

คู่มือการใช้งาน
คาร์ปาสก้ออินเทอร์เน็ตซีเคียวริตี้
2009

ถึง ผู้ใช้ คาร์ปาสกี อินเทอร์เน็ต ซีเคียวริตี้ 2009

ขอบพระคุณท่านที่เลือกใช้งานผลิตภัณฑ์ของเรา เราหวังว่า คู่มือการใช้งานนี้จะช่วยท่านในเรื่องของการใช้งาน รวมทั้งช่วยท่านในการตอบคำถามต่างๆเกี่ยวกับผลิตภัณฑ์

คำเตือน เอกสารฉบับนี้ ถือเป็นทรัพย์สินของคาร์ปาสกีแลป ลิขสิทธิ์ของเอกสารทั้งหมดนี้ถูกต้องตามกฎหมายของสหพันธรัฐรัสเซีย และภายใต้กฎหมายระหว่างประเทศ ไม่ให้มีการทำซ้ำ หรือทำเลียนแบบ คู่มือนี้ ในอันจะเป็นการผิดกฎหมายและจะต้องดำเนินคดีในศาลหากมีการกระทำนั้นเกิดขึ้น ซึ่งถือเป็นการกระทำทางอาชญากรรมตามกฎหมายแห่งสหพันธรัฐรัสเซีย การแปลเอกสารคู่มือนี้ออกไปเป็นภาษาอื่น จะต้องได้รับการอนุญาตจากทางคาร์ปาสกีแลปอย่างเป็นทางการเป็นลายลักษณ์อักษร เอกสารคู่มือ หรือรูปภาพนี้จะไม่นำไปใช้เพื่อการค้า และมีวัตถุประสงค์เพื่อการใช้งานส่วนบุคคลเท่านั้น

เอกสารคู่มือนี้อาจมีการกล่าวถึงรายละเอียดที่มีอยู่ก่อนหน้านี้โดยไม่จำเป็นต้องกล่าวล่วงหน้า สำหรับเวอร์ชันล่าสุดนี้ สามารถเข้าดูได้จากเว็บไซต์ <http://www.thaikaspersky.com> คาร์ปาสกีแลปไม่อนุญาตให้มีการนำส่วนหนึ่งส่วนใดของเอกสาร

เอกสารนี้ประกอบไปด้วย ทั้งส่วนที่ได้รับการลงทะเบียนและไม่ได้รับการลงทะเบียน ทะเบียนการค้าทั้งหมดเป็นสมบัติของเจ้าของ

© Kaspersky Lab, 1996-2008

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

<http://www.kaspersky.com/>

<http://support.kaspersky.com/>

ประเทศไทย <http://www.thaikaspersky.com>

วันที่ทำการปรับปรุง 29 เมษายน 2008

สารบัญ

เรื่อง	หน้า
บทนำ	
ข้อมูลเพิ่มเติมเกี่ยวกับการใช้งาน.....	8
แหล่งข้อมูลที่สามารถค้นหาได้ด้วยตนเอง.....	8
การติดต่อฝ่ายขาย.....	9
การติดต่อส่วนบริการทางเทคนิค.....	9
พูดคุยเรื่องการใช้งานกับคาร์ปาสกี้แลปบนเว็บแสดงความคิดเห็น.....	11
สิ่งเพิ่มเติมในคาร์ปาสกี้อินเทอร์เน็ต ซีเคียวริตี้ 2009.....	12
ภาพรวมการป้องกันในการใช้งาน.....	14
วิซาร์ดและเครื่องมือ.....	15
ตัวช่วยสนับสนุน.....	17
การวิเคราะห์พฤติกรรมของไวรัสแบบฮิวริสติก.....	18
ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ.....	20
ภัยคุกคามต่อความปลอดภัยของคอมพิวเตอร์.....	21
โปรแกรมภัยคุกคาม.....	21
โปรแกรมมุงร้าย.....	22
ไวรัสและหนอนอินเทอร์เน็ต.....	22

เรื่อง	หน้า
โทรจัน.....	22
โปรแกรมเนกประสงค์มั่งร้าย.....	32
โปรแกรมซึ่งอาจไม่พึงประสงค์.....	36
ซอฟต์แวร์โฆษณา.....	37
โปรแกรมเกี่ยวข้องกับเรื่องเพศ.....	37
โปรแกรมที่มีความเสี่ยงอื่นๆ.....	38
วิธีการป้องกันการติดโปรแกรมที่น่าสงสัยเป็นอันตรายโดยโปรแกรม.....	41
ภัยคุกคามทางอินเทอร์เน็ต.....	41
สแปมหรือเมลขยะ.....	41
ฟิชชิ่ง (Phishing).....	42
การจู่โจมของแฮกเกอร์.....	43
การแสดงแบนเนอร์.....	43
การติดตั้งโปรแกรม.....	45
ขั้นตอนที่1 ค้นหาโปรแกรมเวอร์ชันล่าสุด.....	46
ขั้นตอนที่2 ตรวจสอบความต้องการของระบบ.....	46

เรื่อง	หน้า
ขั้นตอนที่3 หน้าต่างการเริ่มต้นวิชาร์ด.....	46
ขั้นตอนที่4 ข้อตกลงทางด้านลิขสิทธิ์.....	47
ขั้นตอนที่5 เลือกประเภทของการติดตั้ง.....	47
ขั้นตอนที่6 เลือกโพลเดอ์การติดตั้ง.....	48
ขั้นตอนที่7 เลือกส่วนประกอบโปรแกรมเพื่อทำการติดตั้ง.....	49
ขั้นตอนที่8 ค้นหาซอฟต์แวร์แอนตี้ไวรัสตัวอื่น.....	50
ขั้นตอนที่9 ขั้นตอนสุดท้ายของการเตรียมการติดตั้ง.....	51
ขั้นตอนที่10 เสร็จสิ้นการติดตั้ง.....	52
ตัวประสานการใช้งานของผู้ใช้กับโปรแกรม.....	53
รูปสัญลักษณ์แสดงการแจ้งเตือน.....	53
เมนูค.....	54
หน้าต่างโปรแกรมหลัก.....	56
การแจ้งเตือน.....	59
หน้าต่างการตั้งค่าโปรแกรม.....	59

เรื่อง	หน้า
การเริ่มต้น.....	60
การเลือกประเภทเครือข่าย.....	61
การอัปเดตโปรแกรม.....	62
การวิเคราะห์ความปลอดภัย.....	63
การตรวจสอบไวรัสในเครื่องคอมพิวเตอร์.....	63
การมีส่วนร่วมในเครือข่ายความปลอดภัยคาร์ปาสกี.....	65
การจัดการความปลอดภัย.....	66
การหยุดปกป้องชั่วคราว.....	68
การตั้งค่าโปรแกรมให้สมบูรณ์.....	70
ทดสอบไวรัส EICAR และการปรับเปลี่ยน.....	70
การทดสอบการปกป้องข้อมูลผ่านทางHTTP.....	75
การทดสอบการปกป้องข้อมูลผ่านทางSMTP.....	75
การตั้งค่าไฟล์เอนดีไวรัสให้สมบูรณ์.....	76
การตั้งการตรวจสอบไวรัสให้สมบูรณ์.....	77
การตั้งการตรวจสอบแอนตี้สแปมให้สมบูรณ์.....	78

เรื่อง	หน้า
ถ้อยแถลงการสะสมข้อมูลทางเครือข่ายความปลอดภัยคาร์ปาสกี	
คาร์ปาสกีแลป.....	86
ผลิตภัณฑ์อื่นๆ ของคาร์ปาสกี.....	87
ติดต่อเรา.....	101

CRYPTOEX LLC

มูลนิธิ มอซิลลา

ข้อตกลงทางลิขสิทธิ์

บทนำ

ส่วนนี้ประกอบไปด้วย

ข้อมูลเพิ่มเติมเกี่ยวกับการใช้งาน

สิ่งเพิ่มเติมในคาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้ 2009

ภาพรวมการป้องกันในการใช้งาน

ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ

ข้อมูลเพิ่มเติมเกี่ยวกับการใช้งาน

หากท่านมีข้อสงสัยประการในเรื่องของการซื้อ การติดตั้ง หรือการใช้งานเรามีคำตอบในส่วนของปัญหาเหล่านั้นอยู่

คาร์ปาสกีแลป มีแหล่งข้อมูลมากมาย สะดวกแก่การค้นหาของท่าน ขึ้นอยู่กับความสำคัญและความเร่งด่วนในการใช้งานข้อมูลเหล่านั้น

แหล่งข้อมูลที่สามารถค้นหาได้ด้วยตนเอง

ท่านสามารถใช้ระบบการช่วยเหลือ [Help](#)

ระบบการช่วยเหลือประกอบไปด้วยข้อมูลในการจัดการการป้องกันคอมพิวเตอร์ การดูแลสุขภาพของการป้องกัน การตรวจจับในพื้นที่ต่างกันของคอมพิวเตอร์และแสดงการทำงานอื่นๆ

เปิดการช่วยเหลือ คลิก [Help](#) เพื่อไปยังหน้าต่างโปรแกรมหลัก หรือกดF1

การติดต่อฝ่ายขาย

หากว่าท่านมีคำถามในเรื่องของการเลือกหรือซื้อ โปรแกรม หรือการต่ออายุการใช้งาน สามารถติดต่อที่แผนกขาย

ท่านสามารถส่งคำถามมาที่แผนกขายได้ที่ sales@thaikaspersky.com

การติดต่อส่วนบริการทางเทคนิค

หากท่านได้ซื้อ โปรแกรมมาเป็นที่เรียบร้อยแล้ว ท่านสามารถได้รับการบริการข้อมูลจากฝ่ายบริการทางเทคนิคได้ทั้งทางโทรศัพท์หรือทางอินเทอร์เน็ต

เจ้าหน้าที่บริการทางด้านเทคนิค จะตอบคำถามของท่านในเรื่องของการติดตั้งและการใช้งานโปรแกรม หากว่าเครื่องคอมพิวเตอร์ของท่านมีการติดสิ่งไม่พึงประสงค์ เราจะช่วยท่านในการกำจัดตามลำดับของมัลแวร์

การร้องขอความช่วยเหลือทางอีเมลล์ต่อส่วนบริการทางด้านเทคนิค (สำหรับผู้ใช้งานที่ทำการลงทะเบียนแล้วเท่านั้น)

ท่านสามารถส่งคำถามของท่านไปยังผู้เชี่ยวชาญทางด้านเทคนิค โดยการเข้าไปยังแบบฟอร์มช่วยเหลือหน้าเว็บ

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

ท่านสามารถเขียนคำถามของท่านได้ทั้งภาษาไทยและภาษาอังกฤษ

ในการส่งข้อความคำถามทางอีเมล 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> และส่งไปยังอีเมลของท่านตามคำขอ

ในการกรอกคำถามบนหน้าเว็บ ท่านควรอธิบายรายละเอียดต่างๆให้มากที่สุดเท่าที่เป็นไปได้ โดยเฉพาะข้อมูลสำคัญดังต่อไปนี้

- ประเภทของคำถามที่กำหนดไว้ คำถามจากผู้ใช้ส่วนมากที่พบบ่อย จะนำมารวมเป็นกลุ่มหัวข้อพิเศษเดียวกัน ตัวอย่างเช่น “การติดตั้งผลิตภัณฑ์ ปัญหาในการถอนโปรแกรม” หรือ “การสแกนไวรัส/ ปัญหาในการถอนโปรแกรม” หากว่าไม่มีหัวข้อที่เหมาะสมกับคำถามของท่าน ให้เลือกหัวข้อ “คำถามทั่วไป”
- ชื่อโปรแกรมและเวอร์ชันที่ใช้งาน
- เนื้อหาที่กำหนดไว้อธิบายปัญหาของท่านให้มากที่สุดเท่าที่จะมากได้

- หมายเลขลูกค้า และรหัสผ่าน กรอกหมายเลขลูกค้าและรหัสผ่านซึ่งท่านจะได้รับเมื่อทำการลงทะเบียนผ่านหน้าเว็บไซต์บริการทางด้านเทคนิค
- ที่อยู่อีเมลล์ ฝ่ายสนับสนุนทางด้านเทคนิคจะส่งคำตอบไปยังอีเมลล์นี้

การสนับสนุนทางเทคนิคทางโทรศัพท์

หากว่าท่านมีปัญหาที่ต้องการความช่วยเหลืออย่างเร่งด่วน ท่านสามารถโทรศัพท์เข้ามาแจ้งความต้องการ ได้กับสำนักงานที่ใกล้ที่สุด ท่านสามารถรายละเอียดได้จาก <http://support.kaspersky.com/support/details> สมัครใช้งานของรัสเซียที่ <http://www.thaikaspersky.com/kaspersky-thai/service.htm> หรือผู้ใช้งานประเทศไทย <http://support.kaspersky.com/support/international>

ส่วนการสนับสนุนทางเทคนิค จะช่วยเหลือท่านตามคำร้องขออย่างรวดเร็วที่สุดเท่าที่เป็นไปได้

พูดคุยเรื่องการใช้งานกับคาร์ปาสกีแลปบนเว็บแสดงความคิดเห็น

หากว่าคำถามของท่าน ไม่ได้เป็นเรื่องเร่งด่วน ท่านสามารถพูดคุยเรื่องราวที่ท่านต้องการทราบกับผู้เชี่ยวชาญของคาร์ปาสกีแลป รวมทั้งผู้ใช้งานคาร์ปาสกีท่านอื่นๆ ได้บนเว็บแสดงความคิดเห็นที่ <http://forum.kaspersky.com/>

ในการแสดงความคิดเห็น ท่านสามารถอ่านหัวข้อที่มีอยู่ ตอบคำถาม สร้างหัวข้อและการใช้งานค้นคว้า

สิ่งเพิ่มเติมในคาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้ 2009

คาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้ 2009 เป็นสิ่งใหม่ทั้งหมดของการป้องกันทางข้อมูล การทำงานหลักของโปรแกรมนั้นเข้มงวดต่อการเข้าถึงทรัพยากรของระบบ ช่วยในการป้องกันการกระทำอันไม่พึงประสงค์โดยโปรแกรมที่น่าสงสัย หรือเป็นอันตราย ความสามารถของโปรแกรมจะทำการปกป้องข้อมูลที่เป็นความลับของผู้ใช้ โดยเพิ่มพูนความสามารถจากเพิ่มมากมาย โปรแกรมนี้ประกอบไปด้วยเครื่องมือ และ วิชาาร์ดเพื่อให้การปกป้องคอมพิวเตอร์เป็นเรื่องง่ายมากขึ้น

คุณลักษณะใหม่ในคาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้ 2009

คุณลักษณะของการปกป้องแบบใหม่

- คาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้ มีส่วนประกอบของตัวกรองใหม่ที่ทำกรป้องกันก่อนการเกิดปัญหา และไฟร์วอลล์ที่ทำงานร่วมกันในการป้องกันระบบทั้งหมดเพื่อด้านทานภัยคุกคาม รวมทั้งภัยคุกคามที่มีอยู่ ทั้งที่รู้จักและไม่รู้จักคาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้สามารถให้ผู้ใช้กำหนดรายการที่น่าเชื่อถือ พิจารณาใส่รายการที่ต้องการได้ (Whitelisting)
- การตรวจสอบระบบการปฏิบัติการและซอฟต์แวร์ที่ได้รับการติดตั้ง เพื่อตรวจจับและกำจัดช่องโหว่หรือจุดอ่อน รักษาระดับของความปลอดภัยในระดับสูง และป้องกันโปรแกรมที่เป็นอันตรายต่อระบบของท่าน
- วิชาาร์ดแบบใหม่ ตัววิเคราะห์ความปลอดภัยและการตั้งค่าบราวเซอร์ที่ง่ายต่อการตรวจจับ และกำจัดภัยคุกคามที่เข้ามาคุกคามความปลอดภัย และจุดอ่อนในโปรแกรมที่ติดตั้ง รวมทั้งการกำหนดค่าของระบบปฏิบัติการและการใช้งาน ระบบปฏิบัติการและการตั้งค่าบราวเซอร์
- คาร์ปาสกีแลปตอบสนองต่อภัยคุกคามใหม่ๆ ที่เกิดขึ้นอย่างรวดเร็ว ผ่านเครือข่ายความปลอดภัย คาร์ปาสกี ที่ทำงานร่วมกันในการรับข้อมูลภัยคุกคามจากเครื่องคอมพิวเตอร์ของผู้ใช้ และส่งต่อไปยังเซิร์ฟเวอร์ของคาร์ปาสกีแลป
- เครื่องมือใหม่ การเฝ้าดูเครือข่าย และการวิเคราะห์แพ็กเก็ตเครือข่าย ให้ความสะดวกสบายในการรวบรวมและวิเคราะห์ข้อมูลเกี่ยวกับกิจกรรมทางเครือข่ายบนเครื่องคอมพิวเตอร์ท่าน

- วิชาร์ดใหม่ การกู้ระบบแบบใหม่ ช่วยในการซ่อมแซมความเสียหายที่เกิดขึ้นต่อระบบของท่านเมื่อมีผู้เข้ามาทำลายระบบ

