟล์อื่น การเปลี่ยนแปลงไวรัส เป็นการเปลี่ยนเนื้อหาของไวรัสมาตรฐาน โดยการเพิ่มส่วนหน้าลงไป (ดูตารางข้างล่าง) เพื่อสร้างการเปลี่ยนแปลงไฟล์ไวรัส ท่านสามารถใช้ข้อความหรือตัวสร้างข้อความหลายมิติ(Hypertext) ตัวอย่างเช่น Microsoft Notepad, UltraEdit32 เป็นต้น

คำเตือน!

ท่านสามารถทำการทดสอบความถูกต้อง ของการทำงานของโปรแกรมโดยการดัดแปลงไวรัสของ EICAR เท่านั้น หากว่าฐานข้อมูลล่าสุดมีการอัพเดทเมื่อวันที่ 24 เดือนตุลาคม 2003

ในตารางด้านล่าง คอลัมน์แรกประกอบไปด้วย คำนำหน้าที่มีการเพิ่มเมื่อตอนเริ่มต้นของข้อความไวรัสมาตรฐาน คอลัมน์ที่สองทำรายการค่าสถานะความเป็นไปได้ที่โปรแกรมทำต่อวัตถุด้วยสถานะเฉพาะสถานะที่แท้จริงมีการกระทำเกิดขึ้นเมื่อมีการตั้งค่าโปรแกรมแล้ว

หลังจากที่ท่านเพิ่มคำนำหน้าที่มีการเพิ่มเมื่อตอนเริ่มต้นของข้อความไวรัสมาตรฐาน ตัวอย่างเช่น eicar_dele.com ให้ทำการบันทึกชื่อไฟล์ที่แตกต่างกัน ทำให้เหมือนกันแบบนี้กับไวรัสที่ทำการเปลี่ยนแปลง

ตารางที่ 6 การเปลี่ยนแปลงการทดสอบไวรัส

คำหน้าหน้า	**สถานะวัตถุ**	**ข้อมูลการดำเนินการวัตถุ**
ใช้ไวรัสมาตรฐาน ไม่มีคำนำหน้า	**ติดเชื้อ** (Infected) เกิดการติดเชื้อด้วยไวรัสที่รู้จัก ไม่สามารถทำลายได้	โปรแกรมระบุว่าเป็นวัตถุติดเชื้อไม่สามารถทำลายได้ เกิดความผิดพลาดขึ้นขณะกระทำการทำลายเชื้อ มีการใช้งานการดำเนินการไม่สามารถทำลายเชื้อได้
CORR–	**เกิดความเสียหาย** (Corrupted)	โปรแกรมสามารถเข้าไปยังวัตถุแต่ไม่สามารถตรวจสอบได้ เพราะว่า มีความเสียหายเกิดขึ้น (ตัวอย่างเช่น โครงสร้างของไฟล์เกิดความเสียหาย หรือไม่ถูกต้อง) จะพบข้อมูลการดำเนินการวัตถุในการรายงานการดำเนินการโปรแกรม

WARN–	**ต้องสงสัย** (Suspicious) วัตถุประกอบไปด้วยรหัสของไวรัสที่ไม่ทราบชื่อ จึงไม่อาจกำจัดได้	วัตถุค้นพบว่าต้องสงสัยโดยตัววิเคราะห์แบบฮิวริสติก ในขณะที่มีการตรวจสอบ ฐานข้อมูลของโปรแกรมไม่มีคำอธิบายของวิธีการในการดำเนินการกับวัตถุ ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้
SUSP–	**ต้องสงสัย** (Suspicious) วัตถุมีรหัสที่ได้รับการเปลี่ยนแปลงของไวรัสที่รู้จัก ไม่อาจกำจัดได้	โปรแกรมได้ตรวจจับการโต้ตอบบางส่วนของรหัสของวัตถุด้วยส่วนของวัตถุมีรหัสที่ได้รับการเปลี่ยนแปลงของไวรัสที่รู้จัก ฐานข้อมูลของโปรแกรมไม่มีคำอธิบายของวิธีการในการดำเนินการกับวัตถุ ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้
ERRO–	การตรวจสอบผิดพลาด	เกิดข้อผิดพลาดขึ้นระหว่างการตรวจสอบวัตถุ โปรแกรมไม่สามารถเข้าถึงวัตถุ และการดำเนินการมีการหยุดชะงัก (ตัวอย่างเช่น ไม่มีจุดสิ้นสุดของปริมาณ) หรือไม่มีการเชื่อมต่อ (หากว่ามีการตรวจสอบบริเวณไดร์ฟเครือข่าย) ท่านสามารถหาข้อมูลเกี่ยวกับการดำเนินการของวัตถุได้จากการรายงานการดำเนินการของโปรแกรม

CURE–	**ติดเชื้อ** (Infected) เกิดการติดเชื้อด้วยไวรัสที่รู้จัก ไม่สามารถทำลายได้	วัตถุประกอบไปด้วยไวรัสที่ไม่สามารถทำลายได้ โปรแกรมจะไม่ทำลายวัตถุ มีการแทนที่เนื้อหาของตัวไวรัส เพื่อแทนที่คำว่า CURE ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้
DELE–	**ติดเชื้อ** (Infected) เกิดการติดเชื้อด้วยไวรัสที่รู้จัก ไม่สามารถทำลายได้	โปรแกรมระบุว่า เป็นไวรัสที่ไม่สามารถทำลายได้ เกิดความผิดพลาดเกิดขึ้นทำให้ไม่สามารถทำลายไวรัส การกระทะจะเกิดขึ้นเฉพาะไวรัสที่ไม่สามารถทำลายได้ ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้

การทดสอบการปกป้องข้อมูลผ่านทาง HTTP

เพื่อเป็นการยืนยันการตรวจจับไวรัสเสร็จสมบูรณ์ผ่านทางโปรโตคอล HTTP ต้องดำเนินการดังต่อไปนี้

ลองดาวน์โหลดการทดสอบไวรัสได้จากเว็บไซต์ขององค์กร EICAR http://www.eicar.org/anti_virus_test_file.htm

เมื่อทำการดาวน์โหลดการทดสอบไวรัส คาร์ปาสกี้แอนตี้ไวรัสจะทำการตรวจจับวัตถุ และระบุวัตถุที่ติดเชื้ออันไม่สามารถทำลายได้ และจะดำเนินการติดตั้งทราฟฟิกHTTP กับวัตถุที่สถานะนี้ ค่าเริ่มต้นเมื่อทำการดาวน์โหลดการทดสอบไวรัส การเชื่อมต่อเว็บไซต์จะสิ้นสุด และบราวเซอร์ก็จะแสดงผลแจ้งผู้ใช้งานมีการทดสอบไวรัสด้วยEICAR-Test-File virus

การทดสอบการปกป้องข้อมูลผ่านทาง SMTP

เพื่อเป็นการตรวจจับกระแสข้อมูลผ่านทาง SMTP ท่านต้องทำการโอนถ่ายข้อมูลผ่านทางระบบอีเมล์ที่ใช้โปรโตคอลนี้

<u>หมายเหตุ</u>

เราแนะนำให้ท่านทำการทดสอบกับคาร์ปาสกี้แอนตี้ไวรัสในการรับมือกับเมล์เข้าและออก รวมทั้งตัวข้อความในเมล์และเอกสารแนบ ในการทดสอบการตรวจจับไวรัสในตัวข้อความ ให้ทำสำเนาข้อความของการทดสอบไวรัสมาตรฐาน หรือไวรัสที่มีการดัดแปลงเข้าไปในตัวข้อความ

- การทดสอบการตรวจจับไวรัสผ่านทาง SMTP

1. สร้างข้อความธรรมดาโดยการใช้อีเมล์ที่มีการติดตั้งบนเครื่องคอมพิวเตอร์

<u>หมายเหตุ</u>

ข้อความที่ใช้ในการทดสอบ ต้องเป็นข้อความที่ไม่ได้มีการตรวจสอบมาก่อน หากว่ามีการสร้างในรูปแบบ RTF หรือ HTML

2. สำเนาข้อความของการทดสอบไวรัสมาตรฐาน หรือไวรัสที่มีการดัดแปลงเข้าไปในตัวข้อความ หรือแนบไฟล์การทดสอบไวรัสลงในข้อความ
3. ส่งข้อความไม่หาผู้ดูแล

โปรแกรมจะทำการตรวจจับวัตถุระบุว่ามีการติดเชื้อและทำการสกัดกั้น

การตั้งค่าไฟล์แอนตี้ไวรัสให้สมบูรณ์

- เพื่อทำการยืนยันไฟล์แอนตี้ไวรัสให้สมบูรณ์ต้องทำการตั้งค่าให้ถูกต้องต่อไปนี้

1. สร้างโฟลเดอร์ลงบนดิสก์ และสำเนาโฟลเดอร์การทดสอบไวรัส EICAR ที่ได้ดาวน์โหลดลงไปและไวรัสที่คุณทำการสร้างขึ้น
2. ตรวจสอบเหตุการณ์ที่บันทึกไว้ ไฟล์การรายงานจะเก็บสะสมเอาไว้ทั้งวัตถุที่มีความเสียหาย และวัตถุที่ไม่ไดรับการตรวจสอบเนื่องเพราะความผิดพลาด
3. ทำการทดสอบไวรัส หรือเวอร์ชั่นที่มีการดัดแปลง

ไฟล์แอนตี้ไวรัสที่แทรกเข้ามาในไฟล์ ให้ทำการตรวจสอบ และดำเนินการระบุลงในการติดตั้ง โดยการเลือกการกระทำที่แตกต่างกัน เพื่อทำการตรวจจับวัตถุ ท่านสามารถเลือกดำเนินการตรวจสอบเต็มรูปแบบของการดำเนินการของส่วนประกอบ

ท่านสามารถดูข้อมูลเกี่ยวกับผลของการดำเนินการไฟล์แอนตี้ไวรัสในรายงานการดำเนินการของส่วนประกอบ

การตั้งการตรวจสอบไวรัสให้สมบูรณ์

- เพื่อเป็นการยืนยันการทำงานตรวจสอบไวรัสที่ถูกต้องควรดำเนินการต่อไปนี้

    1. สร้างโฟลเดอร์ลงบนดิสก์ และสำเนาโฟลเดอร์การทดสอบไวรัส EICAR ที่ได้ดาวน์โหลดลงไป และไวรัสที่คุณทำการสร้างขึ้น
    2. สร้างงานการตรวจสอบไวรัสใหม่ และเลือกโฟลเดอร์เพื่อการตั้งการทดสอบไวรัส ที่วัตถุตรวจสอบ
    3. ตรวจสอบเหตุการณ์ที่บันทึกไว้ ไฟล์การรายงานจะเก็บสะสมเอาไว้ทั้งวัตถุที่มีความเสียหาย และวัตถุที่ไม่ไดรับการตรวจสอบเนื่องเพราะความผิดพลาด
    4. ดำเนินการงานตรวจสอบไวรัส

เมื่อดำเนินการตรวจสอบงานอยู่ การกระทำได้กำหนดไว้ในการตั้งค่างานที่จะตรวจจับวัตถุที่ต้องสงสัยหรือมีการติดเชื้อ โดยการเลือกการกระทำต่างๆ เพื่อการตรวจจับวัตถุ ท่านสามารถทำการตรวจสอบการดำเนินการได้อย่างเต็มทุกส่วนประกอบ

ท่านสามารถดูข้อมูลเกี่ยวกับผลของการดำเนินการไฟล์แอนตี้ไวรัสในรายงานการดำเนินการของส่วนประกอบ

ถ้อยแถลงการสะสมข้อมูลทางเครือข่ายความปลอดภัยคาร์ปาสกี้

บทนำ

โปรดอ่านด้วยความระมัดระวัง ข้อมูลส่วนนี้เป็นส่วนที่สำคัญที่ท่านควรรับทราบก่อนการใช้บริการและสินค้าของเรา โดยการที่ท่านจะต้องยอมรับในข้อความการสะสมข้อมูลทางเครือข่ายความปลอดภัยคาร์ปาสกี้ เราขอสงวนสิทธิ์ในการเปลี่ยนแปลงข้อมูลในถ้อยแถลงนี้เมื่อใด หรือส่วนหนึ่งส่วนใดก็ได้ โปรดตรวจสอบวันที่ในการปรับปรุงการถ้อยแถลงนี้ด้านล่าง เพื่อการตัดสินใจหากว่ามีการเปลี่ยนแปลงนโยบายใดๆ ในตอนที่ท่านทบทวนดูครั้งล่าสุด การใช้งานส่วนหนึ่งส่วนใดของการบริการคาร์ปาสกี้แลป

คาร์ปาสกี้แลปและบริษัทในเครือ (เรียกว่า “คาร์ปาสกี้แลป”) สร้างถ้อยแถลงการสะสมข้อมูล เพื่อแจ้งและเปิดเผยข้อมูลร่วมกันของคาร์ปาสกี้แอนตี้ไวรัส และคาร์ปาสกี้อินเทอร์เน็ตซิเคียวริตี้

คำจากคาร์ปาสกี้แลป

คาร์ปาสกี้มีการตกลงรวมกันอย่างจริงจังในเรื่องของการให้บริการที่เหนือกว่า แก่ลูกค้าของเราทั้งหมด และมีเคารพในความกังวลของการเก็บข้อมูล เราเข้าใจดีว่า ท่านอาจมีคำถามในเรื่องของวิธีการในการเก็บข้อมูลเครือข่ายความปลอดภัยของเรา และหลักการในการเก็บข้อมูล การใช้ข้อมูลที่เป็นของเครือข่ายความปลอดภัยคาร์ปาสกี้(“ถ้อยแถลงการสะสมข้อมูล”. หรือ “ถ้อยแถลง”)

ถ้อยแถลงการสะสมข้อมูลนี้ ประกอบไปด้วยจำนวนรายละเอียดทางเทคนิคและวิธีการ เกี่ยวกับขั้นตอนของการสะสมข้อมูล เรามีการจัดการเพื่อการสะสมข้อมูลที่มีขั้นตอนหลัก เพื่อให้ท่านสามารถให้ข้อมูลที่ท่านสนใจ ส่วนสำคัญที่สุดคือ การได้เข้าถึงในสิ่งที่ท่านต้องการ และแบบความคาดหวังของทุกสิ่งที่เราทำเพื่อการสะสมข้อมูล

รายละเอียดและข้อมูลรวบรวมโดยทางคาร์ปาสกี้แลป หากท่านมีปัญหาหรือข้อสงสัยสามารถสอบถามได้ที่ support@kaspersky.com

เครือข่ายความปลอดภัยของคาร์ปาสกี้คืออะไร

การบริการเครือข่ายคาร์ปาสกี้ทำให้ผู้ใช้งานสินค้าคาร์ปาสกี้แลป มีความสะดวกสบายและลดการเสียเวลาที่จะเกิดจากความเสี่ยงชนิดใหม่ๆ ที่มุ่งเป้ามาสู่เครื่องคอมพิวเตอร์ของท่าน เพื่อการระบุถึงภัยคุกคามใหม่ๆ และเพื่อการปรับปรุงการทำงานด้านความปลอดภัยของเรา รวมทั้งการทำงานของสินค้าเครือข่ายความปลอดภัยคาร์ปาสกี้ รวบรวมความปลอดภัยและข้อมูลโปรแกรมเกี่ยวกับความเสี่ยงภัยที่อาจเกิดขึ้นได้ต่อเครื่องคอมพิวเตอร์ของท่าน และการยอมรับการวิเคราะห์ข้อมูลของคาร์ปาสกี้แลป

ข้อมูลเหล่านี้ประกอบไปด้วย ข้อมูลการแสดงตนเกี่ยวกับผู้ใช้ เพื่อประโยชน์ต่อคาร์ปาสกี้แลปที่ไม่ได้เพื่อวัตถุประสงค์อื่นใด แต่เพื่อการเพิ่มประสิทธิภาพทางด้านความปลอดภัยให้แก่สินค้า และการปรับปรุงอันดีขึ้นต่อไปต่อโปรแกรมมุ่งร้าย ภัยคุกคามและไวรัส คาร์ปาสกี้แลป จะเก็บรักษาและปกป้องข้อมูลไว้ในถ้อยแถลงเครือข่ายความปลอดภัย

การรวบรวมข้อมูลทำให้ท่านเป็นส่วนหนึ่งของเครือข่ายความปลอดภัยคาร์ปาสกี้ ที่มาจากทั่วทุกมุมโลกอย่างปลอดภัย

เกี่ยวกับกฎหมาย

เครือข่ายความปลอดภัยคาร์ปาสกี้เกี่ยวข้องกับกฎหมายบางประการ เนื่องเพราะอาจมีใช้ขอบเขตการตัดสินใจของอำนาจกฎหมายที่แตกต่างกันในแต่ละแห่ง รวมทั้งในสหรัฐอเมริกา คาร์ปาสกี้แลปอาจเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากการยินยอมของท่านหากเป็นความต้องการทางกฎหมาย หรือความจำเป็นในการสืบสวนสอบสวน เพื่อป้องกันการกระทำอันเป็นสิ่งอันตราย ต่อผู้เข้าร่วม ผู้มาเยือน ผู้เกี่ยวข้องหรือทรัพย์สินของคาร์ปาสกี้แลป ตัวอย่างเช่น หากว่าทางสหภาพยุโรปต้องการทราบข้อมูลส่วนบุคคล เพื่อต้องการเก็บรวบรวมข้อมูล การติดต่อทางอิเล็กทรอนิกส์หรือความเป็นส่วนตัว แต่ไม่รวมถึง คำสั่งที่ 2002/58/EC แห่งสภายุโรป และ Council of 12 July 2002 ที่เกี่ยวข้องกับกระบวนการในการเก็บรวบรวมข้อมูลส่วนบุคคล และการป้องกันความเป็นส่วนบุคคลในส่วนของการติดต่อสื่อสารทางอิเล็กทรอนิกส์ และคำสั่งที่ 95/46/EC แห่งสภายุโรป และ Council of 24 October 1995 ในเรื่องของการป้องกันความเป็นส่วนบุคคลอันเนื่องมาจากกระบวนการในการเก็บข้อมูล และการเคลื่อนไหวโดยอิสระ ของข้อมูลตามลำดับที่ออกมาตามตัวบทกฎหมายในสมาชิกสหภาพยุโรป คำตัดสินของคณะกรรมาธิการยุโรป 497/2001/EC ใน

เรื่องของมาตรการทางสัญญามาตรฐาน (การโอนถ่ายข้อมูลส่วนบุคคลไปยังประเทศที่สาม) ที่ออกมาตามตัวบทกฎหมายในสมาชิกสหภาพยุโรป

เครือข่ายความปลอดภัยคาร์ปาสกี้จะทำการแจ้งให้ผู้ใช้ทราบตั้งแต่เริ่มต้นการรวบรวมข้อมูลที่กล่าวมาแล้วข้างต้น เพื่อใช้ในการพัฒนาทางธุรกิจ หรือการแบ่งปันข้อมูลใดๆ และอนุญาตให้ผู้ใช้เหล่านี้เลือกที่จะเข้าร่วม (ในสมาชิกสหภาพยุโรปและประเทศอื่นๆ ที่มีความต้องการเข้าร่วมกระบวนการนี้) หรือเลือกที่จะไม่เข้าร่วม (สำหรับประเทศอื่นๆทั้งหมด) ออนไลน์จากการใช้งานข้อมูลเหล่านี้ทางการค้า และ/ หรือการโอนถ่ายข้อมูลให้กับบุคคลที่สาม