คุณลักษณะการป้องกันทางด้านข้อมูลความลับใหม่

- การกรองโปรแกรมอันเป็นส่วนประกอบใหม่ที่มีประสิทธิภาพในการเข้าถึงข้อมูลความลับ ไฟล์ และโฟลเดอร์ของผู้ใช้โดยโปรแกรม
- ความปลอดภัยของข้อมูลความลับที่เข้าถึงโดยเป็นพิมพ์ เพื่อความมั่นใจในเครื่องมือใหม่ที่เรียกว่าเป็นพิมพ์เสมือน
- คาร์ปาสก์อินเทอร์เน็ต ซีเคียวริตี้ประกอบไปด้วย วิชาร์ดตัวทำความสะอาดความเป็นส่วนตัว ซึ่งลบข้อมูลทั้งหมดเกี่ยวกับการกระทำที่แสดง และเป็นที่สนใจของผู้บุกรุก(รายการของเว็บไซต์ที่เข้าชม ไฟล์ที่ทำการเปิด คຸ້กกี และอื่นๆ) จากคอมพิวเตอร์ของผู้ใช้

คุณลักษณะของแอนตี้สแปมใหม่

- ประสิทธิภาพของตัวกรองแอนตี้สแปม โดยส่วนประกอบแอนตี้สแปม ที่เพิ่มการใช้เทคโนโลยี Recent Term Server.
- การใช้งานของ Microsoft Outlook, Microsoft Outlook Express, Bat! และ Thunderbird extension ที่รวมเข้าไว้ในการตั้งค่าแอนตี้สแปม
- การเพิ่มส่วนของการควบคุมโดยผู้ปกครองให้มีความเข้มงวด และมีประสิทธิภาพในการควบคุมการใช้งานอินเทอร์เน็ตสำหรับเด็ก

คุณลักษณะการปกป้องแบบใหม่สำหรับผู้ใช้งานอินเทอร์เน็ต

- ปรับปรุงส่วนของการปกป้องจากผู้บุกรุกทางอินเทอร์เน็ต รวมทั้งฐานข้อมูลของโปรแกรมในส่วนของเว็บไซต์ปลอมต่างๆ
- ความปลอดภัยในการใช้งานการส่งข้อความแบบทันที ด้วยเครื่องมือที่ทำการตรวจสอบการใช้งานโปรแกรม MSN และ ICQ
- ความปลอดภัยต่อการใช้งานเครือข่ายไร้สายที่สามารถตรวจสอบผ่านทาง การเชื่อมต่อแบบไร้สาย

คุณลักษณะตัวประสานการใช้งานของผู้ใช้งานกับโปรแกรมแบบใหม่

- ตัวประสานการใช้งานแบบใหม่นี้ ครอบคลุมการปกป้องข้อมูลมากขึ้น
- กล่องข้อความที่มีความสามารถสูง ช่วยให้ผู้ใช้ทำการตัดสินใจได้รวดเร็วขึ้น
- ขยายความสามารถในการทำงาน สำหรับการบันทึกสถิติ และการทำรายงาน สามารถเลือกตัวกรองจากรายงาน และเครื่องมือค้นหาทางพลังที่มีความยืดหยุ่นมากขึ้น

ภาพรวมการป้องกันในการใช้งาน

คาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้ปกป้องเครื่องคอมพิวเตอร์ของท่านจากภัยคุกคามทั้งที่รู้จักและไม่รู้จัก รวมไปถึงข้อมูลอันไม่พึงประสงค์ ภัยคุกคามแต่ละประเภทที่แยกตามองค์ประกอบของโปรแกรม การติดตั้งที่มีความยืดหยุ่น ด้วยตัวเลือกการกำหนดค่าการใช้งานที่ง่ายดาย ตามความต้องการของผู้ใช้

คาร์ปาสกีอินเทอร์เน็ต ซีเคียวริตี้ประกอบไปด้วยคุณลักษณะด้านการป้องกันดังต่อไปนี้

- ระบบการเฝ้าระวังพฤติกรรมการใช้งานโปรแกรมของผู้ใช้ การป้องกันการกระทำที่เป็นอันตรายใดๆ
- การปกป้องแบบเรียลไทม์ของการรับส่งข้อมูลทั้งหมด ที่ผ่านเข้าออกเครื่องคอมพิวเตอร์ของท่าน
- ความปลอดภัยออนไลน์ ที่ให้การป้องกันการจู่โจมแบบฟิชซิง

- การมอบหมายงานตรวจสอบไวรัส เพื่อการตรวจสอบไฟล์ส่วนบุคคล ไดรฟ์ พื้นที่เฉพาะ หรือ ตรวจสอบไวรัสในทุกส่วนของคอมพิวเตอร์ งานในการตรวจสอบจะมีการกำหนดค่าเพื่อให้ตรวจจับช่องโหว่ หรือจุดอ่อน ที่อยู่ในโปรแกรมที่ผู้ใช้ติดตั้ง
- การอัปเดตเพื่อให้โปรแกรมอยู่ในสถานะทันต่อเหตุการณ์ที่เกิดขึ้นใหม่อยู่เสมอ ทั้งโมดูลของโปรแกรมและฐานข้อมูลที่ใช้ในการตรวจจับ โปรแกรมอื่นไม่พึงประสงค์ การจำเริญของแฮกเกอร์ และข้อความสแปม
- วิชารค์และเครื่องมือสะดวกต่อการจัดการงานตรวจสอบที่เกิดขึ้นในระหว่างการทำงานของคาร์ปาสก็แอนตี้ไวรัส
- คุณลักษณะที่สนับสนุนการทำงาน โดยมีข้อมูลและตัวช่วยที่ทำงานกับโปรแกรมเพื่อเพิ่มประสิทธิภาพการทำงาน

วิชารค์และเครื่องมือ

การทำให้เกิดความมั่นใจในความปลอดภัยของเครื่องคอมพิวเตอร์ เป็นการทำงานที่ซับซ้อนต้องอาศัยความรู้ของคุณลักษณะในระบบปฏิบัติการ และวิธีการเข้าอาชนะจุดอ่อนของมัน นอกจากนี้ ปริมาณและความหนาแน่นของข้อมูลเกี่ยวกับความปลอดภัยของระบบ ทำให้การวิเคราะห์และการดำเนินการยากขึ้น

เพื่อช่วยในการแก้ไขปัญหาการทำงานแบบเฉพาะในการทำให้เกิดความปลอดภัยต่อคอมพิวเตอร์ คาร์ปาสก็แอนตี้ไวรัสเน็ต ซีเคียวริตี้จึงมีวิชารค์และเครื่องมือดังต่อไปนี้

- วิชารค์วิเคราะห์ความปลอดภัย ใช้ในการวินิจฉัยข้อบกพร่องของเครื่องคอมพิวเตอร์หรือ ส่วนประกอบใด ๆ ของเครื่องเพื่อค้นหาช่องโหว่ หรือจุดอ่อนของโปรแกรมที่ผู้ใช้งานติดตั้ง
- วิชารค์การตั้งค่าใช้งานต่างๆ วิเคราะห์การตั้งค่าโปรแกรมที่ช่วยค้นหาไมโครซอฟต์อินเทอร์เน็ต เอ็กซ์พลอเรอร์ ประเมินเบื้องต้นจากด้านความปลอดภัย
- วิชารค์การกู้คืนระบบ กำจัดการจำเริญของโปรแกรมอื่นไม่พึงประสงค์ออกจากระบบ

- วิชารัตต์ตัว ทำความสะอาดความเป็นส่วนตัว ซึ่งลบข้อมูลทั้งหมดเกี่ยวกับการกระทำที่แสดง และเป็น ที่สนใจของผู้บุกรุก จากคอมพิวเตอร์ของผู้ใช้ อนุญาตให้ถึงการกระทำของผู้ใช้
- วิชารัตการกู้คืนหน่วยบันทึก มีประโยชน์ต่อระบบหลังจากระบบถูกโจมตีให้เกิดความเสียหายต่อ ไฟล์ของระบบปฏิบัติการ เพื่อไม่ให้เครื่องคอมพิวเตอร์ตั้งต้นใหม่อีกครั้ง
- การวิเคราะห์แพ็กเก็ตเครือข่ายที่แทรกแซงเข้ามาในแพ็กเก็ตของเครือข่าย และแสดงผลรายละเอียด
- การเฝ้าดูเครือข่ายที่แสดงรายละเอียดเกี่ยวกับกิจกรรมของเครือข่ายบนเครื่องคอมพิวเตอร์ของท่าน
- แป้นพิมพ์เสมือนที่ให้การปกป้องการแทรกแซงข้อมูลที่เข้ามาจากแป้นพิมพ์

ตัวช่วยสนับสนุน

โปรแกรมรวมคุณลักษณะการสนับสนุน ที่ทำให้โปรแกรมมีความทันสมัยอยู่เสมอ เพื่อเพิ่มความสามารถในการทำงานของโปรแกรม และช่วยในการใช้งานของท่าน

เครือข่ายความปลอดภัยของคาร์ปาสกี

เครือข่ายความปลอดภัยของคาร์ปาสกี คือ ระบบการโอนถ่ายข้อมูลอย่างอัตโนมัติในการตรวจจับภัยคุกคามที่เกิดขึ้นแล้วส่งไปยังฐานข้อมูลส่วนกลางของคาร์ปาสกีแลป ฐานข้อมูลนี้ทำให้คาร์ปาสกี มีความรวดเร็วต่อภัยคุกคามที่แพร่ขยายอย่างรวดเร็ว และแจ้งกลับผู้ใส่ในทันที

ลิขสิทธิ์

เมื่อท่านซื้อคาร์ปาสกีแอนตี้ไวรัส แล้วได้เข้าสู่ข้อตกลงทางลิขสิทธิ์ ซึ่งควบคุมการใช้งานของโปรแกรม การเข้าถึงการอัปเดตฐานข้อมูลโปรแกรม และการสนับสนุนทางด้านเทคนิคนั้นเป็นไปตามอายุของลิขสิทธิ์ การใช้งานเต็มประสิทธิภาพการทำงานตามลิขสิทธิ์

ในส่วนของ “ลิขสิทธิ์” สามารถบอกในส่วนที่เกี่ยวข้องกับลิขสิทธิ์ปัจจุบันของท่าน การซื้อ และการต่ออายุ

การสนับสนุน

ผู้ใช้งานคาร์ปาสกีแอนตี้ไวรัสที่ลงทะเบียนแล้วทั้งหมด สามารถรับประโยชน์ในการบริการสนับสนุนทางด้านเทคนิค โดยดูข้อมูลเกี่ยวกับวิธีการรับความช่วยเหลือทางด้านเทคนิคในส่วน “Support”

เมื่อไปถึงที่ส่วนสนับสนุน จะพบว่ามีส่วนแสดงความคิดเห็นของผู้ใช้คาร์ปาสกี เพื่อส่งรายงานข้อผิดพลาดไปยังส่วนสนับสนุนทางเทคนิค เรามีความยินดีในการบริการท่านผ่านทางโทรศัพท์ในเรื่องเกี่ยวกับโปรแกรม

การวิเคราะห์พฤติกรรมของไวรัสแบบฮิวริสติก

พฤติกรรมของไวรัสแบบฮิวริสติก ใช้ในส่วนของ การปกป้องแบบเรียลไทม์ เช่น การป้องกันไฟล์จากไวรัส การป้องกันเมลล์จากไวรัส การป้องกันเว็บจากไวรัส และในการตรวจสอบไวรัส

การตรวจสอบวัตถุโดยการใช่ลายเซ็นต์ ซึ่งใช้ฐานข้อมูลที่ใช้คำอธิบายครอบคลุมกับขบวนการทั้งหมดที่ระบุไว้เพื่อการตรวจสอบโปรแกรมที่ไม่พึงประสงค์ และอันตราย เป็นโปรแกรมวิเคราะห์รหัสของวัตถุ และเป็นวิธีการตัดสินใจว่าเป็นอันตรายหรือไม่ทางอ้อม ที่สามารถตรวจจับได้ทั้งไวรัสที่รู้จักและไม่รู้จัก ซึ่งไม่เหมือนกับวิธีการแบบลายเซ็นต์

ประโยชน์ของการวิเคราะห์แบบฮิวริสติก นั้นเพื่อการตรวจจับโปรแกรมอันไม่พึงประสงค์ ที่ไม่ได้มีการลงทะเบียนไว้ในฐานข้อมูล เพราะภัยคุกคามและการจู่โจมมีการสร้างขึ้นใหม่ทุกวัน อันเป็นการตรวจจับก่อนการวิเคราะห์ไวรัส

อย่างไรก็ตาม วิธีการฮิวริสติก อาจทำให้การทำงานของระบบหยุดชะงักลงเนื่องเพราะการตรวจจับพบว่ามึรหัสไม่พึงประสงค์ที่ได้จากการตรวจสอบแบบฮิวริสติก

หมายเหตุ

การใช้งานร่วมกันของวิธีการในการตรวจสอบจะทำให้มีความปลอดภัยมากกว่า

เมื่อมีการตรวจสอบวัตถุ การวิเคราะห์แบบฮิวริสติก จะเหนือกว่าในด้านความปลอดภัยในการตรวจจับวัตถุโดยโปรแกรมในสภาพแวดล้อมเสมือน หากว่าการกระทำที่น่าสงสัยที่ค้นเหมือนเป็นวัตถุดำเนินการ ทำให้วัตถุนั้นได้รับการปฏิเสธในการฝังลงเครื่องแม่ และจะมีข้อความเตือนแนะนำผู้ใช้ในการดำเนินการต่อไป

- การแยกวัตถุ ทำการตรวจสอบภัยคุกคามตัวใหม่และดำเนินการในการอัปเดตฐานข้อมูล
- ลบวัตถุ
- ข้ามไป (หากท่านมั่นใจว่าวัตถุนั้นไม่ใช่สิ่งไม่พึงประสงค์)

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

คำเตือน!

การสกัดค้นภัยคุกคามใหม่ๆ โดยการใช้การวิเคราะห์แบบฮิวริสติกของคาร์ปาสกีแลป และวิธีการในการกำจัดนั้นมีการอัปเดตฐานข้อมูลในทุกชั่วโมง

ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ

เพื่อให้การทำงานของซอฟต์แวร์เต็มประสิทธิภาพ คอมพิวเตอร์จะต้องมีความต้องการระบบอย่างน้อยดังต่อไปนี้

- พื้นที่ว่างของฮาร์ดดิสก์ 75 MB
- CD-ROM (สำหรับการติดตั้งโปรแกรมโดยใช้ CD)
- เม้าส์
- IE 5.5 ขึ้นไป (สำหรับการอัปเดตฐานข้อมูลของโปรแกรม 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 สปายแวร์ ฟิชชิ่ง การโจรกรรมของ แสกเกอร์ ซอฟต์แวร์โฆษณาและแบนเนอร์ ซึ่งตัวการหลักของภัยคุกคามเหล่านี้มาจากอินเทอร์เน็ต

เนื้อหาในส่วนนี้ประกอบไปด้วย

โปรแกรมภัยคุกคาม

ภัยคุกคามทางอินเทอร์เน็ต

โปรแกรมภัยคุกคาม

โปรแกรมของคาร์ปาสกีแลป สามารถสกัดกั้นโปรแกรมอันไม่พึงประสงค์กว่าพันโปรแกรม ที่เข้ามาแฝงอยู่ในเครื่องคอมพิวเตอร์ของท่าน บางส่วนของโปรแกรมเหล่านี้ทำการคุกคามการทำงานของเครื่องคอมพิวเตอร์ท่าน และตัวอื่นๆที่จัดว่าอันตราย หลังจากที่โปรแกรมทำการสืบค้นโปรแกรมอันไม่พึงประสงค์ และจัดแยกหมวดหมู่ให้อยู่ในระดับอันตราย(สูง หรือกลาง)

การวิเคราะห์ไวรัสของคาร์ปาสกีแลป จำแนกความแตกต่างออกเป็นสองหมวดหมู่หลักของโปรแกรมภัยคุกคาม คือ โปรแกรมแอบแฝงมุ่งร้าย และโปรแกรมอันไม่พึงประสงค์

โปรแกรมแอบแฝงมุ่งร้าย (Malware) สร้างความเสียหายให้แก่คอมพิวเตอร์ของผู้ใช้ เช่น การขโมยข้อมูล การสกัดกั้น เปลี่ยนแปลงหรือลบข้อมูล รวมทั้งการขัดขวางการทำงานของระบบปฏิบัติการของเครื่องคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

โปรแกรมที่ไม่พึงประสงค์ (PUPs) แตกต่างจากโปรแกรมแอบแฝงมั่งร้าย ที่ไม่ได้เข้าไปทำลายแต่จะเข้าไปแทรกซึมอยู่ในระบบปฏิบัติการของคอมพิวเตอร์

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

โปรแกรมมั่งร้าย

โปรแกรมมั่งร้าย (Malware) เป็นการสร้างตัวเองขึ้นมาเฉพาะเพื่อทำให้เกิดความเสียหายแก่เครื่องคอมพิวเตอร์และผู้ใช้งานเครื่องคอมพิวเตอร์ อันได้แก่ การขโมย การสกัดกั้น เปลี่ยนแปลงหรือลบข้อมูล รวมทั้งการขัดขวางการทำงานของระบบปฏิบัติการของเครื่องคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

โปรแกรมมั่งร้ายแบ่งออกได้เป็น 3 ประเภท คือ ไวรัสและหนอนอินเทอร์เน็ต โทรจัน และโปรแกรมอเนกประสงค์มั่งร้าย

ไวรัสและหนอนอินเทอร์เน็ต สามารถสร้างสำเนาของตัวเอง แพร่กระจายและขยายออกไปซ้ำแล้วซ้ำอีก ทำกระบวนการโดยที่ผู้ใช้งานไม่ทราบการกระทำดังกล่าว หรือดำเนินการที่ผู้ใช้งานมองเห็นการกระทำ โปรแกรมเหล่านี้จะแสดงอาการมั่งร้ายเมื่อตัวมันดำเนินการ

โปรแกรมโทรจัน (Trojan) จะไม่มีการสร้างสำเนาซึ่งไม่เหมือนกับไวรัส หรือหนอนอินเทอร์เน็ต โทรจันมีผลต่อคอมพิวเตอร์ อย่างเช่นจากการที่ผู้ใช้งานส่งอีเมลล์ หรือการเข้าเว็บไซต์เมื่อเข้าไปยังเว็บไซต์ที่มีเชื้ออยู่ โปรแกรมจะแสดงอาการมั่งร้ายเมื่อมีการใช้งาน

โปรแกรมอเนกประสงค์มุ่งร้าย (Malicious tools) สร้างขึ้นเพื่อให้มีผลต่อคอมพิวเตอร์ ทำลายคอมพิวเตอร์ อย่างไรก็ตาม มีความแตกต่างจากโปรแกรมมุ่งร้ายอื่นๆ ที่ไม่ได้มีพฤติกรรมในการมุ่งร้ายเมื่อมีการดำเนินการ โปรแกรม และยังคงมีความปลอดภัยเมื่ออยู่บนเครื่องคอมพิวเตอร์ของผู้ใช้ การกระทำที่แฮกเกอร์ใช้เพื่อการสร้างไวรัส หนอนอินเทอร์เน็ตและโทรจัน จัดการจู่โจมเครือข่ายโดยการรีโมตเซิร์ฟเวอร์ ดัดแปลงแก้ไขโปรแกรมการกระทำมุ่งร้ายอื่นๆ

ไวรัส (Virus)

หมวดหมู่ย่อย: ไวรัสและหนอนอินเทอร์เน็ต

ระดับความรุนแรง: สูง

ไวรัสแบบดั้งเดิม และหนอนอินเทอร์เน็ตที่มีการดำเนินการบนเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตบนเครื่องคอมพิวเตอร์ที่ติดตั้งสามารถสำเนาตัวเอง และแพร่กระจายทั่วคอมพิวเตอร์

ไวรัสแบบดั้งเดิม

หลังจากไวรัสเข้าแทรกซึมไปยังระบบ จะทำการติดฝังไปยังไฟล์ กระตุ้นตัวเอง และแสดงพฤติกรรมมุ่งร้าย รวมทั้งเพิ่มสำเนาตัวเองไปยังไฟล์อื่น

ไวรัสแบบดั้งเดิม ทำสำเนาแค่เพียงทรัพยากรภายในของเครื่องพีซีที่ติดเชื่อ แต่ไม่สามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่น การแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ เกิดขึ้นได้หากว่าไวรัสทำการเพิ่มตัวเองลงไปยังไฟล์แล้วไฟล์นั้นเก็บไว้ยังโพลเดอร์ที่มีการใช้งานร่วมกัน หรือการส่งไฟล์ที่แนบไวรัสไปทางอีเมล

รหัสของไวรัสแบบดั้งเดิม ออกมาเพื่อการแทรกซึมยังส่วนเฉพาะของเครื่องคอมพิวเตอร์ ระบบปฏิบัติการหรือโปรแกรม ขึ้นอยู่กับสิ่งแวดล้อม ระยะทางระหว่างไฟล์ บูท สคริปต์และไวรัสสมภาค

ไวรัสสามารถติดไปกับไฟล์โดยวิธีต่างๆมากมาย การเขียนทับไวรัสที่เขียนโดยรหัสของตัวมันเอง แทนที่รหัสของไฟล์ที่มีการติดไวรัส เข้าทำลายเนื้อหาเดิมของไฟล์ ไฟล์ที่ติดไวรัสจะหยุดการทำงานและไม่สามารถกำจัดได้ ไวรัสปรสิตที่เป็นตัวทำลายจะทำการเปลี่ยนแปลงไฟล์ระบบการทำงานบางส่วนหรือเต็มส่วน ไวรัสร่วมมือจะไม่ทำการเปลี่ยนแปลงไฟล์ แต่จะทำการสำเนา และเมื่อมีการเปิดไฟล์ที่ติดไวรัส ก็จะ

ดำเนินการไวรัสที่ทำสำเนา ประเภทอื่นๆของไวรัสเช่น ไวรัสลิงค์ ไวรัสOBJ ที่แปลว่า โมดูลวัตถุติดเชื่อ ไวรัส VIB ที่แปลว่า ห้องสมุดรวบรวมการติดไวรัส และไวรัสที่เป็นเนื้อหาต้นฉบับที่ติดไวรัสของโปรแกรม

หนอนอินเทอร์เน็ต (Worm)

หลังจากที่มีการเข้าสู่ระบบ หนอนอินเทอร์เน็ต จะมีความคล้ายคลึงกับไวรัส ที่กระตุ้นตัวเองและกระทำการมั่วร้าย หนอนอินเทอร์เน็ตสามารถไปตามช่องทางจากเครื่องหนึ่งสู่อีกเครื่องหนึ่ง แพร่พันธุ์ตัวเองและกระจายไปยังช่องทางข้อมูลต่างๆ

การจัดหมวดหมู่ของหนอนอินเทอร์เน็ต โดยการเพิ่มจำนวนอย่างรวดเร็ว ดังรายการแสดงตารางข้างล่างนี้

ตารางที่ 1 หมวดหมู่ของหนอนอินเทอร์เน็ตแบ่งตามการเพิ่มจำนวน

ประเภท	ชื่อ	คำอธิบาย
หนอนอีเมล	หนอนอีเมล (E-mail worms)	หนอนอีเมล เป็นหนอนที่มาจากการรับส่งอีเมล ข้อความที่มีการติดเชื่อ จะมาจากการแนบไฟล์ รวมทั้งมีการสำเนาหนอนอินเทอร์เน็ต หรือการลิงค์ไปให้อัพโหลดข้อมูลที่มีหนอนอินเทอร์เน็ต เว็บไซต์เหล่านั้นมีการปรับเปลี่ยนหรือเป็นของแฮกเกอร์ เมื่อมีการเปิดไฟล์ที่แนบไป หนอนอินเทอร์เน็ตก็จะเป็นการกระตุ้นหนอนอินเทอร์เน็ต หรืออีกวิธีหนึ่งคือเมื่อคลิกที่ลิงค์ ดาวน์โหลดและเปิดไฟล์ หลังจากนั้นก็จะทำการแพร่ตัวเองโดยการหาอีเมลของคนอื่นและส่งข้อความที่ติดเชื่อนี้ ออกไปอีก

<p>หนอนที่มากับระบบการส่งข้อความทันที</p>	<p>IM Worms</p>	<p>หนอนจะทำการแพร่ไปยังระบบการส่งข้อความทันที(Instant messaging) เช่น ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager and Skype</p> <p>หนอนเหล่านี้จะทำการติดต่อกับรายชื่อผู้ติดต่อที่อยู่รายการชื่อและทำการส่งไฟล์และลิงค์ที่มีการติดเชื่อ เมื่อผู้ใช้ทำการดาวน์โหลดไฟล์และเปิดไฟล์ หนอนก็จะทำงาน</p>
<p>หนอนที่มากับโปรแกรม IRC</p>	<p>IRC Worms</p>	<p>หนอนอินเทอร์เน็ตประเภทนี้จะทำการแพร่เข้าสู่เครื่องคอมพิวเตอร์ของท่านโดยผ่านทางโปรแกรมสนทนา IRC ซึ่งอาศัยช่องทางการสื่อสารแบบเรียลไทม์บนอินเทอร์เน็ต</p> <p>หนอนอินเทอร์เน็ตนี้อยู่บนช่องทางการสนทนาบนอินเทอร์เน็ต ทั้งการทำสำเนาไฟล์หรือการลิงค์ไปยังเว็บอื่น เมื่อผู้ใช้ทำการดาวน์โหลดไฟล์และเปิดไฟล์ หนอนก็จะทำงาน</p>
<p>หนอนที่มากับเครือข่าย</p>	<p>Net Worms</p>	<p>หนอนชนิดนี้ ทำการกระจายผ่านเครือข่ายของคอมพิวเตอร์</p> <p>หนอนประเภทนี้มีความแตกต่างจากหนอนอินเทอร์เน็ต หนอนเครือข่ายมีการแพร่พันธุ์โดยไม่จำเป็นต้องการมีส่วนร่วมของผู้ใช้ หนอนจะทำกษค้นหาเครือข่ายภายในสำหรับคอมพิวเตอร์ซึ่งมีช่องโหว่และอ่อนแอ และทำการกระจายออกไปยังเครือข่าย ด้วยรหัสหรือส่วนของรหัสไปยังแต่ละเครื่องคอมพิวเตอร์ หากเครื่องคอมพิวเตอร์มีความเสี่ยงในเครือข่ายก็จะทำการแทรกซึมโดยการส่งแพ็กเก็ต และเมื่อมีหนอนอยู่เต็มระบบหนอนก็จะปฏิบัติงาน</p>

		ทันที
หนอนที่มากับ โปรแกรม P2P	File exchange Worms	<p>หนอนจากการแลกเปลี่ยนไฟล์ (File exchange worms) แพร่พันธุ์ผ่านทางเครือข่ายแบบ Peer to Peer เช่น Kazaa, Grokster, EDonkey, FastTrack หรือ Gnutella</p> <p>ในการใช้งานเครือข่ายเพื่อการแลกเปลี่ยนไฟล์ หนอนจะทำการสำเนาตัวเองเข้าสู่โพลเดอร์ของไฟล์ที่ทำการแลกเปลี่ยน ซึ่งจะตั้งอยู่บนเครื่องคอมพิวเตอร์</p> <p>หนอนอินเทอร์เน็ตที่มีความซับซ้อนมากกว่าทำการเลียนแบบเน็ตเวิร์กโปรโตคอลของเน็ตเวิร์กที่มีการแลกเปลี่ยนไฟล์ และเสนอการสำเนาตัวเองเข้าไปแทนที่ไฟล์ที่ทำการแลกเปลี่ยนเพื่อให้ดาวน์โหลด</p>
หนอนอินเทอร์เน็ต	หนอนอินเทอร์เน็ตอื่นๆ	<p>หนอนอินเทอร์เน็ตอื่นๆ ประกอบไปด้วย</p> <ul style="list-style-type: none"> • หนอนที่แพร่กระจายโดยการสำเนาตัวเองผ่านทางทรัพยากรเครือข่าย ใช้ความสามารถในการทำหน้าที่ของระบบปฏิบัติการ เข้าไปสู่โพลเดอร์เน็ตเวิร์กที่กำลังทำงานอยู่ เชื่อมต่อไปยังเครื่องคอมพิวเตอร์ในเครือข่ายทั่วโลก และเข้าไปยังไคร์ฟแตกต่างจากหนอนเครือข่ายคอมพิวเตอร์ ที่ผู้ใช้ต้องเปิดไฟล์จึงจะได้รับและทำการสำเนาจากนั้นหนอนจึงทำงาน

โปรแกรมโทรจัน (Trojan)

หมวดหมู่ย่อย: โทรจัน (โปรแกรมโทรจัน)

ระดับความรุนแรง: สูง

แตกต่างจากหนอนและไวรัส โปรแกรมโทรจันจะไม่มีการสร้างสำเนาซึ่งไม่เหมือนกับไวรัส หรือ หนอนอินเทอร์เน็ต โทรจันมีผลต่อคอมพิวเตอร์ อย่างเช่นจากการที่ผู้ใช้งานส่งอีเมลล์ หรือการเข้าเว็บไซต์เมื่อเข้าไปยังเว็บไซต์ที่มีเชื้ออยู่ โปรแกรมจะแสดงอาการมึนงงร้ายเมื่อมีการใช้งาน

โปรแกรมโทรจันมีการทำงานที่เป็นการกระทำมึนงงร้าย หน้าที่หลักของโทรจันคือ การหยุด ดัดแปลง และการลบข้อมูล การขัดขวางการทำงานของระบบคอมพิวเตอร์หรือ เครือข่ายคอมพิวเตอร์ โปรแกรมโทรจันยังสามารถรับและส่งไฟล์ ดำเนินการ แสดงข้อความ การเข้าถึงเว็บเพจ ดาวน์โหลดและติดตั้งโปรแกรม รวมทั้งการเริ่มต้นคอมพิวเตอร์ที่ติดเชื้อ โทรจันเข้าในคอมพิวเตอร์ของเหยื่อโดยปราศจากการตรวจจับ โดยทั่วไปจะอยู่ในรูปของไฟล์แนบอีเมลล์ที่น่าเชื่อถือ เมื่อใดที่โทรจันถูกเปิดโดยผู้รับเมลล์โดยปราศจากความสงสัย นักโจมตีระบบก็จะสามารถเข้าถึงข้อมูลที่เกี่ยวข้องในเครื่องที่ไม่ได้จำกัดสิทธิ์ผู้ใช้ โทรจันสามารถอยู่ในรูปโปรแกรมที่ทำงานซ่อนอยู่ในคอมพิวเตอร์ หรือซ่อนตัวอยู่ในโปรแกรมที่ถูกต้องปลอดภัยหมายความว่า เป็นโปรแกรมที่ผู้สเซอร์ไว้ใจการทำงานของฟังก์ชันต่างๆที่มี

ผู้บุกรุกมักใช้การติดตั้ง โปรแกรมโทรจันเข้าเป็นส่วนประกอบ

โปรแกรมโทรจันมีความแตกต่างกันไปตามลักษณะการคุกคามดังอธิบายได้ตามตารางข้างล่างต่อไป

ตารางที่ 2 ประเภทของโทรจันที่แบ่งตามลักษณะการคุกคามบนเครื่องคอมพิวเตอร์

ประเภท	ชื่อ	คำอธิบาย
Trojan- ArcBomb	โปรแกรมโทรจัน- ระเบิดไฟล์สำรองข้อมูล (Archive Bomb)	ไฟล์สำรองข้อมูลเมื่อมีการขยายออกก็จะเพิ่มขนาดทำให้ขัดขวางการทำงานของเครื่องคอมพิวเตอร์ เมื่อท่านทำการขยายไฟล์สำรองข้อมูล คอมพิวเตอร์อาจทำงานช้าลงจนกระทั่งหยุดการทำงาน งานเก็บข้อมูลอาจเต็มไปด้วยข้อมูลว่างเปล่า ระเบิดไฟล์สำรองข้อมูล (Archive Bomb) เป็นอันตรายต่อเมล์เซิร์ฟเวอร์ หากว่ามีข้อมูลเข้ามาในระบบโดยอัตโนมัติ จนกลายเป็นระเบิดไฟล์สำรองข้อมูล (Archive Bomb) อาจทำให้หยุดการทำงานของเซิร์ฟเวอร์
ประตูหลัง (Backdoor)	โปรแกรมโทรจันในการควบคุมระบบจากระยะไกล (Remote administration Trojan programs)	โปรแกรมเหล่านี้ถือว่าเป็นโปรแกรมที่อันตรายที่สุดในบรรดาโปรแกรมโทรจันทั้งหมด หลักการทำงานอันชาญฉลาดที่มีความคล้ายคลึงกับโปรแกรมในการควบคุมระบบจากระยะไกล โปรแกรมทำการติดตั้งเองโดยที่ผู้ใช้งานไม่ทราบ และให้ผู้บุกรุกเข้ามาทำการควบคุมระบบจากระยะไกล
โทรจัน (Trojans)	โทรจัน (Trojans)	โทรจันประกอบไปด้วย โปรแกรมมุงร้ายดังต่อไปนี้ <ul style="list-style-type: none"> ● โปรแกรมโทรจันแบบดั้งเดิม ทำหน้าที่หลักแบบโทรจัน ได้แก่ การขโมยข้อมูล การสกัดกั้น เปลี่ยนแปลงหรือลบข้อมูล รวมทั้งการขัดขวางการทำงานของระบบปฏิบัติการของเครื่องคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ จะไม่มีการทำลักษณะอื่นเพิ่มเติมเหมือนโปรแกรมโทรจันประเภทอื่นๆ ดังอธิบายไว้ในตาราง ● วัตถุประสงค์หลากหลาย โปรแกรมโทรจัน ที่ทำหน้าที่อื่นๆเพิ่มเติม หลายประเภท