คาร์ปาสกี้แลปมีผลบังคับด้วยตัวกฎหมาย หรือคำติดสินอื่นใดทางกฎหมาย ในเรื่องของความสามารถในการระบุตัวตนเพื่อให้ถูกต้องตามอำนาจแห่งการปกครอง หากมีกฎหมายหรือคำตัดสินทางกฎหมายบังคับให้ทำการจัดหาข้อมูลเหล่านี้เพื่อความถูกต้องทางด้านเอกสาร คาร์ปาสกี้แลปอาจต้องจัดหาข้อมูลเหล่านี้เพื่อให้เป็นไปตามอำนาจบังคับของกฎหมาย ในการปกป้องสิทธิ สุขภาพความปลอดภัยของบุคคลตามกฎหมายแห่งสหภาพยุโรป การบริการเครือข่ายคาร์ปาสกี้ที่เข้าถึงเกี่ยวกับประกาศ

ข้อมูลที่รวบรวม

ข้อมูลที่เราเก็บรวบรวม

การบริการเครือข่ายความปลอดภัยคาร์ปาสกี้จะเก็บข้อมูลที่ได้รับมาครั้งแรก และข้อมูลเพิ่มเติมที่คาร์ปาสกี้แลป เกี่ยวกับเรื่องของความเสี่ยงความปลอดภัยที่อาจเกิดขึ้นได้ต่อเครื่องคอมพิวเตอร์ท่าน

ข้อมูลที่ได้รับมาในครั้งแรก

- ข้อมูลเกี่ยวกับซอฟต์แวร์ ฮาร์ดแวร์ และเครื่องคอมพิวเตอร์ของท่าน ประกอบไปด้วย ระบบปฏิบัติการ และแพ็กบริการที่ติดตั้ง เคอเนล ไดรเวอร์ เซอร์วิส ส่วนขยาย Internet Explorer การพิมพ์ Window Explorer ไฟล์ที่ทำการดาวน์โหลด ตัวติดตั้งกำลังทำงาน ส่วนควบคุมแผง บันทึกการลงทะเบียนและโฮสต์IP address บราวเซอร์ โปรแกรมบริการอีเมล์ และเวอร์ชั่นของคาร์ปาสกี้ เป็นข้อมูลทั่วไปที่ไม่ใช่ข้อมูลส่วนบุคคล

- เลขประจำตัวเฉพาะ ที่สร้างขึ้นจากผลิตภัณฑ์ของคาร์ปาส้กี เพื่อระบุตัวตนของเครื่องมือ โดยไม่มีการระบุผู้ใช้และไม่มีข้อมูลส่วนบุคคล

- ข้อมูลเกี่ยวกับสถานะของการป้องกันไวรัสของเครื่องคอมพิวเตอร์ของท่าน และข้อมูลไฟล์ใดๆ หรือกิจกรรมที่น่าสงสัยว่าจะเป็นโปรแกรมมุ่งร้าย (เช่น ชื่อไวรัส วันที่ เวลาของการตรวจจับได้ ชื่อและขนาดของไฟล์IP หรือพอร์ทที่ถูกโจมตี ชื่อของโปรแกรมที่สงสัยว่าจะเป็นโปรแกรมมุ่งร้าย) ข้อมูลที่เก็บรวบรวมข้างต้นไม่ได้มีข้อมูลที่มีการระบุผู้ใช้และไม่มีข้อมูลส่วนบุคคล

<u>ข้อมูลขยาย</u>

- ข้อมูลเกี่ยวกับโปรแกรมที่ทำการดาวน์โหลดโดยผู้ใช้(URL, ขนาดไฟล์, ชื่อสกุล)

- ข้อมูลเกี่ยวกับโปรแกรมทำการ (ขนาด รายละเอียดของข้อมูล วันที่สร้าง ข้อมูลเกี่ยวกับ PE headers ภูมิภาค ชื่อ สถานที่ โปรแกรมบีบอัดที่ใช้)

ความปลอดภัยของข้อมูลที่เก็บไว้และการส่งข้อมูล

คาร์ปาสกี้แลปรับรองว่า จะทำการรักษาข้อมูลที่เป็นความปลอดภัย ข้อมูลที่เก็บรวบรวมจะรักษาเอาไว้ในเซิร์ฟเวอร์ที่มีการควบคุมการเข้าถึง คาร์ปาสกี้แลปจะทำการรักษาข้อมูลโดยใช้ไฟร์วอลมาตรฐานและระบบการป้องกันรหัสผ่าน คาร์ปาสกี้แลปใช้เทคโนโลยีด้านความปลอดภัยในพิสัยกว้าง และมีวิธีการดำเนินการด้านการรักษาข้อมูลที่เก็บรวบรวมได้ คาร์ปาส้กีแลป มีความมั่นใจในขั้นตอนของการดำเนินการที่มีต่อข้อมูลของท่าน ตามคำกล่าวในถ้อยแถลงนี้ แต่ไม่มีอะไรที่จะรับประกันได้เต็มร้อยถึงการรักษาความปลอดภัยของข้อมูล ไม่ว่าจะเป็นการเก็บ การส่งต่อข้อมูลจากท่านถึงเราหรือจากที่เราส่งบริการไปหาท่าน รวมทั้งขีดจำกัดทางด้านความปลอดภัยของการให้บริการเครือข่ายคาร์ปาส้กี ที่อาจต้องได้รับความเสี่ยงที่เกิดขึ้นได้

ข้อมูลที่ทำการเก็บรวบรวมนี้ จะเป็นไว้ในเซิร์ฟเวอร์ของคาร์ปาส้กีแลป และคาร์ปาส้กีแลป ไม่จำเป็นต้องทำการเตือนล่วงหน้าในเรื่องของความปลอดภัยต่อข้อมูล หากว่าการส่งข้อมูลที่ได้รับมีระดับการ

ป้องกันที่เหมาะสม เราเก็บรักษาข้อมูลเอาไว้ในฐานะที่เป็นข้อมูลความลับ วิธีการในการรักษาความลับและนโยบายการทำงานของบริษัทเกี่ยวกับเรื่องของการป้องกันและการใช้งานของข้อมูลที่เป็นความลับ หลังจากได้ทำการรวบรวมข้อมูลแล้ว เซิร์ฟเวอร์จะมีการเก็บรักษาเอาไว้ทั้งทางกายภาพและทางอิเล็กทรอนิกส์ ที่มีกระบวนการใช้งานรหัสผ่านและบัญชีเข้ารหัส รวมทั้งการรักษาด้วยไฟล์วอลที่กันการเข้าถึงโดยไม่ได้รับอนุญาตจากภายนอก ข้อมูลที่ทำการสะสมโดยเครือข่ายความปลอดภัยคาร์ปาสกี้ ดำเนินการและเก็บรวบรวมไว้ที่สหรัฐอเมริกา และทางกฎหมายอื่นๆ และรวมถึงประเทศอื่นๆที่คาร์ปาสกี้แลปเข้าไปทำธุรกิจ พนักงานของคาร์ปาสกี้ทั้งหมดตระหนักดีถึงนโยบายความปลอดภัย ข้อมูลของท่านที่พนักงานเหล่านั้นเข้าถึง จะต้องมาจากการเข้าถึงในหน้าที่การงาน ข้อมูลที่เก็บรวบรวมเอาไว้จะไม่มีการเชื่อมโยงไปยังข้อมูลส่วนบุคคล คาร์ปาสกี้แลปจะไม่รวมเอาข้อมูลเหล่านั้นมาไว้ด้วยกันไม่ว่าจะเป็น รายการติดต่อ ข้อมูลการเป็นสมาชิก ที่รวบรวมโดยคาร์ปาสกี้แลปเพื่อวัตถุประสงค์อื่น

การใช้งานข้อมูลที่เก็บรวบรวม

<u>เราใช้ข้อมูลส่วนบุคคลท่านอย่างไร</u>

คาร์ปาสกี้แลป ทำการเก็บรวบรวมข้อมูลของท่าน เพื่อการวิเคราะห์ ระบุแหล่งของการเกิดความเสี่ยงต่อความปลอดภัย และปรับปรุงความสามารถในการทำงานของผลิตภัณฑ์คาร์ปาสกี้แลป เพื่อการสืบค้นพฤติกรรมมุ่งร้าย เว็บไซต์หลอกลวง โปรแกรมอาชญากร และภัยคุกคามประเภทอื่นๆบนอินเทอร์เน็ต ในระดับที่ดีที่สุดเพื่อการปกป้องของคาร์ปาสกี้แลปในอนาคต

<u>การเปิดเผยข้อมูลให้แก่บุคคลที่สาม</u>

คาร์ปาสกี้แลปอาจเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากการยินยอมของท่านหากเป็นความต้องการทางกฎหมาย หรือความจำเป็นในการสืบสวนสอบสวน เพื่อป้องกันการกระทำอันเป็นสิ่งอันตรายต่อผู้เข้าร่วม ผู้มาเยือน ผู้เกี่ยวข้องหรือทรัพย์สินของคาร์ปาสกี้แลป ในส่วนของเงื่อนไขและข้อตกลงกับทางบริษัท หรือปกป้องความปลอดภัยแก่ผู้ใช้ และสาธารณะหรือภายใต้ข้อตกลงทางลิขสิทธิ์กับบุคคลที่สาม ที่เข้าร่วมการพัฒนา ปฏิบัติการ หรือรักษาเครือข่ายความปลอดภัยคาร์ปาสกี้ เพื่อการส่งเสริมการตระหนักรู้ การค้นหาและการป้องกันภัยทางอินเทอร์เน็ต คาร์ปาสกี้แลปอาจต้องทำการแบ่งปันข้อมูลกับองค์กรการวิจัยและผู้ขายซอฟต์แวร์อื่นๆ คาร์ปาสกี้แลปอาจใช้สถิติที่ได้จากข้อมูลที่เก็บรวบรวมและทำการตีพิมพ์รายงานแนวโน้มความเสี่ยงด้านความปลอดภัย