<p>โทรจันข่มขู่เรียกค่าไถ่ (Trojan-Ransoms)</p>	<p>โปรแกรมโทรจันที่ ต้องการข่มขู่ผู้ใช้เพื่อ การเรียกค่าไถ่</p>	<p>โทรจันประเภทนี้ จะทำการจับเอาข้อมูลของ เครื่องคอมพิวเตอร์เป็นตัวประกัน คัดแปลงหรือ หยุดการทำงาน หรือขัดขวางการทำงานของ ระบบปฏิบัติการคอมพิวเตอร์ หลังจากนั้นผู้บุกรุก ทำการข่มขู่ผู้ใช้ให้ได้ตามต้องการเพื่อให้เกิด การแลกเปลี่ยนกับการทำลายข้อมูลของเครื่องที่ เป็นตัวประกัน</p>
<p>Trojan- clickers</p>	<p>Trojan- clickers</p>	<p>โปรแกรมนี้เข้าถึงเครื่องคอมพิวเตอร์ของผู้ใช้ จากการที่ผู้ใช้ทำการส่งคำสั่งไปยังเว็บเบราว์เซอร์ หรือการแทนที่เว็บที่เก็บสะสมในไฟล์ระบบ</p> <p>การใช้โปรแกรมเหล่านี้ ผู้บุกรุกจะทำการจู่โจม เครือข่าย หรือเพิ่มการจราจรไปสู่บางส่วนของ ไซต์เพื่อให้ทำการแสดงแบนเนอร์โฆษณา</p>
<p>Trojan- Downloaders</p>	<p>โปรแกรม Trojan- Downloaders</p>	<p>โปรแกรมเหล่านี้ มีการเข้าถึงเว็บเพจของผู้บุกรุก การดาวน์โหลดโปรแกรมมัลแวร์ตัวอื่น และ ติดตั้งลงบนเครื่องคอมพิวเตอร์ของผู้ใช้ ทั้งมีการ เก็บชื่อไฟล์ของโปรแกรมที่เป็นโปรแกรมมัลแวร์ ด้วยรหัสของตัวเอง หรือการรับมาจากการเข้า หน้าเว็บที่มีโปรแกรมเหล่านี้</p>
<p>Trojan-Droppers</p>	<p>โปรแกรม Trojan- Droppers</p>	<p>โปรแกรมเหล่านี้เป็นการเก็บโปรแกรมโทรจัน ตัวอื่นๆ บนจานข้อมูลของเครื่องคอมพิวเตอร์ และติดตั้งลงไป</p> <p>ผู้บุกรุกสามารถใช้ Trojan-Droppers ในการ กระทำดังต่อไปนี้</p> <ul style="list-style-type: none"> • ติดตั้งโปรแกรมมัลแวร์โดยที่ผู้ใช้ไม่ ทราบ เนื่องจาก Trojan-Droppers ไม่มี ข้อความใดปรากฏในการติดตั้ง หรือการ แสดงข้อความเท็จ ตัวอย่างเช่น การแจ้ง ให้ทราบเครื่องคอมพิวเตอร์เกิดปัญหา หรือการใช้งานระบบปฏิบัติการผิดเวอร์

		<p>ชั้น</p> <ul style="list-style-type: none"> ● เพื่อให้โปรแกรมมัลแวร์ร้ายสามารถสืบค้นได้ เพราะว่าโปรแกรมแอนตี้ไวรัสบางตัวก็ไม่สามารถตรวจจับโปรแกรมมัลแวร์ที่แฝงอยู่ใน Trojan-Droppers
Trojan- Notifies	โปรแกรม Trojan-Notifies	<p>โปรแกรมจะทำการแจ้งแก่ผู้บุกรุกว่า สามารถเชื่อมต่อเครื่องคอมพิวเตอร์ได้แล้ว และทำการโอนถ่ายข้อมูลจากเครื่องคอมพิวเตอร์ไปยังผู้บุกรุก ได้แก่ หมายเลข IP จำนวนพอร์ตที่เปิด หรือที่อยู่อีเมล โปรแกรมมีการสื่อสารกับผู้บุกรุกผ่านทาง FTP อีเมล หรือทางหน้าเว็บของผู้บุกรุก</p> <p>Trojan- Notifies พบมากในโปรแกรมโทรจันที่ติดตั้งแบบสมบูรณ์ โปรแกรมจะทำการแจ้งว่าโปรแกรมโทรจันตัวอื่นมีกาติดตั้งเสร็จสิ้นแล้วบนเครื่องคอมพิวเตอร์ของผู้ใช้</p>
Trojan-Proxies	Trojan-Proxies	<p>โปรแกรมนี้จะปล่อยให้ผู้บุกรุกเข้ามายังหน้าเว็บแบบไม่เปิดเผย โดยการใช้การระบุตัวตนของคอมพิวเตอร์ของผู้ใช้ และทำการส่งสแปมออกไป</p>
Trojan-PSWs	โทรจันขโมยรหัสผ่าน	<p>โทรจันขโมยรหัสผ่าน (Password Stealing Ware) เป็นโปรแกรมที่เข้ามาขโมยเอาบัญชีผู้ใช้ ตัวอย่างเช่น ข้อมูลการลงทะเบียน โปรแกรมจะทำการค้นหาข้อมูลที่เป็นความลับในไฟล์ระบบ และทำการลงทะเบียนส่งไปยังผู้คิดค้นโปรแกรม โดยการส่งอีเมล หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก</p> <p>โทรจันบางโปรแกรมก็สามารถจำแนกได้ในหัวข้อนี้ รวมไปถึง Trojan-Bankers, Trojans-</p>

		IMs และ Trojans-GameThieves
Trojan-Spies	โปรแกรมสายลับโทรจัน	โปรแกรมนี้ใช้สำหรับการสอดแนมผู้ใช้ โดยทำการสะสมข้อมูลเกี่ยวกับการกระทำของผู้ใช้คอมพิวเตอร์ ตัวอย่างเช่น เข้าไปดักข้อมูลการเข้าถึงยังเป็นพิมพ์ของผู้ใช้ การยิงส่มภาพแล้วจับเอารายการของโปรแกรมที่กำลังทำงาน หลังจากนั้นโปรแกรมได้รับข้อมูล ก็จะโอนถ่ายข้อมูลไปโดยการส่งอีเมลล์ หรือผ่านทางFTP และเข้าสู่เว็บของผู้บุกรุก
Trojan-DoS	โปรแกรมโทรจันจู่โจมเครือข่าย	การโจมตีจู่โจมไม่ให้บริการได้ (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 โดยการส่งอีเมลล์ หรือผ่านทางFTP และเข้าสู่เว็บของผู้บุกรุก
รูทคิทส์ (Rootkits)	รูทคิทส์ (Rootkits)	โปรแกรมเหล่านี้ จะซ่อนเร้นอยู่ในโปรแกรมมุ่งร้ายอื่นๆ การกระทำของโปรแกรมนี้อคือการขยายบางโปรแกรมออกไปในระบบ ซ่อนไฟล์กระบวนการในหน่วยความจำของเครื่องคอมพิวเตอร์ที่ติดเชื้อ หรือซ่อนการโอนถ่ายข้อมูลระหว่างโปรแกรมที่ติดตั้งลงในเครื่องคอมพิวเตอร์ของผู้ใช้ และเครื่องคอมพิวเตอร์

		อื่นๆ ในเครือข่าย
Trojan-SMS	โปรแกรมโทรจัน ข้อความบริการส่ง ข้อความ	โปรแกรมนี้เป็นโปรแกรมที่เกิดปัญหาใน โทรศัพท์เคลื่อนที่ และทำการส่งข้อความจำนวน มากออกจากเครื่องโทรศัพท์ของผู้ใช้
Trojan-GameThieves	โปรแกรมโทรจันขโมย ข้อมูลส่วนบุคคลของ ผู้ใช้งานเครือข่ายเกมส์	โปรแกรมนี้จะทำการขโมยข้อมูลบัญชีของผู้ใช้ เกมส์เครือข่าย และทำการโอนถ่ายข้อมูลเหล่านี้ ไปยังผู้บุกรุกโดยการส่งอีเมลล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก
Trojan-Bankers	โปรแกรมโทรจันขโมย ข้อมูลบัญชีธนาคาร	โปรแกรมนี้จะทำการขโมยข้อมูลบัญชีทาง ธนาคาร หรือข้อมูลบัญชีการเงินดิจิทัล หรือ อิเล็กทรอนิกส์ และทำการโอนถ่ายข้อมูลเหล่านี้ ไปยังผู้บุกรุกโดยการส่งอีเมลล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก
Trojan-Mailfinders	โปรแกรมโทรจันสะสม ที่อยู่อีเมลล์	โปรแกรมนี้จะทำการสะสมที่อยู่อีเมลล์บนเครื่อง คอมพิวเตอร์ และทำการโอนถ่ายข้อมูลเหล่านี้ไป ยังผู้บุกรุก โดยการส่งอีเมลล์ หรือผ่านทาง FTP และเข้าสู่เว็บของผู้บุกรุก ผู้บุกรุกจะใช้ที่อยู่อีเมลล์ เหล่านี้ในการส่งสแปมต่อไป

โปรแกรมอเนกประสงค์มั่งร้าย (Malicious tools)

หมวดหมู่ย่อย: โปรแกรมอเนกประสงค์มั่งร้าย

ระดับความรุนแรง: ปานกลาง

โปรแกรมอเนกประสงค์เหล่านี้ สร้างขึ้นเพื่อให้มีผลต่อคอมพิวเตอร์ ทำลายคอมพิวเตอร์ อย่างไรก็ดี ตาม มีความแตกต่างจากโปรแกรมมัลแวร์อื่นๆ ที่ไม่ได้มีพฤติกรรมในการมัลแวร์เมื่อมีการดำเนินการ โปรแกรม และยังคงมีความปลอดภัยเมื่ออยู่บนเครื่องคอมพิวเตอร์ของผู้ใช้ การกระทำที่แฮกเกอร์ใช้เพื่อการสร้างไวรัส หนอนอินเทอร์เน็ตและโทรจัน จัดการจู่โจมเครือข่ายโดยการรีโมตเซิร์ฟเวอร์ คัดแปลงแก้ไข โปรแกรมการกระทำมัลแวร์อื่นๆ

ประเภทของโปรแกรมอเนกประสงค์มัลแวร์มีอยู่มากมายตามลักษณะของการทำงาน ดังอธิบายไว้ในตารางด้านล่างต่อไปนี้

ตารางที่ 3 ประเภทของโปรแกรมอเนกประสงค์มัลแวร์ตามลักษณะการทำงาน

ประเภท	ชื่อ	คำอธิบาย
Constructor	ผู้สร้าง (Constructors)	ผู้สร้าง (Constructors) ใช้ในการสร้างไวรัส หนอนอินเทอร์เน็ต และโปรแกรมโทรจันตัวใหม่ๆ โปรแกรมผู้สร้างบางตัวมีหน้าตาเป็นวินโดวส์ ที่ให้แฮกเกอร์สามารถเลือกสร้างประเภทของโปรแกรมมัลแวร์ได้หลากหลาย วิธีการของโปรแกรมนี จะใช้การดำเนินการแก้ไขข้อบกพร่อง และคุณสมบัติอื่นๆที่คล้ายคลึงกัน
DoS	การจู่โจมเครือข่าย	การโจมตีจู่โจมไม่ให้บริการได้ (DoS- Denial of Service) การส่งการร้องขอจากเครื่องคอมพิวเตอร์ของผู้ใช้เป็นจำนวนมากไปยังเซิร์ฟเวอร์ทางไกล เมื่อเซิร์ฟเวอร์ได้รับการร้องขอจำนวนมากก็จะหยุดการทำงาน
Exploit	Exploit	Exploit เป็นโปรแกรมที่ได้รับการออกแบบมาเพื่อให้ทำการเจาะระบบโดยอาศัย ช่องโหว่ของโปรแกรม หรือช่องโหว่ต่างๆเพื่อที่จะเข้ามาทำการครอบครอง หรือควบคุมคอมพิวเตอร์ เพื่อที่จะให้กระทำการบางอย่าง ตัวอย่างเช่น Exploit สามารถเขียน หรืออ่านไฟล์ หรือพาไปยังเว็บที่ติดเชื่อ

		<p>Exploit ที่แตกต่างกันจะใช้ช่องโหว่ของโปรแกรมที่แตกต่างกัน หรือบริการเครือข่ายที่ต่างกัน Exploit ที่ส่งผ่านไปทางเครือข่ายจะไปยังเครื่องคอมพิวเตอร์ต่างๆ ตามรูปแบบของแพ็กเก็ตของเครือข่าย การค้นหาเครื่องคอมพิวเตอร์ในเครือข่ายที่อ่อนแอ ตัวอย่างเช่น Exploit เข้ามาในไฟล์เอกสาร เพื่อหาช่องโหว่ของเนื้อหาในไฟล์เอกสาร (DOC) เมื่อผู้ใช้เปิดใช้งานไฟล์เอกสารที่ติดเชื่อ ก็จะปฏิบัติตามคำสั่งของผู้บุกรุกสามารถเข้ามาในระบบได้แล้วก็จะเริ่มทำการเปลี่ยนแปลงข้อมูลในระบบ ข้อมูลของระบบ หรือว่าโปรแกรมของเซิร์ฟเวอร์ เพื่อให้ส่งข้อมูลไปหาตัวเอง หรือว่าเพื่อให้ Exploit สามารถเข้ามาสู่ระบบได้อีกครั้งหนึ่งถึงแม้ว่าช่องโหว่เดิมได้ถูกปิดไปแล้ว Exploit สามารถเข้าอยู่ในเนื้อหาของอีเมลเพื่อหาช่องโหว่ที่อยู่ในโปรแกรมอีเมล และเริ่มการกระทำมุ่งร้ายตราบเท่าที่ผู้ใช้ปิดไฟล์ที่ติดเชื่อนี้</p> <p>Exploit สามารถใช้การแพร่กระจายผ่านทางนอนเครือข่าย Exploit-Nukers เป็นแพ็กเก็ตเครือข่ายที่ทำให้เครื่องคอมพิวเตอร์ทำงานไม่ได้</p>
FileCryptors	ตัวเข้ารหัสไฟล์ (File Cryptors)	ตัวเข้ารหัสไฟล์ (File Cryptors) ทำการสร้างรหัสลับโปรแกรมมุ่งร้ายอื่น เพื่อซ่อนไม่ให้แอนตี้ไวรัสมองเห็น
Flooders	โปรแกรมทำให้เครือข่ายท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากผ่านยังช่องทางเครือข่าย รวมไปถึงช่องทางการสนทนา IRC <p>อย่างไรก็ตาม หมวดหมู่ของโปรแกรมมุ่งร้ายนี้ไม่ได้รวมถึงการทำให้ อีเมล การส่งข้อความทันที หรือการส่งข้อความท่วมท้น ซึ่งแยกหมวดหมู่เอาไว้ดังตารางข้างล่าง (Email-Flooder, IM-Flooder และ SMS-Flooder).</p>

HackTools	เครื่องมือเจาะโปรแกรม (Hacking Tools)	เครื่องมือเจาะโปรแกรม (Hacking Tools) จะให้เพื่อการเจาะเครื่องคอมพิวเตอร์ที่มีโปรแกรมนี้อยู่ หรือเพื่อการเตรียมการเจาะเครื่องคอมพิวเตอร์เครื่องอื่น เช่น การสร้างบัญชีผู้ใช้ระบบใหม่ที่ไม่ได้รับอนุญาต หรือการล้างข้อมูลบันทึกเพื่อปิดบังว่ามีผู้ใช้ใหม่ขึ้นมาในระบบ บางครั้งก็มีการแสดงการทำงานที่มุ่งร้าย ตัวอย่างเช่น การระงับรหัสผ่าน โปรแกรมสแนฟเฟอร์ (Sniffers) เป็นโปรแกรมซึ่งทำหน้าที่ดักจับแพ็กเกตในเครือข่าย
not-virus: Hoax	โปรแกรม Hoax	โปรแกรมเหล่านี้ทำให้ผู้ใช้หวาดกลัวด้วยข้อความเหมือนไวรัส โปรแกรมทำการตรวจค้นไวรัสในไฟล์หรือแสดงข้อความเกี่ยวกับการฟอร์แมตงานข้อมูลทั้งที่ไม่ได้มีเกิดขึ้น
Spoofers	การปลอมแปลง (Spoofers)	โปรแกรมเหล่านี้จะทำการส่งข้อความการร้องขอของเครือข่าย ด้วยที่อยู่ของผู้ส่งที่ปลอมแปลงขึ้น ผู้บุกรุกใช้การปลอมแปลงนี้เป็นคำสั่ง ตัวอย่างเช่น การทำเหมือนว่าเป็นผู้ส่งจริง
VirTools	เครื่องมือที่ใช้ในการสร้างปรับเปลี่ยนโปรแกรมมุ่งร้าย	โปรแกรมนี้ทำให้มีโอกาสในการเปลี่ยนแปลงโปรแกรมมุ่งร้ายอื่นๆ เพื่อซ่อนโปรแกรมมุ่งร้ายจากโปรแกรมต่อต้านไวรัส
Email-Flooders	โปรแกรมทำให้อีเมลท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากไปยังที่อยู่อีเมล ทำให้เกิดการไหลของข้อมูลจำนวนมาก ทำให้ผู้ใช้ไม่สามารถรับอีเมลที่เข้ามาแล้วไม่ใช้สแปมได้
IM-Flooders	โปรแกรมทำให้ระบบส่งข้อความทันทีท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากไปยังระบบส่งข้อความทันที (Instant messaging) เช่น ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager and Skype ทำให้ผู้ใช้ไม่สามารถรับข้อความที่เข้ามาแล้วไม่ใช้สแปมได้
SMS-Flooders	โปรแกรมทำให้อีข้อความบริการส่งข้อความท่วมท้น	โปรแกรมเหล่านี้จะทำการส่งข้อความจำนวนมากไปยังบริการส่งข้อความบนโทรศัพท์เคลื่อนที่