ทางเลือกของท่าน

ท่านมีสิทธิเลือกในการเข้าร่วมเป็นส่วนหนึ่งของเครือข่ายความปลอดภัยคาร์ปาสกี้ คุณสามารถทำการเริ่มต้นหรือเลิกล้มได้ตลอดเวลา โดยการเข้าไปยังส่วนการตั้งค่าตอบกลับ ในตัวเลือกบนหน้าของคาร์ปาสกี้แลป

เมื่อระยะเวลาของการบริการของคาร์ปาสกี้แลปสิ้นสุดลง การทำงานของคาร์ปาสกี้ซอฟต์แวร์อาจดำเนินต่อไปในบางอย่าง แต่การส่งข้อมูลถึงคาร์ปาสกี้แลปจะสิ้นสุดลง

เรามีสิทธิที่จะส่งข้อความเตือนไปยังผู้ใช้เพื่อแจ้งการเปลี่ยนแปลงเฉพาะ ที่อาจเกิดผลกระทบต่อความสามารถในการทำงานและการบริการของเรา ที่มีอยู่ก่อนหน้านี้ เรามีสิทธิในการติดต่อกับท่านในส่วนการดำเนินการทางด้านกฎหมาย การฝ่าฝืนในเรื่องของการใช้งานทางลิขสิทธิ์ การรับประกันและสัญญาการซื้อขาย

คาร์ปาสกี้แลปสงวนรักษาสิทธิ์เนื่องมาจากข้อจำกัดบางกรณี ที่อาจทำการติดต่อกับท่านอันเป็นสิ่งสำคัญสำหรับท่าน อันไม่เกี่ยวกับด้านการตลาดและการออกคำสั่งที่ไม่ค่อยมีการติดต่อสื่อสาร

การสะสมข้อมูลในเรื่องของคำถามและข้อติชม

คาร์ปาสกี้แลปมีความตั้งใจจริงในอันที่จะรับฟังข้อคิดเห็น คำถาม หรือคำติชมจากผู้ใช้งาน โดยการส่งอีเมล์เรื่องของข้อคิดเห็น คำถาม หรือคำติชม ที่เกี่ยวกับคาร์ปาสกี้แลปมาที่ support@thaikaspersky.com

อธิบายข้อความรายละเอียดให้ชัดเจนที่สุด เราจะทำการตอบในทุกข้อคิดเห็น คำถาม หรือคำติชม

ผู้ใช้งานสามารถยกเลิกการใช้งานด้านการสะสมสมข้อมูลได้ตลอดเวลา โดยการเข้าไปยังส่วนของ “Feedback” บนหน้า “Settings” ของผลิตภัณฑ์คาร์ปาสกี้ใดๆ

คาร์ปาสกี้แลป

คาร์ปาสกี้แลปผู้นำแห่งเทคโนโลยีความปลอดภัยทางด้านข้อมูล ก่อตั้งขึ้นเมื่อปี 2540 ผลิตซอฟต์แวร์ที่มีประสิทธิภาพสูงในการทำงานเป็น แอนตี้ไวรัส แอนตี้สแปม และแอนตี้ระบบแฮกเกอร์

คาร์ปาสกี้แลปเป็นบริษัทนานาชาติ สำนักงานใหญ่อยู่ที่สหพันธรัฐรัสเซีย มีสำนักงานอยู่ที่สหราชอาณาจักร ฝรั่งเศส เยอรมัน ญี่ปุ่น เบเนลักซ์ จีน โปแลนด์ โรมาเนีย และสหรัฐอเมริกา (แคลิฟอร์เนีย) สำนักงานใหม่เป็นสำนักงานการวิจัยแอนตี้ไวรัส ในประเทศฝรั่งเศสมีกว่า 500 ประเทศจากทั่วโลกที่เป็นพันธมิตรกับคาร์ปาสกี้

ปัจจุบันนี้ พนักงานในคาร์ปาสกี้แลปกว่า450 คนที่เป็นผู้เชี่ยวชาญ ในระดับปริญญาโทกว่าสิบคน ปริญญาเอก 16 คน ผู้เชี่ยวชาญในคาร์ปาสกี้แลปส่วนหนึ่งเป็นสมาชิกอาวุโสขององค์กรนักวิจัยแอนตี้ไวรัสคอมพิวเตอร์ (CARO)

สินทรัยพ์ของเราคือผู้เชี่ยวชาญที่ร่วมกันทำงานต่อต้านไวรัสมากว่า 14 ปี การวิเคราะห์ไวรัสคอมพิวเตอร์ ตลอดจนการวิเคราะห์กิจกรรมของไวรัสโดยผู้ชำนาญการของบริษัท ที่มองเห็นเหตุการณ์ล่วงหน้าของการพัฒนาทางด้านโปรแกรมมุ่งร้าย การต่อต้านการรุกรานในอนาคตที่เป็นพื้นฐานของสินค้าคาร์ปาสกี้ สินค้าของบริษัทยังคงส่งต่อไปยังผู้ค้าเพื่อทำการคุ้มครองลูกค้าของเรา

ตลอดหลายปีที่ทำงานหนักเพื่อให้บริษัทก้าวเป็นบริษัทแอนตี้ไวรัสอันดับหนึ่งของโลก คาร์ปาสกีแลปเป็นบริษัทแห่งแรกที่ทำการพัฒนาทางด้านซอฟต์แวร์แอนตี้ไวรัสที่มีมาตรฐานทันสมัยเป้าหมายสำคัญของบริษัทคาร์ปาสกี้ คือการผลิตสินค้าที่เต็มไปด้วยมาตรฐานแห่งการป้องกัน แก่เครือข่ายและสถานีการทำงาน ไฟล์เซิร์ฟเวอร์ ระบบเมล์ ไฟร์วอล ช่องทางอินเทอร์เน็ต และคอมพิวเตอร์พกพา ให้ง่ายต่อการจัดการสำหรับเครื่องคอมพิวเตอร์และเครือข่าย ผู้ผลิตที่มีชื่อเสียงจำนวนมากเลือกใช้งานคาร์ปาสกี้ อย่างเช่น Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybaris (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada)

ลูกค้าของคาร์ปาสกี้แลป ได้รับบริการเสริมเพิ่มเติมที่มั่นใจ ในบริษัทที่มั่นคง ผลิตภัณฑ์ของบริษัทตามความต้องการของธุรกิจ เราออกแบบให้มีการทำงานและสนับสนุนการใช้งานแอนตี้ไวรัสในที่อัน

ซับซ้อน ฐานข้อมูลของคาร์ปาสกี้แลปมีการอัพเดททุกชั่วโมง รวมทั้งการมีหน่วยสนับสนุนทางเทคนิคตลอด 24 ชั่วโมง

<u>เนื้อหาในส่วนนี้ประกอบไปด้วย</u>

ผลิตภัณฑ์อื่นๆ ของคาร์ปาสกี้

ติดต่อเรา

ผลิตภัณฑ์อื่นๆ ของคาร์ปาสกี้

<u>หน่วยข่าวของคาร์ปาสกี้แลป</u>

โปรแกรมหน่วยข่าวของคาร์ปาสกี้แลปเป็นการดำเนินการด้านข่าวสารที่รวดเร็วของคาร์ปาสกี้แลปในอันที่จะแจ้งให้ทราบถึงเรื่องของการเกิดไวรัส และเหตุการณ์ล่าสุด โปรแกรมทำการอ่านรายการช่องข่าวที่มีอยู่และข้อมูลที่ประกอบขึ้นจากเซิร์ฟเวอร์ข่าวคาร์ปาสกี้ที่มีช่วงเวลาเหตุการณ์

นอกจากนี้หน่วยงานยังให้ผู้ใช้ทำได้ต่อไปนี้

- มองเห็นสภาพของไวรัสในระบบแผงควบคุม
- บอกรับหรือปฏิเสธการรับข่าวจากช่องทางของคาร์ปาสกี้แลป
- รับข่าวในแต่ละช่องทางที่บอกรับด้วยการเลือกจากความถี่ในการบอกรับ หรือการเลือกเพิ่มเติมสำหรับข่าวที่ยังไม่ได้อ่าน
- ดูข่าวบนช่องทางที่บอกรับ
- ดูรายการของช่องทางบนสถานะของช่องทาง
- เปิดหน้าบราวเซอร์เพื่อดูรายละเอียดของข่าว

หน่วยข่าวสามารถทำงานได้บน Microsoft Windows และยังทำงานลงบนโปรแกรมเดี่ยวอื่นๆ อีก รวมทั้งการแก้ปัญหาที่รวมกันของคาร์ปาสกี้แลป

Kaspersky® Online Scanner

โปรแกรมนี้เป็นโปรแกรมฟรีใช้กับผู้ที่เข้ามาเยี่ยมชมเว็บไซต์ของบริษัท แล้วโปรแกรมจะทำการตรวจจับไวรัสที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ของผู้ที่เข้ามาเยี่ยมชม และทำการกำจัดไวรัสเหล่านั้นออนไลน์ Kaspersky® Online Scanner ทำงานบนบราวเซอร์ และทำการตัดสินใจว่ามีใครเป็นโปรแกรมมุ่งร้าย ในการตรวจจับผู้ใช้งานสามารถทำได้ดังต่อไปนี้

- แยกตัวเก็บและฐานข้อมูลของเมล์ออกจากการตรวจสอบ
- ใช้ฐานข้อมูลมาตรฐานและฐานข้อมูลเพิ่มเติมในการตรวจสอบ
- บันทึกผลการตรวจจับไว้ในไฟล์txt หรือ html

Kaspersky® Online Scanner Pro

โปรแกรมนี้เป็นโปรแกรมบอกรับเป็นสมาชิก ใช้กับผู้ที่เข้ามาเยี่ยมชมเว็บไซต์ของบริษัท แล้วโปรแกรมจะทำการตรวจจับไวรัสที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ของผู้ที่เข้ามาเยี่ยมชม และทำการกำจัดไวรัสเหล่านั้นออนไลน์ Kaspersky® Online Scanner Pro ทำงานได้โดยตรงบนบราวเซอร์ ในการตรวจจับผู้ใช้งานสามารถทำได้ดังต่อไปนี้