โปรแกรมซึ่งอาจไม่พึงประสงค์

โปรแกรมซึ่งอาจไม่พึงประสงค์ แตกต่างจากโปรแกรมมัลแวร์ และไม่ได้ต้องการทำให้เกิดความเสียหาย อย่างไรก็ตาม ก็เป็นการผิดต่อความปลอดภัยของคอมพิวเตอร์

โปรแกรมซึ่งอาจไม่พึงประสงค์ ประกอบไปด้วย ซอฟต์แวร์โฆษณา โปรแกรมเกี่ยวข้องกับเรื่องเพศ โปรแกรมที่มีความเสี่ยงอื่นๆ

ซอฟต์แวร์โฆษณา เป็นการแสดงข้อความโฆษณาส่งถึงผู้ใช้

โปรแกรมเกี่ยวข้องกับเรื่องเพศ แสดงข้อมูลทางเพศส่งถึงผู้ใช้

โปรแกรมที่มีความเสี่ยงอื่นๆ เป็นโปรแกรมที่เป็นประโยชน์ต่อผู้ใช้คอมพิวเตอร์ อย่างไรก็ตาม หากผู้บุกรุกเข้ามาล้วงล้ำด้วยโปรแกรมเหล่านี้ หรือเข้ามาติดตั้งลงในเครื่องคอมพิวเตอร์ของผู้ใช้ ก็จะเป็นการผิดต่อความปลอดภัยของคอมพิวเตอร์

โปรแกรมซึ่งอาจไม่พึงประสงค์จะมีวิธีการในการติดตั้งลงเครื่องคอมพิวเตอร์อยู่สองวิธีดังต่อไปนี้

- ติดตั้งเองโดยผู้ใช้ ร่วมกับการติดตั้งโปรแกรมอื่น หรือติดตั้งโปรแกรมเดียว ตัวอย่างเช่น นักพัฒนาซอฟต์แวร์ร่วมกับโปรแกรมโฆษณาที่ติดมากับซอฟต์แวร์ฟรี และแชร์แวร์
- การติดตั้งโดยผู้บุกรุก ตัวอย่างเช่น รวมมาในโปรแกรมที่เป็นโปรแกรมมัลแวร์อื่นๆ โดยการอาศัยช่องโหว่ของเว็บเบราว์เซอร์ หรือตัวดาวน์โหลดโทรจัน หรือดรอปปอร์เมื่อผู้ใช้เข้ามายังเว็บไซต์ที่มีการติดเชื่อ

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 ผู้ใช้งานมักติดตั้งโปรแกรมเหล่านี้ด้วยตัวเอง จากการค้นหา หรือดาวน์โหลดข้อมูลที่เกี่ยวข้องกับเรื่องเพศ

ผู้บุกรุกก็สามารถทำการติดตั้งโปรแกรมเหล่านี้ที่เครื่องคอมพิวเตอร์ของผู้ใช้ เพื่อแสดงการโฆษณา รูปแบบการค้าและบริการเรื่องเพศแก่ผู้ใช้ โดยปราศจากการยินยอมของผู้ใช้ ในการติดตั้งผู้บุกรุกจะอาศัยช่องโหว่ของระบบปฏิบัติการหรือเว็บเบราว์เซอร์ แล้วทำการแพร่กระจายตัวดาวน์โหลดโทรจัน หรือครอปเปอร์

โปรแกรมเกี่ยวข้องกับเรื่องเพศ (Pornware) มีอยู่ 3 ประเภทตามตารางแสดงด้านล่างนี้

ตารางที่ 4 ประเภทของโปรแกรมเกี่ยวกับเรื่องเพศ (Pomware)

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

โปรแกรมที่มีความเสี่ยงอื่นๆ

หมวดหมู่ย่อย: โปรแกรมที่มีความเสี่ยงอื่นๆ

ระดับความรุนแรง: ระดับกลาง

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

อย่างไรก็ตาม หากว่าผู้บุกรุกเข้ามาล้วงล้ำผ่านทางโปรแกรมเหล่านี้ หรือติดตั้งลงบนคอมพิวเตอร์ ผู้ใช้ ก็จะเป็นการฝ่าฝืนต่อความปลอดภัยของคอมพิวเตอร์

ตารางแสดง โปรแกรมที่มีความเสี่ยง แบ่งกลุ่มตามหน้าที่

ตารางที่ 5 ประเภทของโปรแกรมที่มีความเสี่ยงแบ่งกลุ่มตามหน้าที่

ประเภท	ชื่อ	คำอธิบาย
Client-IRC	โปรแกรมการสนทนา กับลูกข่าย	ผู้ใช้งานทำการติดตั้ง โปรแกรมเพื่อการสื่อสารผ่าน ทาง IRC ผู้บุกรุกอาศัยช่องทางนี้ในการแพร่กระจาย โปรแกรมมัลแวร์
Dialers	โปรแกรมหมุนโทรออก อัตโนมัติ	โปรแกรมนี้จะทำการซ่อนตัวติดตั้งการเชื่อมต่อผ่าน ทางโมเด็ม
Downloaders	Downloaders	โปรแกรมเหล่านี้สามารถดาวน์โหลดไฟล์จากเว็บไซต์
Monitors	Monitors	โปรแกรมเหล่านี้ทำการเฝ้าดูการกระทำของ คอมพิวเตอร์ที่มีการติดตั้ง รวมไปถึงการเฝ้าดูการ ทำงานของโปรแกรม และการแลกเปลี่ยนข้อมูลกับ โปรแกรมบนเครื่องคอมพิวเตอร์เครื่องอื่น
PSWTools	เครื่องมือกู้คืนรหัสผ่าน	โปรแกรมเหล่านี้ใช้เพื่อทำการดูและกู้คืนรหัสผ่านที่จำ ไม่ได้ ผู้บุกรุกจะใช้ในวิธีการเดียวกันเมื่อทำการติดตั้ง โปรแกรมบนคอมพิวเตอร์ของผู้ใช้
RemoteAdmin	โปรแกรมในการ ควบคุมระบบจาก ระยะไกล	โปรแกรมนี้มีการใช้งานอย่างมากจากผู้ดูแลระบบ ที่ ทำการเข้าถึงคอมพิวเตอร์ด้วยการควบคุมระยะไกล เพื่อการเฝ้าดูและจัดการ ผู้บุกรุกใช้โปรแกรมนี้ใน วิธีการเดียวกันเมื่อทำการติดตั้งโปรแกรมบน คอมพิวเตอร์ของผู้ใช้ โปรแกรมที่มีความเสี่ยงในการควบคุมระบบจาก ระยะไกล มีความแตกต่างจากโทรจัน (หรือว่าประจูด หลัง) โปรแกรมโทรจันสามารถแทรกเข้ามาได้อย่าง เป็นอิสระภายในระบบ และทำการติดตั้งตัวเอง โปรแกรมที่ถูกต้องตามกฎหมายไม่มีการทำงานนี้
Server-FTP	FTPServers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น FTP servers ผู้บุกรุก จะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้เพื่อ ทำการควบคุมระยะไกลผ่านทางโปรโตคอลFTP
Server-Proxy	Proxy servers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น Proxy servers ผู้บุกรุก จะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้ เพื่อทำการควบคุมระยะไกลผ่านทางโปรโตคอล

		Proxy
Server-Telnet	Telnet servers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น Telnet servers ผู้บุกรุกจะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้เพื่อทำการควบคุมระยะไกลผ่านทางโปรโตคอล Telnet
Server-Web	Web servers	โปรแกรมเหล่านี้จะทำหน้าที่เป็น Web servers ผู้บุกรุกจะเข้ามาติดตั้งโปรแกรมเหล่านี้บนเครื่องของผู้ใช้เพื่อทำการควบคุมระยะไกลผ่านทางโปรโตคอล HTTP
RiskTool	เครื่องมือคอมพิวเตอร์ ภายใน	เครื่องมือเหล่านี้ทำให้ผู้ใช้มีความสามารถเพิ่มเติมในการทำงานภายในเครื่องคอมพิวเตอร์ของผู้ใช้ โปรแกรมนี้ยอมให้แฮกเกอร์แอบแฝงไฟล์เข้ามา แอบแฝงหน้าต่างโปรแกรม หรือการปิดการดำเนินการที่กำลังทำอยู่
NetTool	เครื่องมือเครือข่าย	เครื่องมือเหล่านี้ยอมให้ผู้ใช้จัดการเครื่องคอมพิวเตอร์ เครื่องอื่นๆ ในเครือข่าย ตัวอย่าง การรีเซ็ตตัวเอง การค้นหาพอร์ทที่เปิด หรือการดำเนินการโปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์เหล่านี้
Client-P2P	โปรแกรมลูกข่ายแบบ Peer to peer	โปรแกรมเหล่านี้ใช้สำหรับการจัดการระบบเครือข่ายแบบ Peer to Peer ผู้บุกรุกสามารถใช้เพื่อปล่อยโปรแกรมมัลแวร์
Client-SMTP	SMTP clients	โปรแกรมเหล่านี้ ทำการส่งข้อความทางอีเมล และซ่อนการกระทำเอาไว้ในอีเมล เพื่อส่งสแปมไปยังผู้ใช้ที่มีภาระ
WebToolbar	แถบเครื่องมือเว็บ	โปรแกรมเหล่านี้มีการเพิ่มเติมแถบเครื่องมือการค้นหาเพื่อไปยังแถบเครื่องมือเบราว์เซอร์อื่น
FraudTool	โปรแกรมการหลอกลวง	โปรแกรมเหล่านี้มีการอำพรางโปรแกรมจริงตัวอื่น ตัวอย่างเช่น โปรแกรมป้องกันไวรัสแบบปลอม มีการแฝงการตรวจสอบซอฟต์แวร์มัลแวร์ แต่ไม่ได้ค้นหาหรือไม่ได้ทำการกำจัดแต่อย่างใด

วิธีการป้องกันการติดโปรแกรมที่น่าสงสัยเป็นอันตรายโดยโปรแกรม

คาร์ปาสกีแอนตี้ไวรัส ทำการค้นหาโปรแกรมมุงร้ายโดยใช้วิธีการ 2 วิธี คือ การค้นหาแบบตอบสนอง (โดยการใช้ฐานข้อมูล) และการค้นหาแบบเชิงรุก (ใช้การวิเคราะห์แบบฮิวริสติก)

ฐานข้อมูลของโปรแกรมประกอบไปด้วยการรายงานที่ระบุว่าคุณคิดว่ามัน ที่ได้รับการตรวจสอบ รายงานนี้ประกอบไปด้วยข้อมูลที่มาจากทั้งส่วนของการควบคุม และอัลกอริทึมสำหรับการกำจัดโปรแกรมเหล่านี้ ตัววิเคราะห์แอนตี้ไวรัสของคาร์ปาสกีแลปทำการวิเคราะห์โปรแกรมมุงร้ายใหม่ๆ เป็นร้อยละ โปรแกรมประจำวัน สร้างการรายงานผลและระบุตัวตน รวมทั้งมีการอัปเดตลงในไฟล์ฐานข้อมูล

ภัยคุกคามทางอินเทอร์เน็ต

โปรแกรมของคาร์ปาสกีแลปใช้เทคโนโลยีพิเศษ เพื่อการปกป้องคอมพิวเตอร์จากภัยคุกคามความปลอดภัยดังต่อไปนี้

- สเปนหรือเมลล์ขยะ
- ฟิชชิง (Phishing)
- การจู่โจมของแฮกเกอร์
- การแสดงแบนเนอร์

สเปนหรือเมลล์ขยะ

โปรแกรมของคาร์ปาสกีแลปให้การปกป้องผู้ใช้จากสเปน สเปนคือเมลล์ขยะที่เข้ามาในกล่องจดหมายส่วนมากแล้วเป็นพวกโฆษณา สเปนทำให้พนักงานต่อช่องทางเซิร์ฟเวอร์ของเมลล์ ผู้รับจะต้องเสียจำนวนโทรฟิคต่อการรับเมลล์ขยะทำให้ช้าลง สเปนเป็นสปีดกฎหมายในหลายประเทศ

คาร์ปาสกีแลปทำการตรวจสอบเมลล์ที่เข้ามาทาง Microsoft Office Outlook, Microsoft Outlook Express และ The Bat! Messages หากพบว่าเป็นข้อความสแปม ก็จะมีการกระทำให้ท่านเลือก อย่างเช่น การย้ายข้อความไปยังโฟลเดอร์พิเศษ หรือการลบมันไป

โปรแกรมของคาร์ปาสกีแลป ทำการสืบค้นด้วยระดับความแม่นยำที่สุด โดยการใช้เทคโนโลยีการกรองสแปมหลายชั้น โดยใช้พื้นฐานจากที่อยู่ของผู้ส่ง และคำหรือวลีที่มานบนหัวเรื่องที่ส่ง การตรวจจับสแปมภาพและการใช้อัลกอริทึมของตัวเองเพื่อค้นหาสแปมจากเนื้อหา

ฐานข้อมูลแอนตี้สแปม ประกอบไปด้วย รายการชื่อผู้ส่งที่ต้องการ (White list) และไม่ต้องการ (Black list)

ฟิชชิง (Phishing)

ฟิชชิง เป็นประเภทของการกระทำหลอกลวงที่คล้ายกับการตกปลา ล่อลวงผู้ใช้ให้บอกหมายเลขเครดิต รหัส และข้อมูลส่วนตัวอื่นๆ เพื่อการขโมยเอาเงิน

ฟิชชิง เป็นการกระทำที่พบได้บ่อยในเรื่องของการเงินธนาคารทางอินเทอร์เน็ต ผู้บุกรุกสามารถทำการสร้าง ตำนานของธนาคารเป้าหมายและส่งข้อความไปยังลูกค้าธนาคาร โดยการอ้างว่าเนื่องจากมีการเปลี่ยนแปลง หรือมีความผิดพลาดทางด้านเว็บซอฟต์แวร์ของธนาคาร ทำให้บัญชีของผู้ใช้เกิดการสูญหาย และต้องการให้ผู้ใช้ทำการยืนยันใหม่อีกครั้ง หรือทำการเปลี่ยนแปลงข้อมูลบนเว็บไซต์ของธนาคาร ผู้ใช้ทำการคลิกลิงค์เพื่อเข้าไปยังเว็บไซต์ที่ผู้บุกรุกสร้างขึ้น และเข้าไปยังข้อมูลส่วนตัวของผู้ใช้

ฐานข้อมูลแอนตี้ฟิชชิง ประกอบไปด้วยรายการชื่อ URL ของเว็บไซต์ที่พบว่าเป็นเว็บฟิชชิง

โปรแกรมของคาร์ปาสกีแลป ทำการวิเคราะห์ข้อความที่เข้ามาทาง Microsoft Office Outlook และ Microsoft Outlook Express และหากเจอ URL ที่อยู่ในฐานข้อมูลก็จะทำเครื่องหมายว่าเป็นสแปม หากผู้ใช้พยายามเปิดและลิงค์ไปยังเว็บไซต์เหล่านั้น โปรแกรมก็จะทำการสกัดกั้นเว็บไซต์นี้

การโจมตีของแฮกเกอร์

การโจมตีของแฮกเกอร์ เป็นการเข้ามาบุกรุกเพื่อเข้าสู่ระบบของเครือข่ายแบบระยะไกล เพื่อทำการควบคุม และเป็นสาเหตุที่ทำให้ล้มเหลว หรือการเข้าถึงข้อมูลที่ต้องการป้องกัน

การโจมตีทางเครือข่ายนั้นมีทั้งการกระทำของผู้กรุก (เช่น การตรวจสอบพอร์ต การเข้าเอารหัสผ่าน) หรือ โปรแกรมมัลแวร์ที่ดำเนินการบนความรับผิดชอบของผู้ใช้ และส่งผ่านข้อมูลไปยังส่วนอื่นที่เกี่ยวข้องกับการโจมตีเครือข่าย ประกอบไปด้วยโปรแกรมโทรจันบางประเภท การโจมตีDOS บทสคริปต์ที่เป็นมัลแวร์ และหนอนเครือข่าย