- แยกตัวเก็บและฐานข้อมูลของเมล์ออกจากการตรวจสอบ
- ใช้ฐานข้อมูลมาตรฐานและฐานข้อมูลเพิ่มเติมในการตรวจสอบ
- ทำการกำจัดไวรัสเมื่อพบการติดเชื้อ
- บันทึกผลการตรวจจับไว้ในไฟล์txt หรือ html

Kaspersky Anti-Virus® Mobile

Kaspersky Anti-Virus® Mobile เพื่อการปกป้องไวรัสบนอุปกรณ์เคลื่อนที่ ที่ทำงานบนSymbian OS หรือระบบปฏิบัติการ Microsoft Windows Mobile การทำงานการตรวจสอบไวรัสประกอบไปด้วย

- การตรวจสอบตามคำสั่งของหน่วยความจำบนเครื่อง การ์ดความจำ โฟลเดอร์และไฟล์แยก เมื่อพบว่ามีการติดเชื้อจะทำการแยกออกและกำจัดได้
- การป้องกันแบบเรียลไทม์ วัตถุที่มีการเปลี่ยนแปลงหรือเข้ามายังอุปกรณ์จะมีการตรวจจับ เมื่อไฟล์นั้นเข้ามายังอุปกรณ์
- การป้องกันสแปม SMS และ MMS

Kaspersky Anti-Virus for File Servers

ชุดซอฟต์แวร์นี้ เพื่อให้ความมั่นใจในการปกป้องโปรแกรมมุ่งร้ายสำหรับระบบไฟล์ของเซิร์ฟเวอร์ที่ดำเนินการบน Microsoft Windows, Novell NetWare และระบบปฏิบัติการ Linux ชุดซอฟต์แวร์นี้ประกอบไปด้วย

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Anti-Virus for Novell Netware
- Kaspersky Anti-Virus for Samba Server

<u>ความสามารถในการทำงานและประโยชน์</u>

- การปกป้องแบบเรียลไทม์แก่ระบบไฟล์ของเซิร์ฟเวอร์ ไฟร์ของเซิร์ฟเวอร์ทั้งหมดจะได้รับการตรวจสอบเมื่อมีการเปิดการทำงาน หรือการบันทึกลงบนเซิร์ฟเวอร์
- การป้องการเกิดไวรัสแบบกระทันหัน
- การตรวจสอบไฟล์ระบบทั้งหมดตามความต้องการ หรือไฟล์หรือโฟลเดอร์แยก

- ใช้เทคโนโลยีสูงสุดในการตรวจสอบวัตถุจองระบบไฟล์ของเซิร์ฟเวอร์
- กู้คืนระบบหลังจากการติดเชื้อ
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- รักษาความสมดุลของการโหลดในระบบ (Load balance)
- สร้างรายการน่าเชื่อถือ ต่อกิจกรรมที่เกิดขึ้นในเซิร์ฟเวอร์เพื่อไม่ต้องเฝ้าระวังในรายการนี้
- การควบคุมระยะไกล รวมทั้งการติดตั้งจากส่วนกลาง การตั้งค่าและการจัดการ
- เก็บสำเนาข้อมูลสำรองของวัตถุที่ลบทิ้งหรือติดเชื้อในกรณีต้องการกู้คืน
- แยกวัตถุที่ต้องสงสัยยังพื้นที่เก็บพิเศษ
- รักษารายงานอย่างละเอียด
- อัพเดทฐานข้อมูลอย่างอัตโนมัติของชุดซอฟต์แวร์

Kaspersky Open Space Security

Kaspersky Open Space Security เป็นชุดซอฟต์แวร์ด้านความปลอดภัยตัวใหม่ที่ตรงกับเครือข่ายบริษัทที่มีความทันสมัยในทุกรูปแบบ และให้การปกป้องส่วนกลางของระบบข้อมูลและการควบคุมออฟฟิศระยะไกล รวมทั้งผู้ใช้งานเคลื่อนที่

ชุดซอฟต์แวร์ประกอบไปด้วย

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

คำอธิบายของแต่ละผลิตภัณฑ์มีดังต่อไปนี้

Kaspersky Work Space Security เป็นผลิตภัณฑ์ ที่ออกแบบมาเพื่อการปกป้องส่วนกลางสำหรับสถานีการทำงานในเครือข่ายองค์กรและอื่นๆ เพื่อการต่อต้านภัยคุกคามทางอินเทอร์เน็ตสมัยใหม่อย่างเช่น ไวรัส สปายแวร์ การบุกรุก และสแปม

<u>ความสามารถในการทำงานและประโยชน์</u>

- ป้องกันจากไวรัส สปายแวร์ การบุกรุก และสแปม อย่างเต็มรูปแบบ
- ปกป้องก่อนการเกิดโปรแกรมมุ่งร้ายตัวใหม่
- ไฟร์วอลส่วนบุคคลด้วยระบบการตรวจจับผู้บุกรุก และป้องกันการจู่โจมระบบ
- ย้อนกลับไปก่อนการเกิดโปรแกรมมุ่งร้ายทำลายระบบ
- ปกป้องการจู่โจมแบบฟิชชิ่งและสแปม
- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- ตรวจสอบทราฟฟิกอีเมล์และอินเทอร์เน็ตในแบบเรียลไทม์
- สกัดกั้นหน้าต่างแสดงโฆษณาและแบนเนอ์บนอินเทอร์เน็ต
- ให้ความปลอดภัยด้านการทำงานกับเครือข่าย ประเภทไวไฟ
- มีเครื่องมือในการกู้ข้อมูลหลังจากการจู่โจมจากไวรัส
- ระบบที่พัฒนาเต็มรูปแบบในการรายงานเกี่ยวกับสถานะการปกป้อง
- อัพเดทฐานข้อมูลอย่างอัตโนมัติ
- สนับสนุนการทำงานของระบบปฏิบัติการ64-bit
- เหมาะสมกับการใช้งานบนคอมพิวเตอร์พกพา (Intel® Centrino® Duo technology for mobile PC)

- กำจัดไวรัสในระยะไกล(Intel® Active Management technology, component Intel® vPro™)

Kaspersky Business Space Security เพื่อความมั่นใจในการปกป้องที่ดีที่สุดของทรัพยากรข้อมูล เพื่อต่อต้านภัยคุกคามทางอินเทอร์เน็ตสมัยใหม่Kaspersky Business Space Security จึงมีการพัฒนาเพื่อการทำงานได้กับทั้งสถานีการทำงาน และไฟล์เซิร์ฟเวอร์เพื่อป้องกันประเภทของไวรัส โปรแกรมโทรจันและหนอนอินเทอร์เน็ต ป้องกันการเกิดไวรัสแบบกระทันหัน และความมั่นใจต่อความปลอดภัยของข้อมูล และการเข้าถึงแหล่งทรัพยากรเครือข่ายในทันที

<u>ความสามารถในการทำงานและประโยชน์</u>

- ระบบการจัดการระยะไกลของโปรแกรม ทำให้สามารถจัดการ และตั้งค่า รวมทั้งติดตั้งโปรแกรมได้ในระยะไกล
- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- ปกป้องสถานีการทำงานและไฟล์เซิร์ฟเวอร์จากภัยคุกคามทางอินเทอร์เน็ตทุกประเภท
- กระจายการโหลดระหว่างตัวดำเนินการของเซิร์ฟเวอร์
- แยกโปรแกรมมุ่งร้ายออกไปเก็บที่พิเศษ
- กู้คืนระบบหลังจากการติดเชื้อ
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- รักษาความสมดุลของการโหลดในระบบ (Load balance)
- สร้างรายการน่าเชื่อถือ ต่อกิจกรรมที่เกิดขึ้นในเซิร์ฟเวอร์เพื่อไม่ต้องเฝ้าระวังในรายการนี้
- การควบคุมระยะไกล รวมทั้งการติดตั้งจากส่วนกลาง การตั้งค่าและการจัดการ
- เก็บสำเนาข้อมูลสำรองของวัตถุที่ลบทิ้งหรือติดเชื้อในกรณีต้องการกู้คืน

- แยกวัตถุที่ต้องสงสัยยังพื้นที่เก็บพิเศษ
- รักษารายงานอย่างละเอียด
- อัพเดทฐานข้อมูลอย่างอัตโนมัติของชุดซอฟต์แวร์

Kaspersky Enterprise Space Security

โปรแกรมนี้ใช้เพื่อการปกป้องสถานีการทำงาน และกลุ่มเซิร์ฟเวอร์เพื่อป้องกันประเภทของไวรัส โปรแกรมโทรจันและหนอนอินเทอร์เน็ต ป้องกันการเกิดไวรัสแบบกระทันหัน และความมั่นใจต่อความปลอดภัยของข้อมูล และการเข้าถึงแหล่งทรัพยากรเครือข่ายในทันที

<u>ความสามารถในการทำงานและประโยชน์</u>

- ปกป้องสถานีการทำงาน และกลุ่มเซิร์ฟเวอร์เพื่อป้องกันประเภทของไวรัส โปรแกรมโทรจันและหนอนอินเทอร์เน็ต ป้องกันการเกิดไวรัสแบบกระทันหัน
- ปกป้องซอฟต์แวร์เมล์เซิร์ฟเวอร์ รวมทั้งSendmail, Qmail, Postfix และ Exim
- ตรวจสอบข้อความทั้งหมดในMicrosoft Exchange server รวมทั้งโฟลเดอร์ร่วม
- ดำเนินการกับข้อความ ฐานข้อมูล และวัตถุอื่นๆของLotus Domino servers
- ป้องกันการเกิดฟิชชิ่งและสแปม
- ป้องกันการเกิดเมล์ล้นและไวรัสกระทันหัน
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- ระบบการจัดการระยะไกลของโปรแกรม ทำให้สามารถจัดการ และตั้งค่า รวมทั้งติดตั้งโปรแกรมได้ในระยะไกล
- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- ไฟร์วอลส่วนบุคคลด้วยระบบการตรวจจับผู้บุกรุก และป้องกันการจู่โจมระบบ