การโจมตีเครือข่าย จะแพร่กระจายไปยังพื้นที่ภายในและเครือข่ายภายนอก โดยการอาศัยช่องโหว่ในระบบปฏิบัติการและโปรแกรม โดยสามารถโอนถ่ายแพ็กเก็ตข้อมูลIP ระหว่างการเชื่อมโยงเครือข่าย

โปรแกรมของคาร์ปาสกีแลป หยุดการโจมตีทางเครือข่ายโดยไม่ต้องหยุดการเชื่อมต่อเครือข่าย โดยการใช้ฐานข้อมูลไฟร์วอลล์พิเศษ ฐานข้อมูลเหล่านี้ประกอบไปด้วยลักษณะของแพ็กเก็ตข้อมูลIP ที่ระบุของโปรแกรมดักลอบต่างๆ โปรแกรมทำการวิเคราะห์การเชื่อมต่อเครือข่าย และหยุดการทำงานของIP ที่เป็นอันตราย

การแสดงผลแบนเนอร์

แบนเนอร์หรือการโฆษณา เป็นการเชื่อมโยงไปยังเว็บไซต์ของผู้โฆษณาที่ส่วนมากแล้วไม่ได้แสดงผลออกมาเฉพาะภาพ การแสดงผลแบนเนอร์บนเว็บไซต์ไม่ได้เป็นสิ่งที่ขัดต่อความปลอดภัยของคอมพิวเตอร์ แต่เป็นการรบกวนการทำงานของคอมพิวเตอร์ การกระพริบของแบนเนอร์บนจอ ทำให้ลดประสิทธิภาพในการทำงานลง ทำให้เกิดความรำคาญ การตามลิงค์แบนเนอร์ไปเป็นการเพิ่มทราฟฟิกอินเทอร์เน็ต

องค์กรหลายแห่งทำการสั่งห้าม ไม่ให้มีการแสดงผลแบนเนอร์ในส่วนของบริษัทความปลอดภัยข้อมูล

โปรแกรมคาร์ปาสกีแลป ทำการสกัดกั้นแบนเนอร์บนเว็บไซต์ ซึ่งเป็นแบนเนอร์ที่มีลิงค์ ฐานข้อมูลแอนตี้แบนเนอร์สามารถทำการอัปเดตได้ ซึ่งมีเครือข่ายรัสเซียและต่างชาติ โปรแกรมทะลุไปยังลิงค์ของ

เว็บไซต์ เพื่อทำการเปรียบเทียบที่อยู่ในฐานข้อมูล และการตามลิงค์ที่แน่นอน การลบลิงค์จากที่ตั้งและ
ดำเนินการโหลดหน้านั้น

การติดตั้งโปรแกรม

ขั้นตอนที่1 ค้นหาโปรแกรมเวอร์ชันล่าสุด

ขั้นตอนที่2 ตรวจสอบความต้องการของระบบ

ขั้นตอนที่3 หน้าต่างการเริ่มต้นวิซาร์ด

ขั้นตอนที่4 ข้อตกลงทางด้านลิขสิทธิ์

ขั้นตอนที่5 เลือกประเภทของการติดตั้ง

ขั้นตอนที่6 เลือกโฟลเดอร์การติดตั้ง

ขั้นตอนที่7 เลือกส่วนประกอบโปรแกรมเพื่อทำการติดตั้ง

ขั้นตอนที่8 ค้นหาซอฟต์แวร์แอนตี้ไวรัสตัวอื่น

ขั้นตอนที่9 ขั้นตอนสุดท้ายของการเตรียมการติดตั้ง

ขั้นตอนที่10 เสร็จสิ้นการติดตั้ง

ขั้นตอนที่ 1 ค้นหาโปรแกรมเวอร์ชันล่าสุด

ก่อนทำการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ของท่าน วิศวกรการติดตั้งของคาร์ปาสกีแลป จะเข้าทำการตรวจสอบค้นหาโปรแกรมเวอร์ชันล่าสุดบนเซิร์ฟเวอร์ของคาร์ปาสกีแลป

หากไม่พบว่ามีโปรแกรมเวอร์ชันที่ใหม่กว่า วิศวกรจะเริ่มดำเนินการติดตั้งเวอร์ชันปัจจุบันที่มีอยู่

หากพบว่ามีเวอร์ชันที่ใหม่กว่าบนเซิร์ฟเวอร์ของคาร์ปาสกีแลป ระบบจะขอให้ท่านทำการดาวน์โหลดและติดตั้ง หากท่านยกเลิกการดาวน์โหลด วิศวกรจะเริ่มดำเนินการติดตั้งเวอร์ชันปัจจุบันที่มีอยู่หากท่านทำการดาวน์โหลดเวอร์ชันที่ใหม่กว่า ก็จะทำให้การดาวน์โหลดไฟล์การติดตั้งลงบนเครื่องคอมพิวเตอร์ของท่าน และวิศวกรการติดตั้งก็จะเป็นของเวอร์ชันใหม่อย่างอัตโนมัติ สำหรับรายละเอียดการติดตั้งของเวอร์ชันใหม่ กรุณาดูที่เอกสารของเวอร์ชันใหม่

ขั้นตอนที่ 2 ตรวจสอบความต้องการของระบบ

ก่อนการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ วิศวกรจะทำการยืนยัน ความต้องการขั้นต่ำของระบบ (ดูได้จากส่วนของ ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ) เพื่อทำการยืนยันความต้องการของระบบที่ถูกต้องในการติดตั้งซอฟต์แวร์

หากว่าไม่มีตามความต้องการของระบบ จะมีการแสดงข้อความขึ้น แนะนำให้ท่านทำการอัปเดต โดยการใช **Window Update** และลงโปรแกรมที่ตรงตามความต้องการของระบบ ก่อนการติดตั้งคาร์ปาสกี แอนตี้ไวรัสอีกครั้ง

ขั้นตอนที่ 3 หน้าต่างการเริ่มต้นวิศวกร

หากระบบของท่านตรงตามความต้องการของระบบ (ดูได้จากส่วนของ ความต้องการซอฟต์แวร์และฮาร์ดแวร์ของระบบ) และไม่มีโปรแกรมเวอร์ชันที่ใหม่กว่า จากการตรวจสอบค้นหาโปรแกรมเวอร์ชันล่าสุดบนเซิร์ฟเวอร์ของคาร์ปาสกีแลป หรือท่านได้ยกเลิกการดาวน์โหลด วิศวกรจะเริ่มดำเนินการติดตั้งเวอร์ชันปัจจุบันที่มีอยู่

เมื่อปรากฏกรอบสนทนาแรกของวิศว์การติดตั้งบนหน้าจอ แสดงว่ากำลังเข้าสู่ขั้นตอนการติดตั้ง
เริ่มกระบวนการติดตั้งโดยการกดปุ่ม **Next** ยกเลิกการติดตั้งกดปุ่ม **Cancel**

ขั้นตอนที่ 4 ข้อตกลงทางด้านลิขสิทธิ์

กรอบสนทนาต่อไปของวิศว์การแสดงข้อตกลงทางด้านลิขสิทธิ์ ระหว่างท่านและคาร์ปาสกีแลป
อ่านโดยละเอียดและหากท่านยอมรับข้อตกลงและเงื่อนไขแล้วให้เลือกที่ **I accept the terms of the
license agreement** และกดปุ่ม **Next** เพื่อดำเนินการติดตั้งต่อไป

ยกเลิกการติดตั้งกดปุ่ม **Cancel**

ขั้นตอนที่ 5 เลือกประเภทของการติดตั้ง

ระหว่างขั้นตอนนี้จะมีคำถามให้ท่านเลือกประเภทของการติดตั้งที่เหมาะสมสำหรับท่านดังนี้

- **การติดตั้งด่วน (Express installation)** หากท่านเลือกการติดตั้งนี้ จะทำการติดตั้งโปรแกรมทั้งหมดลงบนเครื่องคอมพิวเตอร์ของท่าน รวมทั้งการตั้งค่าป้องกันเริ่มต้นที่ทางคาร์ปาสกีแลปแนะนำ เมื่อการติดตั้งเสร็จสิ้น จะเริ่มต้นวิศว์การตั้งค่าโปรแกรมขึ้น
- **การติดตั้งแบบเลือกเอง (Custom installation)** หากท่านเลือกการติดตั้งนี้ ระบบจะถามให้ท่านเลือกส่วนที่ท่านต้องการเลือกลง เพื่อระบุไฟล์ของโปรแกรมที่ท่านต้องการ (ดูที่ขั้นตอนที่ 6 เลือกไฟล์เคอร์การติดตั้ง) เพื่อเริ่มการทำงานของโปรแกรม และการตั้งค่าการใช้งานโดยวิศว์การตั้งค่าโปรแกรม

หากท่านเลือกการติดตั้งแบบแรก วิศว์การติดตั้งโปรแกรมจะข้ามไปยังขั้นตอนที่ 8 (ดูที่ ขั้นตอน
ที่ 8 ค้นหาซอฟต์แวร์แอนตี้ไวรัสตัวอื่น) ถ้าเป็นอีกแบบการติดตั้ง ท่านสามารถทำตามขั้นตอนตามแต่ละ
ขั้นตอนของการติดตั้ง

ขั้นตอนที่ 6 เลือกโฟลเดอร์การติดตั้ง

หมายเหตุ

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

ในขั้นตอนนี้จะมีคำถามให้ท่านระบุโฟลเดอร์ของการติดตั้งบนเครื่องคอมพิวเตอร์ที่ต้องการติดตั้ง
เส้นทางคำสั่งเริ่มต้นคือ

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

ท่านสามารถระบุโฟลเดอร์ที่แตกต่างจากนี้โดยการเลือกปุ่ม **Browse** และเลือกโฟลเดอร์ในกล่อง
สนทนาโฟลเดอร์มาตรฐาน หรือเข้าไปยังทางผ่านของโฟลเดอร์

คำเตือน!

โปรดสังเกตว่า หากท่านเลือกการเข้าเส้นทางคำสั่งด้วยมือสู่โฟลเดอร์การติดตั้ง ความยาวของ
อักขระจะต้องไม่เกิน 200 อักขระ และต้องไม่มีเส้นทางเป็นคำสั่งที่มีอักขระพิเศษ

กดปุ่ม **Next** เพื่อการติดตั้งต่อไป

ขั้นตอนที่ 7 เลือกส่วนประกอบโปรแกรมเพื่อทำการติดตั้ง

หมายเหตุ

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

ในการติดตั้งแบบเลือกเอง ท่านจะต้องทำการเลือกส่วนประกอบโปรแกรมเพื่อทำการติดตั้งตามที่ท่านต้องการลงบนเครื่องคอมพิวเตอร์ โดยค่าเริ่มต้น ทุกส่วนประกอบของโปรแกรมจะตั้งเอาไว้ที่ การปกป้อง การตรวจสอบและการอัปเดตไฟล์โปรแกรมที่ท่านต้องการ

ข้อมูลที่มีอยู่เกี่ยวกับแต่ละส่วนประกอบของโปรแกรม จะมีส่วนช่วยท่านในการเลือกตัดสินใจตามที่ท่านต้องการ เลือกส่วนประกอบจากรายการและอ่านรายละเอียดข้อมูลประกอบการด้านล่าง ข้อมูลจะเป็นการอธิบายคร่าวๆ เกี่ยวกับส่วนประกอบรวมทั้งข้อมูลพื้นที่ของหน่วยเก็บข้อมูลที่ต้องการหากทำการติดตั้ง

ก่อนทำการติดตั้งส่วนประกอบใดๆ ให้ทำการเปิดเมนูถัด โดยการคลิกที่สัญลักษณ์หน้าชื่อของส่วนประกอบ และเลือกที่รายการ Component will not be available ฟังระวัง หากท่านเลือกยกเลิกการติดตั้งส่วนประกอบใดๆ รายการนั้นจะไม่มีการป้องกันจากโปรแกรมที่เป็นอันตราย

การเลือกส่วนประกอบของการติดตั้งโปรแกรม เปิดที่เมนูถัดโดยการคลิกที่สัญลักษณ์ถัดไปต่อจากชื่อของส่วนประกอบ และเลือกที่ Component will be installed on local hard drive

เมื่อเสร็จสิ้นการเลือกไฟล์ที่ต้องการติดตั้ง กดที่ปุ่ม **Next** หากต้องการย้อนกลับเลือกรายการของส่วนประกอบตามค่าเริ่มต้น ให้กดปุ่ม **Clear**

ขั้นตอนที่ 8 ค้นหาซอฟต์แวร์แอนตี้ไวรัสตัวอื่น

ในขั้นตอนนี้ วิศวกรจะทำการค้นหาโปรแกรมแอนตี้ไวรัสตัวอื่น รวมทั้งโปรแกรมอื่นของคาร์ปาสกีแลป ที่จะเป็นการทำงานขัดกับโปรแกรม

หากพบว่ามีโปรแกรมใดๆ บนเครื่องคอมพิวเตอร์ของท่าน จะมีการแสดงรายการให้เห็นบนจอ และจะมีการถามให้ท่านเลือกลบโปรแกรมเหล่านั้นทิ้ง ก่อนการดำเนินการติดตั้ง

หากว่ารายการของโปรแกรมแอนตี้ไวรัสที่ตรวจพบได้ รวมไปถึงโปรแกรม 7.0 ของคาร์ปาสกีแลป มีการบันทึกไฟล์คีย์ในตอนทำการลบทิ้งไป ท่านสามารถใช้คีย์นี้สำหรับเวอร์ชันปัจจุบัน เราขอแนะนำให้ท่านเก็บรักษาแยกเอาไว้และในที่เก็บหน่วยเก็บสำรอง วัตถุประสงค์นี้จะเคลื่อนย้ายฮาร์ดไดรฟ์เมื่อมีการแยกออก จากเวอร์ชันปัจจุบัน และสามารถทำการตรวจสอบซ้ำหลังการติดตั้ง

หากเลือกการลบทิ้งคาร์ปาสกีเวอร์ชัน 7.0 แบบฮาร์ดไดรฟ์ จะมีการบันทึกข้อมูลการเริ่มต้นโปรแกรม และการนำกลับมาใช้ใหม่ในระหว่างการติดตั้งเวอร์ชัน 2009

คำเตือน!

โปรแกรมนี้ยอมรับไฟล์คีย์สำหรับเวอร์ชัน 6.0 หรือ 7.0 เท่านั้น ไม่สนับสนุนการทำงาน สำหรับเวอร์ชัน 5.0 หรือเวอร์ชันก่อนหน้า

ขั้นตอนที่ 9 ขั้นตอนสุดท้ายของเตรียมการติดตั้ง

ขั้นตอนนี้เป็นการเสร็จสิ้นการเตรียมการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ของท่าน

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

หมายเหตุ

หากการติดตั้งโปรแกรมเป็นการติดตั้งระยะไกลจากการใช้ Remote Desktop ท่านสามารถเลือกไม่เลือก Enable Self-Defense before installation หากมีการตรวจสอบการติดตั้งอาจไม่สามารถทำงานได้หรืออาจมีการทำงานผิดพลาด

กดปุ่ม Next เพื่อดำเนินการติดตั้ง ไฟล์การติดตั้งจะเริ่มต้นสำเนาลงบนเครื่องคอมพิวเตอร์ของท่าน

คำแนะนำ

ในช่วงของการติดตั้ง การเชื่อมต่อเครือข่ายที่มีอยู่อาจมีความหน่วง ถ้าแพ็คเกจของโปรแกรมมีการแทรกเข้ามาในกราฟฟิกของเครือข่าย การเชื่อมต่อจะกลับมาเป็นปกติเมื่อการติดตั้งสิ้นสุดลง

ขั้นตอนที่ 10 เสร็จสิ้นการติดตั้ง

หน้าต่าง Installation complete การติดตั้งเสร็จสิ้น จะแสดงข้อมูลการติดตั้งที่เสร็จสิ้นของโปรแกรมบนคอมพิวเตอร์ของท่าน

ตัวอย่างเช่น วินโดว์จะแสดงความจำเป็นในการเปิดเครื่องใหม่เพื่อความสำเร็จของการติดตั้ง หลังจากระบบได้เริ่มใหม่อีกครั้ง วิศวกรการติดตั้งก็จะเสร็จสมบูรณ์

หากไม่ต้องการเริ่มระบบใหม่ ให้เลือกปุ่ม Next เพื่อเริ่มวิศวกรการตั้งค่าการใช้งาน

ตัวประสานการใช้งานของผู้ใช้กับโปรแกรม

รูปสัญลักษณ์แสดงการแจ้งเตือน

เมนูลัด

หน้าต่างโปรแกรมหลัก



การแจ้งเตือน

หน้าต่างการตั้งค่า โปรแกรม





รูปสัญลักษณ์แสดงการแจ้งเตือน

ทันทีหลังจากการติดตั้งโปรแกรม รูปสัญลักษณ์ของโปรแกรมจะปรากฏบนบริเวณแถบงานของไมโครซอฟต์วินโดวส์ (Microsoft Windows taskbar) ตรงมุมขวาด้านล่าง