- ให้ความปลอดภัยภายในเครือข่ายระบบไร้สายไวไฟ
- ตรวจสอบทราฟฟิกในอินเทอร์เน็ตแบบเรียลไทม์
- กู้คืนระบบหลังจากการติดเชื้อ
- จัดสรรพื้นที่แบบไดนามิกแก้แหล่งทรัพยากรระหว่างการตรวจสอบ
- แยกโปรแกรมมุ่งร้ายออกไปเก็บที่พิเศษ
- ระบบที่พัฒนาเต็มรูปแบบในการรายงานเกี่ยวกับสถานะการปกป้อง
- อัพเดทฐานข้อมูลอย่างอัตโนมัติ

Kaspersky Total Space Security

โปรแกรมนี้เป็นที่ควบคุมกระแสเข้าออกของข้อมูล อีเมล์ ทราฟฟิกเว็บ และการปฏิสัมพันธ์การทำงานทั้งหมดของเครือข่าย มีส่วนผสมของการปกป้องสถานีการทำงานและอุปกรณ์เคลื่อนที่ เพื่อความมั่นใจในความปลอดภัยของผู้ใช้ในองค์กรผ่านอินเทอร์เน็ต และรับประกันได้ถึงความมั่นใจในการสื่อสารทางเมล์

<u>ความสามารถในการทำงานและประโยชน์</u>

- การปกป้องที่ครอบคลุมในเรื่องของไวรัส การจู่โจมบุกรุก และสแปมในระดับของเครือข่ายบริษัท จากสถานีการทำงานถึงเกตเวย์
- ปกป้องก่อนการเกิดโปรแกรมมุ่งร้ายตัวใหม่ในสถานีการทำงาน

- ปกป้องเมล์เซิร์ฟเวอร์และแชร์เซิร์ฟเวอร์
- การตรวจสอบแบบเรียลไทม์ ของทราฟฟิกเว็บภายใน (HTTP / FTP)
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- สกัดกั้นการทำงานจากสถานีการทำงานที่ติดเชื้อ
- ป้องกันการเกิดไวรัสแบบกระทันหัน
- การจัดการส่วนกลางในการรายงานสถานะการป้องกัน
- ระบบการจัดการระยะไกลของโปรแกรม ทำให้สามารถจัดการ และตั้งค่า รวมทั้งติดตั้งโปรแกรมได้ในระยะไกล
- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- สนับสนุน hardware proxy servers
- กรองทราฟฟิกอินเทอร์เน็ตตามรายการเซิร์ฟเวอร์ที่น่าเชื่อถือ ประเภทของวัตถุและกลุ่มของผู้ใช้
- ใช้เทคโนโลยีของ iSwift เพื่อกำหนดการตรวจสอบภายในเซิร์ฟเวอร์
- จัดสรรพื้นที่แบบไดนามิกแก้แหล่งทรัพยากรระหว่างการตรวจสอบ
- ไฟร์วอลส่วนบุคคลด้วยระบบการตรวจจับผู้บุกรุก และป้องกันการจู่โจมระบบ
- ให้ความปลอดภัยภายในเครือข่ายระบบไร้สายไวไฟ
- ป้องกันการเกิดฟิชชิ่งและสแปม
- กำจัดไวรัสในระยะไกล (Intel® Active Management technology, component Intel® vPro™)

- กู้คืนระบบหลังจากการติดเชื้อ
- เทคโนโลยีการปกป้องตนเองของโปรแกรมที่มีต่อโปรแกรมมุ่งร้าย
- สนับสนุนการทำงานของระบบปฏิบัติการ64-bit
- อัพเดทฐานข้อมูลอย่างอัตโนมัติ

Kaspersky Security for Mail Servers

ชุดซอฟต์แวร์ตัวนี้ป้องกันเมล์เซิร์ฟเวอร์และแชร์เซิร์ฟเวอร์ การปกป้องเมล์เซิร์ฟเวอร์ อันได้แก่ Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix และ Exim ประกอบไปด้วย

- Kaspersky Administration Kit
- Kaspersky Mail Gateway
- Kaspersky Anti-Virus for Lotus Notes/Domino
- Kaspersky Anti-Virus for Microsoft Exchange
- Kaspersky Anti-Virus® for Linux Mail Server.

<u>ความสามารถในการทำงานและประโยชน์</u>

- การปกป้องที่น่าเชื่อถือในการต่อต้านโปรแกรมมุ่งร้าย และโปรแกรมที่อันตรายทั้งหลาย
- ตัวกรองสแปม
- การตรวจสอบเมล์เข้าและออกรวมทั้งไฟล์แนบ

- การตรวจสอบแอนตี้ไวรัสของข้อความทั้งหมดบนMicrosoft Exchange server รวมทั้งโฟลเดอร์ที่เปิดร่วม
- การตรวจสอบข้อความ ฐานข้อมูลและวัตถุอื่นๆในLotus Domino servers
- การกรองข้อความที่แนบมา
- แยกโปรแกรมมุ่งร้ายออกไปเก็บที่พิเศษ
- ระบบการจัดการที่สะดวก
- การป้องกันไวรัสแบบกระทันหัน
- เฝ้าดูสถานะระบบการป้องกันโดยการแจ้งเตือน
- ระบบการรายงานเกี่ยวกับกาดำเนินการโปรแกรม
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- อัพเดทฐานข้อมูลอย่างอัตโนมัติ

Kaspersky Security for Gateways

ชุดซอฟต์แวร์นี้ เพื่อให้เกิดความปลอดภัยต่อการเข้าถึงอินเทอร์เน็ตของพนักงานทั้งบริษัท การเคลื่อนย้ายโปรแกรมมุ่งร้ายอัตโนมัติ และโปรแกรมที่มีความเสี่ยงออกจากข้อมูลที่ได้รับผ่านทางเครือข่ายโปรโตคอล HTTP/FTP การแก้ปัญหานี้ประกอบด้วย

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Proxy Server
- Kaspersky Anti-Virus for Microsoft ISA Server
- Kaspersky Anti-Virus for Check Point FireWall-1

ความสามารถในการทำงานและประโยชน์

- การปกป้องที่น่าเชื่อถือในการต่อต้านโปรแกรมมุ่งร้าย และโปรแกรมที่อันตรายทั้งหลาย
- ตรวจสอบทราฟฟิกอินเทอร์เน็ต HTTP/FTP ในโหมดเรียลไทม์
- กรองทราฟฟิกอินเทอร์เน็ต ตามรายการเซิร์ฟเวอร์ที่น่าเชื่อถือ ประเภทของวัตถุและกลุ่มของผู้ใช้
- แยกวัตถุที่ต้องสงสัยไว้ในโฟลเดอร์พิเศษ
- ระบบการควบคุมที่สะดวก
- ระบบการรายงานเกี่ยวกับการดำเนินการของโปรแกรม
- สนับสนุนการทำงานhardware proxy servers
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- อัพเดทฐานข้อมูลอย่างอัตโนมัติ

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam เป็นซอฟต์แวร์ของชาวรัสเซีย ที่ทำการปกป้องบริษัทขนาดเล็กและขนาดกลางจากสแปม ผลิตภัณฑ์ผสมผสานเทคโนโลยี ที่ได้มาจากการวิเคราะห์เนื้อหาทางภาษา ด้วยวิธีการที่ทันสมัยในการกรองสแปม(รวมทั้ง DNS ที่มาจากข้อความ) และการบริการที่มีความเป็นหนึ่งเดียว ช่วยให้ผู้ใช้ลดปริมาณทราฟฟิกที่ไม่ต้องการได้ถึงร้อยละ95

Kaspersky® Anti-Spam มีการกระทำที่เรียกว่าการกรองทางเข้า ของเครือข่ายบริษัท ทำการตรวจสอบข้อความเข้าเพื่อหาสแปม โดยสามารถทำงานร่วมกับเครือข่ายของผู้ใช้ที่มีการติดตั้งเมล์เซิร์ฟเวอร์เอาไว้

ประสิทธิภาพสูงของโปรแกรม ช่วยให้สามารถทำการอัพเดทได้ทุกวัน กับฐานข้อมูลการกรองเนื้อหา โดยการใช้ตัวอย่างที่จัดขึ้นโดยผู้เชี่ยวชาญคาร์ปาสกี้แลป ที่ออกมาทุก20 นาที

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper ให้ความมั่นใจได้ในตรวจสอบไวรัสความเร็วสูง สำหรับเซิร์ฟเวอร์ที่ใช้งาน Clearswift MIMEsweeper สำหรับ SMTP / Clearswift MIMEsweeper สำหรับ Exchange / Clearswift MIMEsweeper สำหรับ Web

โปรแกรมนี้แค่ทำการใส่เข้าไป (โมดูลเพิ่มเติม) และมีการทำงานตรวจสอบไวรัสในแบบเรียลไทม์ ในข้อความเมล์เข้าและออก

ติดต่อเรา

บริษัทไอคอมเทค จำกัด

33/4 The 9th Tower, ชั้น G (ห้อง G10,G11) ถ.พระราม9 แขวงห้วยขวาง เขตห้วยขวาง

กรุงเทพฯ 10310

โทร 662-6432150-1 Fax 662-6432152

www.thaikaspersky.com

CRYPTOEX LLC

เพื่อการสร้างและยืนยันลายเซ็นต์ดิจิตอล คาร์ปาสกี้แอนตี้ไวรัสจึงใช้ Crypto Ex LLC's data security software library, Crypto C

Crypto Ex เป็นลิขสิทธิ์จาก Federal Agency for Government Communications and Information (สาขาการบริการความปลอดภัยสหพันธรัฐ) เพื่อการพัฒนา การผลิต และกระจายซอฟต์แวร์เข้ารหัสที่ไม่ได้มีการบัญญัติไว้ในเอกสารเก่า

Crypto C library ออกแบบมาเพื่อการปกป้องคลาด KS1 อันเป็นข้อมูลความลับที่ได้รับการออกอนุญาตที่ No. SF/114-0901 เมื่อวันที่1 กรกฎาคม 2549

เทคโนโลยีในการเข้ารหัส ถอดรหัส ของขนาดข้อมูลที่มีการกำหนดขอบเขตมีดังต่อไปนี้

- อัลกอริทึมการเข้ารหัสภาพ(GOST 28147-89);
- อัลกอริทึมสำหรับการสร้างและยืนยันลายเซ็นต์อิเล็กทรอนิกส์บนอัลกอริทึม(GOST R 34.10-94 and GOST 34.10-2001);
- ทำหน้าที่อย่างละเอียด (GOST 34.11-94);
- สร้างคีย์ข้อมูลในการใช้การสุ่มเทียม
- สร้างคีย์ข้อมูลในการกระตุ้นระบบการสร้างเวกเตอร์(GOST 28147-89).

รูปแบบของไลบรารีจะอยู่ใน ANSI มาตรฐาน C และสามารถเข้าสู่โปรแกรมได้ทั้งรหัสโหลดเคลื่อนไหวและคงที่ ประกอบไปด้วย x86, x86-64, Ultra SPARC II และแพลตฟอร์มทีทำงานร่วมกันได้ที่

ระบบปฏิบัติการ Microsoft Windows NT/XP/98/2000/2003, UNIX (Linux, FreeBSD, SCO Open UNIX 8.0, SUN Solaris, SUN Solaris สำหรับ Ultra SPARC II)

สำหรับข้อมูลเพิ่มเติมให้เข้าไปที่ CryptoEx LLC corporate เว็บไซต์ http://www.cryptoex.ru, or ติดต่อทางอีเมล์ที่ info@cryptoex.ru

มูลนิธิ มอซิลลา

Library Gecko SDK ver. 1.8 ใช้เพื่อการพัฒนาส่วนประกอบของโปรแกรม

สำหรับรายละเอียดเพิ่มดูได้ที่ library Gecko SDK เว็บไซต์ http://developer.mozilla.org/en/docs/Gecko_SDK.

Mozilla Foundation website: http://www.mozilla.org

ข้อตกลงทางลิขสิทธิ์

ข้อตกลงทางลิขสิทธิ์กับผู้ใช้แบบมาตรฐาน

เรียนผู้ใช้ทราบว่า กรุณาอ่านอย่างละเอียดสำหรับข้อตกลงทางกฎหมาย (หรือเรียกว่า “ข้อตกลง”) สำหรับลิขสิทธิ์คาร์ปาสกี้แอนตี้ไวรัส (หรือเรียกว่า “ซอฟต์แวร์”) ที่ผลิตโดยคาร์ปาสกี้แลป (หรือเรียกว่า “คาร์ปาสกี้แลป”)

หากว่าท่านทำการซื้อซอฟต์แวร์นี้ผ่านทางอินเทอร์เน็ต โดยการคลิกที่ปุ่มตกลงการซื้อ ท่าน (ทั้งที่เป็นบุคคล หรือกลุ่มคณะ) ได้ยินยอมแล้วในการเข้าร่วมเป็นส่วนหนึ่งในข้อตกลงทางลิขสิทธิ์นี้ หากว่าท่านไม่เห็นด้วยตามข้อตกลงนี้ ให้คลิกที่ปุ่มไม่ตกลงและไม่ต้องทำการติดตั้งซอฟต์แวร์นี้

หากว่าท่านทำการซื้อซอฟต์แวร์นี้ผ่านทางตัวแทนการขาย ท่าน (ทั้งที่เป็นบุคคล หรือกลุ่มคณะ) ได้ทำการเปิด CD เรียบร้อยแล้ว จะถือว่าท่านได้ยินยอมแล้วในการเข้าร่วมเป็นส่วนหนึ่งในข้อตกลงทางลิขสิทธิ์นี้ หากว่าท่านไม่เห็นด้วยตามข้อตกลงนี้ท่านจะต้องไม่ทำการเปิดCD ดาวน์โหลด ติดตั้ง หรือใช้งานซอฟต์แวร์

ตามบทกฎหมาย เนื่องด้วยซอฟต์แวร์คาร์ปาสกี้ เป็นการใช้งานส่วนบุคคล หากท่านจะซื้อผ่านทางคาร์ปาสกี้แลปออนไลน์ หรือเว็บไซต์ของพันธมิตร ลูกค้าจะมีเวลา14 วันหลังจากวันที่ได้รับส่งมอบของเพื่อการคืนสินค้าหรือการคืนเงิน หากยังไม่มีการใช้งานซอฟต์แวร์

เนื่องด้วยซอฟต์แวร์คาร์ปาสกี้ เป็นการใช้งานส่วนบุคคล หากลูกค้าไม่ได้ซื้อซอฟต์แวร์ผ่านทางออนไลน์อินเทอร์เน็ต ไม่มีการคืนสินค้ายกเว้นทางพันธมิตรมีการกระทำในกรณีตรงข้ามกัน ในกรณีนี้คาร์ปาสกี้แลปจะไม่ยึดถือจากตัวบทของพันธมิตร

สิทธิของการคืนสินค้านั้นจะต้องเป็นสินค้าของดั้งเดิมเท่านั้น

การอ้างอิงทั้งหมดถึง“ซอฟต์แวร์” ถือว่ารวมไปถึงรหัสการเริ่มต้นทำงานซอฟต์แวร์ ที่ได้รับมาจากการเป็นส่วนหนึ่งของคาร์ปาสกี้แอนตี้ไวรัสของคาร์ปาสกี้แลป

1. <u>การอนุญาตทางลิขสิทธิ์</u> ภายใต้เงื่อนไขการชำระเงินให้กับอายุของลิขสิทธิ์ และภายใต้เงื่อนไขและข้อตกลงแห่งสัญญา คาร์ปาสกี้แลปยินยอมให้มีการใช้งานซอฟต์แวร์และเอกสารคู่มือ ("เอกสารคู่มือ") ภายใต้เงื่อนไขของตามธุรกิจที่ท่านอาจติดตั้งโปรแกรม 1 ครั้งสำเนาของซอฟต์แวร์กับคอมพิวเตอร์เครื่องเดียว

   1.1 การใช้ หากว่าซอฟต์แวร์ที่ซื้อมาจากสื่อกลาง ท่านมีสิทธิในการใช้ซอฟต์แวร์ในการปกป้องจำนวนของคอมพิวเตอร์ตามที่กำหนดเอาไว้ตอนซื้อ หรือตอนที่สั่งซื้อซอฟต์แวร์การปกป้อง

      1.1.1 ซอฟต์แวร์ที่ใช้ในเครื่องคอมพิวเตอร์ เมื่อมีการโหลดลงในหน่วยความจำชั่วคราว (เช่นหน่วยความจำแบบสุ่ม หรือแรม) หรือมีการติดตั้งลงในหน่วยความจำถาวร (เช่น ฮาร์ดดิกส์ CD-ROM หรือหน่วยเก็บความจำอื่นๆ) ของเครื่องคอมพิวเตอร์ อำนาจของลิขสิทธิ์นี้ ตามกฎหมายหากท่านมีการทำสำเนาเพื่อการสำรองข้อมูล ไว้ในที่ต่างๆ หรือการทำสำเนาส่วนหนึ่งส่วนใดของซอฟต์แวร์อันเป็นสมบัตินั้น ก็เพื่อการสำรองข้อมูลเท่านั้น ท่านจะต้องทำการเก็บรักษาสำเนาข้อมูลเหล่านั้นเพื่อการป้องกันการนำเอาซอฟต์แวร์ไปใช้โดยไม่ได้รับอนุญาต

      1.1.2 ซอฟต์แวร์ปกป้องคอมพิวเตอร์ป้องกันไวรัส ประกอบไปด้วยฐานข้อมูลในการอัพเดทลายเซ็นต์ไวรัสซึ่งมีอยู่บนเซิร์ฟเวอร์ของคาร์ปาสกี้

      1.1.3 หากว่าท่านขายเครื่องคอมพิวเตอร์ที่มีการติดตั้งซอฟต์แวร์ ท่านต้องแน่ใจว่าได้ลบซอฟต์แวร์เวอร์ชั่นก่อนหน้าไปเรียบร้อยแล้ว

      1.1.4 ท่านจะไม่ทำการถอดโปรแกรม แก้ไขทางวิศวกร แยกหรือทำการลดส่วนใดของซอฟต์แวร์เพื่อให้บุคคลที่สามที่ไม่ได้รับอนุญาตสามารถอ่านได้ ข้อมูลจำเป็นของตัวประสานการทำงานระหว่างผู้ใช้เพื่อให้มีการทำงานร่วมกันของซอฟต์แวร์ที่ทำขึ้นเพิ่มจำนวนโปรแกรมคอมพิวเตอร์ โดยคาร์ปาสกี้มีค่าใช้จ่ายที่

สมเหตุสมผลในการดำเนินการนั้น ด้วยเหตุที่คาร์ปาสกี้แลปไม่มีแนวโน้มในการทำขั้นตอนให้สามารถทำงานร่วมกันได้ เราจะมีการทำการถอดโปรแกรม แก้ไขทางวิศวกร แยกหรือทำการลดส่วนใดของซอฟต์แวร์โดยได้รับอนุญาตจากกฎหมายเท่านั้น

1.1.5 ท่านจะไม่ทำการแก้ไข เปลี่ยนแปลง แปลความหรือไม่ทำอะไรนอกเหนือไปจากเดิมของซอฟต์แวร์ จากบุคคลที่สามผู้ที่ไม่ได้รับอนุญาต

1.1.6 ท่านจะไม่ทำการให้เช่า เช่าช่วงหรือให้ยืมซอฟต์แวร์แก่บุคคลใดและไม่ทำการโอนถ่ายลิขสิทธิ์ของท่านไปให้ใคร

1.1.7 ท่านจะไม่จัดหาคีย์หรือรหัสให้แก่บุคคลที่สาม รหัสการเริ่มต้นโปรแกรมนั้นถือว่าเป็นข้อมูลความลับ