รูปสัญลักษณ์แสดงถึงการทำงานในตอนนี้ของโปรแกรม บอกถึงสถานะการป้องกัน แสดงจำนวนพื้นฐานการทำงานของโปรแกรม

ถ้ารูปสัญลักษณ์  เป็นสีแดงที่กำลังทำงาน มีการดำเนินการในบางส่วนหรือทั้งหมดของโปรแกรม แต่หากว่ารูปสัญลักษณ์  เป็นสีดำ แสดงว่าไม่มีการทำงาน


รูปสัญลักษณ์ของโปรแกรมมีการเปลี่ยนแปลงไปตามการดำเนินการต่อไปนี้

-  กำลังทำการตรวจสอบอีเมล
-  กำลังอัปเดตฐานข้อมูลและโมดูล โปรแกรม
-  จำเป็นต้องมีการปิดและเปิดเครื่องคอมพิวเตอร์ใหม่เพื่อการอัปเดต
-  เกิดข้อผิดพลาดในบางส่วน of โปรแกรม

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

การเปิดเมนูหลัก ให้ทำการคลิกขวาบนสัญลักษณ์ของโปรแกรม

การเปิดหน้าต่างโปรแกรมหลัก ให้คลิกสองครั้งที่สัญลักษณ์ของโปรแกรม หน้าต่างหลักเมื่อเปิดจะแสดงส่วนของ Protection เสมอ

หากมีข่าวสารจากคาร์ปาสกี รูปสัญลักษณ์ข่าวสารจะปรากฏในแถบงาน  ที่บริเวณมุมขวาด้านล่าง เมื่อทำการคลิกสองครั้งบนรูปสัญลักษณ์จะมีหน้าต่างแสดงข่าวขึ้นมา

เมนูหลัก

ท่านสามารถกำหนดการดำเนินการเพื่อการปกป้องพื้นฐาน ได้จากรายการดังต่อไปนี้

- Update เริ่มต้นโมดูลโปรแกรม และการอัปเดตฐานข้อมูล รวมทั้งการติดตั้งการอัปเดตลงบนเครื่องคอมพิวเตอร์
- Full Computer Scan เริ่มการตรวจสอบอย่างเต็มรูปแบบให้แก่คอมพิวเตอร์พ้นจากวัตถุอันตราย โดยทำการตรวจสอบทุกไคร์ฟรอม ไปถึงสื่อเก็บข้อมูลที่เคลื่อนย้ายได้
- Virus Scan เลือกวัตถุแล้วทำการตรวจสอบไวรัส รายการเริ่มต้นสำหรับตรวจสอบมีไม่ที่รายการ เช่น โฟลเดอร์ My documents และตัวเก็บอีเมล ท่านสามารถเพิ่มเติมให้ทำการตรวจสอบได้ตามความต้องการ
- Network Monitor ดูรายการของการเชื่อมต่ออินเทอร์เน็ต พอร์ตที่เปิดและทราฟฟิก
- Virtual keyboard สลับไปใช้งานแป้นพิมพ์เสมือน
- Kaspersky Internet Security เปิดหน้าต่างโปรแกรมหลัก (ดูที่ เรื่องของ หน้าต่างโปรแกรมหลัก)
- Setting ดูและปรับเปลี่ยนการตั้งค่าโปรแกรม
- Activate การเริ่มต้นโปรแกรม เพื่อเป็นผู้ใช้ที่จดทะเบียนแล้ว ท่านจะต้องทำการเริ่มต้นโปรแกรมของท่าน รายการเมนูนี้จะคงอยู่หากว่าท่านยังไม่ได้ทำการเริ่มต้นโปรแกรม
- About ข้อมูลแสดงผลเกี่ยวกับโปรแกรม

- Pause protection/ Resume protection การหยุดการทำงานชั่วคราว หรือการเปิดให้ใช้งานป้องกันแบบเรียลไทม์ ตัวเลือกเมนูนี้จะไม่ส่งผลต่อการอัปเดตโปรแกรม หรือการดำเนินการตรวจสอบไวรัส
- Block network traffic การหยุดชั่วคราวในการเชื่อมต่อเครือข่ายคอมพิวเตอร์ทั้งหมด หากท่านต้องการให้คอมพิวเตอร์มีการติดต่อกับเครือข่าย ให้เลือกรายการนี้จากเมนูบริบทอีกครั้ง
- Exit ปิดโปรแกรมและปลดโปรแกรมออกจากความจำของเครื่อง



รูปที่ 1 เมนูลัด

หากกำลังมีการทำงานตรวจสอบไวรัส เมื่อท่านเปิดเมนูลัด จะขึ้นเป็นสถานะการดำเนินการ (อัตราร้อยละที่เสร็จสมบูรณ์) ไว้ที่เมนูลัด ในการเลือกงานท่านจะเปิดจากหน้าต่างโปรแกรมหลัก ซึ่งมีรายงานผลการดำเนินการของงานตรวจสอบอยู่

หน้าต่างโปรแกรมหลัก

หน้าต่างโปรแกรมหลักประกอบไปด้วย 3 ส่วนคือ

- ส่วนบนสุดของหน้าต่างแสดงให้เห็นถึงสถานะของการป้องกันขณะนั้นของคอมพิวเตอร์

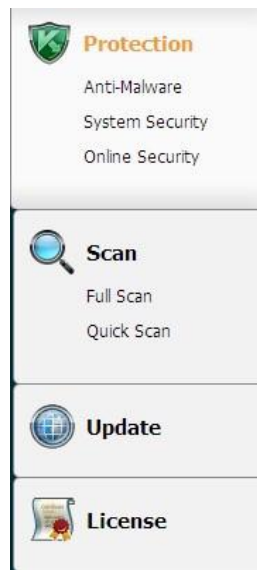


ภาพที่ 2 สถานะของการป้องกันปัจจุบันของคอมพิวเตอร์

สถานะของการป้องกันปัจจุบันของคอมพิวเตอร์แบ่งออกเป็น 3 ค่า โดยที่แต่ละค่าจะมีสีประจำคล้ายกับสีของไฟจราจร สีเขียวหมายถึง สถานะของการป้องกันปัจจุบันของคอมพิวเตอร์อยู่ในระดับที่ถูกต้อง ขณะที่สีเหลืองและสีแดงนั้น อยู่ในสถานะที่มีภัยคุกคามต่อความปลอดภัยในการตั้งค่าระบบ หรือการดำเนินการ โปรแกรม เนื่องมาจากฐานข้อมูลโปรแกรมมั่วร้าย และภัยคุกคามไม่ทันสมัย การปิดส่วนการทำงานของการป้องกัน และการเลือกการติดตั้งการป้องกันในระดับน้อย

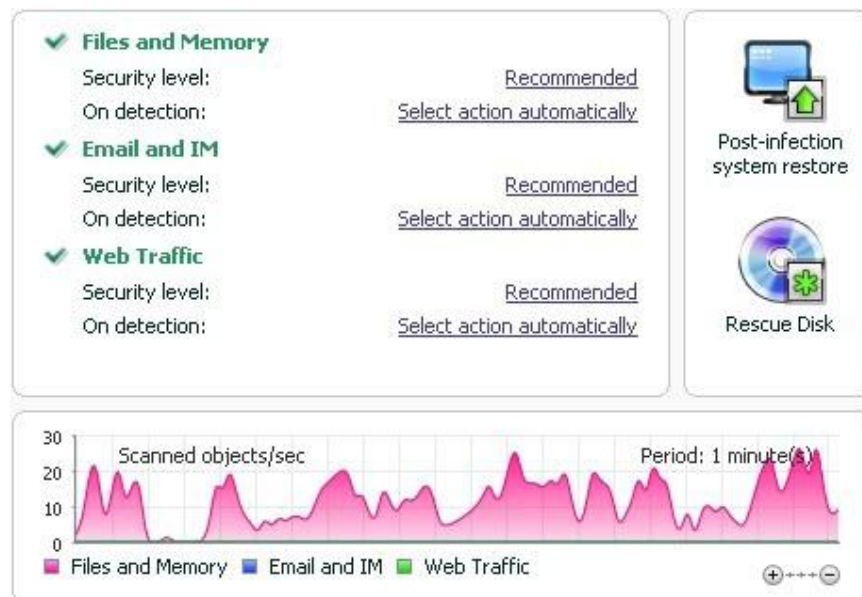
ภัยคุกคามความปลอดภัย จำกัดออกไปได้ทันทีที่ปรากฏ เลือกคลิก fix it now เพื่อรับทราบข้อมูลเกี่ยวกับมันแล้วกำจัดมันอย่างรวดเร็ว (ดูที่ภาพข้างล่าง)

- ส่วนด้านซ้ายมือของหน้าต่าง แถบนำทาง (Navigation bar) จะนำเข้าสู่ส่วนการทำงานของโปรแกรมอย่างรวดเร็ว รวมทั้งการตรวจสอบไวรัสและการอัปเดตงาน



ภาพที่ 3 ส่วนทางซ้ายของหน้าต่าง

- ส่วนทางด้านขวาของหน้าต่างประกอบไปด้วยข้อมูลเกี่ยวกับการทำงานของโปรแกรม ที่ได้เลือกไปในส่วนทางด้านซ้ายมือ และใช้เพื่อการตั้งค่าตัวเลือกการทำงานและเครื่องมือแสดงการทำงาน ด้านการตรวจสอบไวรัส การควั่นไหลด์ตัวอัปเดต เป็นต้น



ท่านสามารถใช้ปุ่มดังต่อไปนี้ได้ด้วย

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

หมายเหตุ

ท่านสามารถเปลี่ยนแปลงหน้าต่างการแสดงผลของโปรแกรม โดยการสร้าง และใช้ภาพกราฟฟิกและสีของตนเองได้

การแจ้งเตือน

เมื่อเกิดเหตุการณ์ขึ้นระหว่างการดำเนินการ การแจ้งเตือนพิเศษจะปรากฏขึ้นบนหน้าจอ แสดงเป็นข้อความขึ้นทันทีเหนือรูปสัญลักษณ์ของโปรแกรมในแถบล่างด้านขวา

การแจ้งเตือนจะแตกต่างกันไป ขึ้นอยู่กับความร้ายแรงต่อความปลอดภัยของเครื่องคอมพิวเตอร์ ที่มีดังต่อไปนี้

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

หน้าต่างการตั้งค่าโปรแกรม

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

หน้าต่างการตั้งค่า โปรแกรมประกอบไปด้วยสองส่วนคือ

- ส่วนทางด้านซ้ายมือของหน้าต่าง ประกอบไปด้วยการเข้าถึงส่วนประกอบของโปรแกรม เช่นงานการตรวจสอบไวรัส และการอัปเดตงาน
- ส่วนทางด้านขวาของหน้าต่างประกอบด้วยรายการการตั้งค่าสำหรับส่วนประกอบ หรืองานที่ได้เลือกไว้ทางด้านซ้ายของหน้าต่าง

การเริ่มต้น

หนึ่งในวัตถุประสงค์หลักของการที่คาร์ปาสกีแลป สร้างคาร์ปาสกีอินเทอร์เน็ตซีเคียวริตี้ ถือว่าเป็น การสร้างโปรแกรมที่ดีที่สุดสำหรับเป็นทางเลือกของโปรแกรมทั้งหมด เพื่อให้ผู้ใช้งานคอมพิวเตอร์ไม่เกิด ความยุ่งยาก สามารถทำงานได้ทันทีหลังจากการติดตั้ง โดยไม่ต้องใช้เวลานานในการเปลี่ยนแปลงการติดตั้ง

เพื่อความสะดวกสบายแก่ผู้ใช้ เราจึงรวมเอาขั้นตอนในการตั้งค่าเบื้องต้น เข้าไว้ในวิซาร์ดการติดตั้ง เริ่มแรกในตอนเริ่มต้นการทำงานของโปรแกรม โดยการตามคำแนะนำของวิซาร์ด ท่านสามารถทำการ เริ่มต้นโปรแกรม ตั้งค่าสำหรับการอัปเดต การจำกัดการเข้าถึงโปรแกรมโดยการเข้ารหัสผ่าน และการทำการ ติดตั้งอื่นๆ

เครื่องคอมพิวเตอร์ของท่านอาจมีการติดโปรแกรมมุงร้ายก่อนมีการติดตั้งโปรแกรม เพื่อการ ตรวจสอบโปรแกรมมุงร้ายที่มีอยู่ ต้องทำการตรวจสอบคอมพิวเตอร์ (ดูที่ การตรวจสอบไวรัสในเครื่อง คอมพิวเตอร์)

อันเนื่องมาจากการติดโปรแกรมมุงร้าย หรือความล้มเหลวของระบบ การตั้งค่าของเครื่อง คอมพิวเตอร์อาจมีการผิดพลาด ให้ดำเนินการวิซาร์ดการวิเคราะห์ความปลอดภัย เพื่อค้นหาช่องโหว่หรือ จุดอ่อนใดๆ ในซอฟต์แวร์ที่มีการติดตั้งและความผิดปกติของการตั้งค่าระบบ

โปรแกรมในปัจจุบัน ฐานข้อมูลโปรแกรมที่มากับชุดการติดตั้งอาจเป็นรุ่นเก่า ให้เริ่มต้นการอัปเดต โปรแกรม หากไม่ได้มีการดำเนินการในวิซาร์ดการตั้งค่า หรือกระทำอย่างอัตโนมัติหลังจากมีการติดตั้ง โปรแกรม

ส่วนประกอบแอนตี้สแปมที่อยู่ในโปรแกรม นั้นใช้อัลกอริทึมที่ฝึกฝนด้วยตนเองเพื่อค้นหา ข้อความที่ไม่พึงประสงค์ การตั้งค่าแอนตี้สแปม สามารถทำการโต้ตอบกับท่านได้ด้วยวิซาร์ด

หลังจากดำเนินการเสร็จสมบูรณ์ในส่วนนี้ โปรแกรมก็พร้อมปกป้องเครื่องคอมพิวเตอร์ของท่าน เพื่อประเมินการดำเนินการของเครื่องคอมพิวเตอร์ท่าน ให้ใช้วิซาร์ดการจัดการความปลอดภัย(ดูที่ส่วนของการจัดการความปลอดภัย)

เนื้อหาในส่วนนี้ประกอบไปด้วย

การเลือกประเภทเครือข่าย

การอัปเดตโปรแกรม

การวิเคราะห์ความปลอดภัย

การตรวจสอบไวรัสในเครื่องคอมพิวเตอร์

การมีส่วนร่วมในเครือข่ายความปลอดภัยคาร์ปาสกี

การจัดการความปลอดภัย

การหยุดปกป้องชั่วคราว

การเลือกประเภทเครือข่าย

หลังจากการติดตั้ง

After the application is installed, the Firewall component will analyze the active network connections on your computer. Each network connection will be assigned a status determining the allowed network activities. If you selected the interactive mode of Kaspersky Internet Security operation, a notification will be displayed each time a network connection is established. You can select the status for new networks in the notification window:

Public network - for network connections with the status access to your computer from the outside is not allowed. For this networks access to public folders and printers is also allowed. This status is recommended to assign to the Internet network.

Local network - for the network connections with such status access to public folders and network printers is allowed. It is recommended to assign this status to protected local networks, for example, a corporate network.

Trusted network - for the network connections with this status any activities are allowed. It is recommended to assign only for the absolutely security areas.

การอัปเดตโปรแกรม

คำเตือน!