1.1.8 คาร์ปาสกี้แลปอาจขอให้ท่านทำการติดตั้งเวอร์ชันล่าสุด ของซอฟต์แวร์ (เวอร์ชั่นล่าสุดและเวอร์ชั่นรักษาล่าสุด)

1.1.9 ท่านจะไม่ใช้โปรแกรมไปในทางการสร้างไวรัสโดยอัตโนมัติกึ่งอัตโนมัติหรือด้วยมือ ให้เป็นไวรัส ข้อมูลหรือรหัสใดที่เป็นโปรแกรมมุ่งร้าย

1.1.10 ด้วยความยินยอมของท่านในข้อตกลงนี้ คาร์ปาสกี้แลปมีสิทธิในการรวบรวมข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ของเครื่องคอมพิวเตอร์ของท่าน เพื่อนำข้อมูลเหล่านั้นมาเป็นการปรับปรุงการทำงานของคาร์ปาสกี้แลป

2. <u>การสนับสนุน</u>

(i) คาร์ปาสกี้แลปจัดหาบริการการสนับสนุน ("การบริการการสนับสนุน") ตามระยะเวลาของลิขสิทธิ์ที่ระบุไว้ข้างล่างใน License Key File (ระยะเวลาการบริการ) ที่แสดงไว้ในหน้าต่าง "Service" จากการกระทำดังนี้

a. การชำระเงินตามค่าการสนับสนุน และ

b. การกรอกเอกสารการบอกรับการบริการการสนับสนุนที่ได้ให้ไว้ในข้อตกลงนี้ หรืออยู่ที่คาร์ปาสกี้เว็บไซต์ ซึ่งท่านต้องกรอกรหัสการเริ่มต้นโปรแกรม (Activation code) ที่เป็นไปตามสัญญานี้ การตัดสินใจขั้นเด็ดขาดขึ้นอยู่กับคาร์ปาสกี้แลป หรือความพอใจของท่านตามเงื่อนไขของการบริการสนับสนุน

การบริการสนับสนุนเริ่มขึ้นเมื่อมีการเริ่มต้นโปรแกรมโดยการลงทะเบียน ฝ่ายสนับสนุนทางเทคนิคของคาร์ปาสกี้ จะเข้าสู่ความต้องการในการสนับสนุนทางเทคนิคของท่านเพื่อทำการยืนยันการสนับสนุน

(ii) การบริการการสนับสนุนจะสิ้นสุดลงเมื่อไม่มีการต่ออายุลิขสิทธิ์โดยการชำระเงิน เมื่อมีการชำระเงินประจำปีอีกครั้งก็จะสามารถเข้าสู่แบบการขอสนับสนุนทางเทคนิคได้

(iii) "การบริการการสนับสนุน" หมายถึง

a. การอัพเดทปกติของแอนตี้ไวรัส

b. การอัพเดทซอฟต์แวร์ฟรี รวมถึงการอัพเดทเวอร์ชั่นใหม่

c. การสนับสนุนทางเทคนิคผ่านทางอินเทอร์เน็ตและสายด่วยจากผู้ขาย

d. การตรวจจับไวรัสและการกำจัดตลอด 24 ชั่วโมง

(iv) การบริการการสนับสนุนมีการจัดหาให้ในกรณีที่มีเวอร์ชั่นล่าสุด (รวมถึงการบำรุงรักษา) ที่มีอยู่บนเว็บไซต์ทางการของคาร์ปาสกี้(www.thaikaspersky.com) ที่ติดตั้งบนเครื่องคอมพิวเตอร์ท่าน

3. สิทธิความเป็นเจ้าของ ซอฟต์แวร์นี้มีการปกป้องโดยทางกฎหมายสำเนาถูกต้อง ที่สงวนให้เฉพาะผู้จำหน่ายที่ถูกต้องของคาร์ปาสกี้ คาร์ปาสกีขอสงวนสิทธิ ในชื่อและทั้งหมดในซอฟต์แวร์ รวมทั้งสำเนาถูกต้อง สิทธิบัตร การค้าและทรัพย์สินทางปัญญาอื่นๆ ความเป็นเจ้าของ การติดตั้ง หรือกธใช้งานซอฟต์แวร์ที่ไม่ได้มีการโอนถ่ายทรัพย์สินทางปัญหาจากซอฟต์แวร์ไปยังท่าน และท่านไม่ได้มีสิทธิครอบครองในส่วนนี้ตามข้อตกลงนี้

4. การรักษาความลับ ท่านตกลงให้ซอฟต์แวร์และเอกสาร รวมทั้งการออกแบบโครงสร้างของโปรแกรมเฉพาะนั้นถือเป็นสมบัติของคาร์ปาสกี้แลป ท่านจะได้รับมาตรการการป้องกันอย่างสมเหตุสมผล เพื่อการปกป้องข้อมูลที่เป็นความลับ แต่ไม่มีข้อจำกัด

5. การจำกัดการรับประกัน

    (i) คาร์ปาสกี้มีการรับประกันการดาวน์โหลดใน 6 เดือนแรกของการดาวนโหลดหรือการติดตั้ง ซอฟต์แวร์ที่ซื้อมาจากสื่อกลาง ตามการทำงานที่อธิบายไว้ในเอกสารเมื่อมีการทำงานอย่างปกติ

    (ii) ท่านยอมรับในความรับผิดชอบในการเลือกซอฟต์แวร์ที่ท่านต้องการ คาร์ปากี้จะไม่รับประกันหากว่าเกิดจากการเลือกโปรแกรมที่ผิด ไม่เหมาะสมกับการใช้งาน

    (iii) คาร์ปาสกี้แลป จะไม่รับประกันเนื่องจากการรายงานผลไวรัสที่ไม่ถูกต้องหรือเกิดจากความเข้าใจผิดในส่วนที่ไม่ได้เกิดจากการติดเชื้อไวรัส

    (iv) การรักษาหรือความรับผิดชอบทั้งหมด ของคาร์ปาสกี้แลปสำหรับการทำผิดสัญญาในข้อ (i) จะเป็นตัวเลือกของคาร์ปาสกี้ในการซ่อม เปลี่ยน หรือคืนเงินค่าซอฟต์แวร์ หากการรายงานยังคาร์ปาสกี้แลปหรือผู้ได้รับการแต่งตั้งระหว่างระยะเวลาของการรับประกัน ท่านจะจัดหาข้อมูลทั้งหมดเท่าที่จำเป็นเพื่อช่วยในการแก้ปัญหา

(v) การรับประกันในข้อ (i) จะไม่เกิดขึ้นหากว่าท่าน a) ทำหรือเป็นสาเหตุของการเปลี่ยนแปลงซอฟต์แวร์ โดยปราศจากการยินยอมของคาร์ปาสกี้แลป b) ใช้ซอฟต์แวร์เพื่อการอื่นโดยไม่เจตนา c) ใช้ซอฟต์แวร์ในทางที่ไม่ได้อยู่ภายใต้ข้อตกลง

(vi) การรับประกันและเงื่อนไข ในข้อตกลงนี้ หรือเงื่อนไขอื่นใด ที่ทำให้เกิดความผิดพลาดในซอฟต์แวร์หรือเอกสารคู่มือ (vi) มีผลระหว่างคาร์ปาสกี้แลปและท่าน หรือหากว่าท่านไม่ให้ความร่วมมือในข้อตกลงนี้ หรือมีสัญญาใดที่ใกล้เคียงกันไม่ว่าจะเป็นกฎหมายอื่นใด (รวมทั้งการไม่มีข้อจำกัด เงื่อนไขเป็นนัย การรับประกันหรือเงื่อนไขอื่นใด ที่เป็นสิ่งที่เหมาะสมกับวัตถุประสงค์ที่ใช้หรือสมเหตุสมผลกับทักษะหรือการดูแล)

6. ข้อจำกัดของความรับผิดชอบ

(i) ไม่มีสิ่งใดในข้อตกลงนี้ ที่ทางคาร์ปาสกี้จะไม่รับผิดชอบสำหรับa)

(ii) ภายใต้หัวข้อข้างบนที่กล่าวมา คาร์ปาสกี้แลป จะไม่รับผิดชอบ (ไม่ว่าจะในสัญญา

(a) การสูญเสียรายได้

(b) การสูญเสียกำไรที่แท้จริง หรือกำไรที่ควรได้ (รวมทั้งกำไรตามสัญญา);

(c) สูญเสียการใช้เงิน

(d) การสูญเสียเงินสะสม

(e) สูญเสียทางธุรกิจ

(f) สูญเสียโอกาส

(g) สูญเสียมิตร

(h) สูญเสียชื่อเสียง

(i) ข้อมูลสูญเสีย เสียหายหรือถูกทำลายหรือ

(j) การสูญเสียที่เกิดขึ้นตามลำดับ หรือความเสียหายที่มาจากสาเหตุใดก็ตาม รวมทั้งเหตุการณ์อันหลีกเลี่ยงไม่ได้ในข้อ(ii), (a) ถึง (ii), (i)

(iii) ภายใต้ข้อความ (i) ข้างต้น ความรับผิดชอบของคาร์ปาสกี้แลป ขึ้นอยู่กับการเชื่อมต่อด้วยซอฟต์แวร์ที่อยู่ในสภาพแวดล้อมที่เหมาะสมและจำนวนที่เท่ากับที่ท่านจ่ายไป

7. ข้อตกลงนี้ประกอบไปด้วยความเข้าใจทั้งหมดระหว่าง ้ทั้งสองฝ่ายที่เกี่ยวข้องกันมาในทั้งหมดนี้ ความเข้าใจก่อนหน้านี้ที่เป็นลายลักษณ์อักษร หรือด้วยปากเปล่าระหว่างคุณและคาร์ปาสกี้แลป ซึ่งมาจากการตกลงกันระหว่างเราหรือตัวแทนของเราก่อนหน้าสัญญานี้ให้ถือเป็นโมฆะทั้งหมด และมีผลตามวันที่บังคับการมีผลนี้