คุณต้องทำการเชื่อมต่ออินเทอร์เน็ตเพื่อการอัปเดตคาร์ปาส์อินเทอร์เน็ตซีเคียวริตี้

ฐานข้อมูลประกอบไปด้วยหลายเซิร์ฟเวอร์ที่ขึ้นอยู่กับสถานะการกระจายโปรแกรม อย่างไรก็ตาม เมื่อโปรแกรมได้ทำการติดตั้งเป็นที่เรียบร้อยแล้วอาจยังไม่ใหม่เพียงพอ เมื่อคาร์ปาส์ที่แลปทำการอัปเดตแล้ว ฐานข้อมูลและโมดูลก็จะอยู่ในสภาพปกติ

ท่านสามารถระบุการอัปเดตงานเมื่อวิศวกรติดตั้งดำเนินการคาร์ปาส์อินเทอร์เน็ตซีเคียวริตี้ จะทำการตรวจสอบการอัปเดตจากเซิร์ฟเวอร์ของคาร์ปาส์ที่แลปให้อย่างอัตโนมัติตามค่าการเริ่มต้น หากว่าเซิร์ฟเวอร์พบว่ามีการอัปเดตใหม่ก็จะทำการดาวน์โหลดและติดตั้งต่อไป

เพื่อให้เครื่องคอมพิวเตอร์ของคุณทันต่อฐานข้อมูล ขอแนะนำให้ทำการอัปเดตคาร์ปาส์อินเทอร์เน็ตซีเคียวริตี้หลังจากการติดตั้ง

- สำหรับการอัปเดตคาร์ปาส์อินเทอร์เน็ตซีเคียวริตี้ด้วยมือ

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

เนื่องมาจากว่า คาร์ปาส์อินเทอร์เน็ตซีเคียวริตี้ จะเริ่มทำการอัปเดต รายละเอียดของกระบวนการจะแสดงผลให้เห็นทางหน้าต่างพิเศษ

การวิเคราะห์ความปลอดภัย

ระบบปฏิบัติการของเครื่องคอมพิวเตอร์อาจโดนทำลายจากความล้มเหลวของระบบ และกิจกรรมของโปรแกรมมัลแวร์ นอกจากนี้โปรแกรมผู้ใช้งานที่ติดตั้งลงไปในเครื่องคอมพิวเตอร์ของท่าน ก็อาจเป็นช่องโหว่ให้ผู้บุกรุกสามารถเข้ามาทำลายเครื่องคอมพิวเตอร์ของท่าน

เพื่อการค้นหาและการกำจัดปัญหาทางต้นความปลอดภัย แนะนำให้ดำเนินการ วิเคราะห์วิเคราะห์ความปลอดภัย *Security Analyzer Wizard* ทันทีหลังจากที่คุณทำการติดตั้ง โปรแกรมเรียบร้อยแล้ว สำหรับความเสียหายของระบบปฏิบัติการ และการติดตั้ง

- เริ่มต้นการทำงาน
 1. เปิดหน้าต่าง โปรแกรมหลัก
 2. ทางด้านซ้ายของหน้าต่าง เลือก System Security
 3. เริ่มต้นการทำงานที่ Security Analyzer

การตรวจสอบไวรัสในเครื่องคอมพิวเตอร์

นักพัฒนาโปรแกรมมัลแวร์จะทำทุกวิถีทางเพื่อการเข้าถึงเครื่องคอมพิวเตอร์ และที่อาจทราบได้ว่าโปรแกรมมัลแวร์เหล่านั้นเข้ามาเครื่องคอมพิวเตอร์ของเราได้อย่างไร

เมื่อท่านติดตั้งคาร์ปาสกีแอนตี้ไวรัสลงบนเครื่องคอมพิวเตอร์ของท่าน โปรแกรมจะดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ของท่านอย่างอัตโนมัติ ด้วยการทำ Quick scan งานนี้จะทำการค้นหาเพื่อการทำลายโปรแกรมที่เป็นอันตรายภายในเครื่อง ซึ่งจะทำให้ระบบปฏิบัติการของเครื่องทำงานหนัก

ผู้เชี่ยวชาญของคาร์ปาสกีแลป แนะนำให้ท่านทำการตรวจสอบเครื่องแบบเต็มรูปแบบดังต่อไปนี้

- เริ่มต้น/หยุดการตรวจสอบไวรัส

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

การมีส่วนร่วมในเครือข่ายความปลอดภัยคาร์ปาสกี

ภัยคุกคามใหม่ๆ เกิดขึ้นมากมายทุกวัน เพื่อให้ท่านได้รับความสะดวกสบายในการรับทราบข้อมูลทางสถิติ ข่าวสารเกี่ยวกับการเกิดภัยคุกคาม รับทราบที่มาของภัยคุกคามและวิธีในการกำจัด คาร์ปาสกีแลกเปลี่ยนเชิญท่านใช้บริการเครือข่ายความปลอดภัยคาร์ปาสกี

การใช้งานเครือข่ายความปลอดภัยคาร์ปาสกี รวมถึงการส่งข้อมูลเข้าสู่คาร์ปาสกีแลปมีดังต่อไปนี้

- การตั้งชื่อที่มีความเป็นหนึ่งเดียวบนเครื่องคอมพิวเตอร์ของท่าน ชื่อนี้จะมีลักษณะอยู่บนการตั้งค่าเครื่องคอมพิวเตอร์ของท่าน และไม่มีข้อมูลอื่นใด
- ข้อมูลเหล่านี้เป็นข้อมูลเกี่ยวกับภัยคุกคามที่จับได้จากโปรแกรม โครงสร้างและเนื้อหาของข้อมูลขึ้นอยู่กับประเภทของภัยคุกคาม
- ข้อมูลระบบ ประกอบไปด้วย เวอร์ชันของระบบปฏิบัติการ รวบรวมการบริการ ไดรฟ์เวอร์ และการบริการที่สามารถดาวน์โหลดได้ บราวเซอร์ เวอร์โปรแกรมอีเมล การขยาย บราวเซอร์ จำนวนเวอร์ชันของคาร์ปาสกีแอนตี้ไวรัสที่ทำการติดตั้ง

เครือข่ายความปลอดภัยของคาร์ปาสกี รวมไปถึงสถิติที่ขยายอันมีข้อมูลเกี่ยวกับ

- แฟ้มการกระทำในระบบ และโปรแกรมที่มีการลงชื่อที่ได้ดาวน์โหลดบนเครื่องคอมพิวเตอร์
- โปรแกรมที่ทำงานอยู่บนเครื่องคอมพิวเตอร์ของท่าน

ข้อมูลเกี่ยวกับทางสถิตินี้ ส่งออกไปเมื่อโปรแกรมได้ทำการอัปเดตเป็นที่เรียบร้อยแล้ว

คำถาม!

คาร์ปาสกีแลปให้การรับประกันว่าจะไม่มีการเก็บรวบรวมชื่อและข้อมูลส่วนบุคคลของผู้ใช้ หรือทำการแจกจ่ายข้อมูลส่วนบุคคลของผู้ใช้ ในการดำเนินการเกี่ยวกับเครือข่ายความปลอดภัยคาร์ปาสกี

- การตั้งค่าการส่งสถิติ

1. เปิดหน้าต่างการตั้งค่าโปรแกรม
2. เลือก Feedback ที่อยู่ทางด้านซ้ายของหน้าต่าง
3. เลือกช่อง I agree to participate in Kaspersky Security Network เพื่อยืนยันในการเข้าร่วมเครือข่ายความปลอดภัยคาร์ปาสกี 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) ที่เกิดขึ้นเมื่อท่านคลิกลิงค์ Fix it now (ดูที่ภาพข้างบน)



ภาพที่ 6 การแก้ปัญหาความปลอดภัย

แถบแสดงรายการของปัญหาที่เกิดขึ้น รายการปัญหาจะลำดับตามความสำคัญ ประการแรกเป็นปัญหาที่มีความรุนแรงมากที่สุด มีรูปสัญลักษณ์ที่เป็นสีแดง ประการที่สอง จะเป็นปัญหาที่มีความสำคัญ

น้อยรองลงมา จะเป็นรูปสัญลักษณ์สีเขียว คำอธิบายอย่างละเอียดแยกไปตามแต่ละปัญหา และการกระทำที่มีอยู่ตามมา

- **กำจัดทันที (Eliminate immediately)** ใช้ปุ่มเพื่อการตอบสนอง ท่านสามารถเริ่มทำศกแก้ไขปัญหา 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 จากเมนูหลักของโปรแกรม (ดูที่ส่วนของเมนูหลัก)
 2. เมื่อเปิดหน้าต่างขึ้นมา ให้เลือกคาบเวลาที่ต้องการหยุดการปกป้อง
 - ในช่วงเวลา (In <time interval>) การป้องกันจะเกิดขึ้นเมื่อเวลาผ่านไป

- หลังการเริ่มต้นทำงานใหม่ (After restart) การป้องกันจะเกิดหลังจากการเริ่มต้นทำงานใหม่ของระบบ
- โดยมือ Manually การป้องกันที่เกิดขึ้นจากการที่ผู้ใช้ตั้งค่าการป้องกันด้วยตัวเอง โดยการเลือก Resume protection จากเมนูหลักของ โปรแกรม

ด้วยเหตุที่ว่า มีการหยุดการป้องกันชั่วคราว การป้องกันในส่วนประกอบต่างๆ ก็หยุดลง โดยมีการแสดงให้เห็นดังต่อไปนี้

- ชื่อไม่มีการทำงาน (เป็นสีเทา) สำหรับส่วนประกอบที่ปิดการทำงานในส่วนของการ Protection ของหน้าต่างหลัก
- รูปสัญลักษณ์ของโปรแกรมไม่มีการทำงาน (เป็นสีเทา) (ดูที่ส่วนของ รูปสัญลักษณ์แสดงการแจ้งเตือน) ในรายชื่อระบบ
- สีแดงเป็นรูปสัญลักษณ์แสดงสถานะ และสำหรับรายชื่อของหน้าต่าง โปรแกรมหลัก

ถ้ามีการเชื่อมต่อเครือข่ายใหม่ ในเวลาเดียวกับการหยุดการป้องกัน การแจ้งเตือนจะมีข้อความแสดงเกี่ยวกับการหยุดการเชื่อมต่อ

การตั้งค่าโปรแกรมให้สมบูรณ์

หลังจากการติดตั้งและตั้งค่าโปรแกรมเป็นที่เรียบร้อยแล้ว
โปรแกรมที่ถูกต้อง โดยการทดสอบไวรัสและการปรับเปลี่ยนค่า

ท่านควรทำการยืนยันการติดตั้ง

เนื้อหาในส่วนนี้มีดังต่อไปนี้

ทดสอบไวรัส EICAR และการปรับเปลี่ยน

การทดสอบการปกป้องข้อมูลผ่านทางHTTP

การทดสอบการปกป้องข้อมูลผ่านทางSMTP

การตั้งค่าไฟล์แอนตี้ไวรัสให้สมบูรณ์

การตั้งการตรวจสอบไวรัสให้สมบูรณ์

การตั้งการตรวจสอบแอนตี้สแปมให้สมบูรณ์

ทดสอบไวรัส EICAR และการปรับเปลี่ยน

การทดสอบไวรัสออกแบบโดย EICAR (สถาบันการค้นคว้าแอนตี้ไวรัสคอมพิวเตอร์แห่งยุโรป)
สำหรับการทดสอบผลิตภัณฑ์แอนตี้ไวรัส

ทดสอบไวรัสที่ไม่ใช่ไวรัส เพราะว่ามีรหัสที่ทำอันตรายต่อเครื่องคอมพิวเตอร์ของท่าน อย่างไรก็ตาม
ตาม ผู้ผลิตส่วนมากของผลิตภัณฑ์แอนตี้ไวรัสระบุว่าไฟล์เหล่านี้เป็นไวรัส

คำเตือน!

ไม่มีการใช้ไวรัสจริงในการทดสอบระบบการทำงานของผลิตภัณฑ์แอนตี้ไวรัส

ท่านสามารถดาวน์โหลดการทดสอบไวรัสได้จากเว็บไซต์ขององค์กร

EICAR

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

หมายเหตุ

ก่อนทำการดาวน์โหลดไฟล์ ต้องทำการปิดการทำงานของการป้องกันแอนตี้ไวรัสของคอมพิวเตอร์ไม่เช่นนั้นแล้ว 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 ของการทำงานของโปรแกรมโดยการตัดแปลงไวรัสของ EICAR เท่านั้น หากว่าฐานข้อมูลล่าสุดมีการอัปเดตเมื่อวันที่ 4 เดือนตุลาคม 2003

ในตารางด้านล่าง คอลัมน์แรกประกอบไปด้วย คำนำหน้าที่มีการเพิ่มเมื่อตอนเริ่มต้นของข้อความไวรัสมาตรฐาน คอลัมน์ที่สองทำรายการค่าสถานะความเป็นไปได้ที่โปรแกรมทำต่อวัตถุด้วยสถานะเฉพาะสถานะที่แท้จริงมีการกระทำเกิดขึ้นเมื่อมีการตั้งค่าโปรแกรมแล้ว

หลังจากที่ท่านเพิ่มคำนำหน้าที่มีการเพิ่มเมื่อตอนเริ่มต้นของข้อความไวรัสมาตรฐาน ตัวอย่างเช่น eicar_dele.com ให้ทำการบันทึกชื่อไฟล์ที่แตกต่างกัน ทำให้เหมือนกันแบบนี้กับไวรัสที่ทำการเปลี่ยนแปลง

ตารางที่ 6 การเปลี่ยนแปลงการทดสอบไวรัส

คำนำหน้า	สถานะวัตถุ	ข้อมูลการดำเนินการวัตถุ
ใช้ไวรัสมาตรฐาน ไม่มีคำนำหน้า	ติดเชื้อ (Infected) เกิดการติดเชื้อด้วยไวรัสที่รู้จัก ไม่สามารถทำลายได้	โปรแกรมระบุว่าเป็นวัตถุติดเชื้อ ไม่สามารถทำลายได้ เกิดความผิดพลาดขึ้นขณะกระทำการทำลายเชื้อ มีการใช้งานการดำเนินการไม่สามารถทำลายเชื้อได้
CORR-	เกิดความเสียหาย (Corrupted)	โปรแกรมสามารถเข้าไปยังวัตถุ แต่ไม่สามารถตรวจสอบได้ เพราะว่า มีความเสียหายเกิดขึ้น (ตัวอย่างเช่น โครงสร้างของไฟล์เกิดความเสียหาย หรือไม่ถูกต้อง) จะพบข้อมูลการดำเนินการวัตถุในการรายงานการดำเนินการโปรแกรม

WARN-	<p>ต้องสงสัย (Suspicious)</p> <p>วัตถุประกอบไปด้วยรหัสของไวรัสที่ไม่ทราบชื่อ จึงไม่อาจกำจัดได้</p>	<p>วัตถุค้นพบที่ต้องสงสัยโดยตัววิเคราะห์แบบฮิวริสติก ในขณะที่มีการตรวจสอบ ฐานข้อมูลของโปรแกรมไม่มีคำอธิบายของวิธีการในการดำเนินการกับวัตถุ ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้</p>
SUSP-	<p>ต้องสงสัย (Suspicious)</p> <p>วัตถุมีรหัสที่ได้รับการเปลี่ยนแปลงของไวรัสที่รู้จัก ไม่อาจกำจัดได้</p>	<p>โปรแกรมได้ตรวจจับการโต้ตอบบางส่วนของรหัสของวัตถุด้วย ส่วนของวัตถุมีรหัสที่ได้รับการเปลี่ยนแปลงของไวรัสที่รู้จัก ฐานข้อมูลของโปรแกรมไม่มีคำอธิบายของวิธีการในการดำเนินการกับวัตถุ ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้</p>
ERRO-	<p>การตรวจสอบผิดพลาด</p>	<p>เกิดข้อผิดพลาดขึ้นระหว่างการตรวจสอบวัตถุ โปรแกรมไม่สามารถเข้าถึงวัตถุ และการดำเนินการมีการหยุดชะงัก (ตัวอย่างเช่น ไม่มีจุดสิ้นสุดของปริมาณ) หรือไม่มีการเชื่อมต่อ (หากว่ามีการตรวจสอบบริเวณไคร์ฟเครือข่าย) ท่านสามารถหาข้อมูลเกี่ยวกับการดำเนินการของวัตถุได้จากการรายงานการดำเนินการของโปรแกรม</p>

CURE-	<p>ติดเชื้อ (Infected)</p> <p>เกิดการติดเชืด้วยไวรัสที่รู้จัก ไม่สามารถทำลายได้</p>	<p>วัตถุประกอบไปด้วยไวรัสที่ไม่สามารถทำลายได้ โปรแกรมจะไม่ทำลายวัตถุ มีการแทนที่เนื้อหาของตัวไวรัส เพื่อแทนที่คำว่า CURE ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้</p>
DELE-	<p>ติดเชื้อ (Infected)</p> <p>เกิดการติดเชืด้วยไวรัสที่รู้จัก ไม่สามารถทำลายได้</p>	<p>โปรแกรมระบุว่า เป็นไวรัสที่ไม่สามารถทำลายได้</p> <p>เกิดความผิดพลาดเกิดขึ้นทำให้ไม่สามารถทำลายไวรัส การกระทงจะเกิดขึ้นเฉพาะไวรัสที่ไม่สามารถทำลายได้</p> <p>ท่านจะได้รับแจ้งเมื่อมีการตรวจจับวัตถุนี้</p>

การทดสอบการปกป้องข้อมูลผ่านทาง HTTP

เพื่อเป็นการยืนยันการตรวจจับไวรัสเสร็จสมบูรณ์ผ่านทางโปรโตคอล HTTP ต้องดำเนินการดังต่อไปนี้

ลองดาวน์โหลดการทดสอบไวรัสได้จากเว็บไซต์ขององค์กร

EICAR

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

เมื่อทำการดาวน์โหลดการทดสอบไวรัส คาร์ปาสกีแอนตี้ไวรัสจะทำการตรวจจับวัตถุ และระบุวัตถุที่ติดเชื้อมันไม่สามารถทำลายได้ และจะดำเนินการติดตั้งทราฟฟิก HTTP กับวัตถุที่สถานะนี้ ค่าเริ่มต้นเมื่อทำการดาวน์โหลดการทดสอบไวรัส การเชื่อมต่อเว็บไซต์จะสิ้นสุด และบราวเซอร์ก็จะแสดงผลแก่ผู้ใช้งาน มีการทดสอบไวรัสด้วย EICAR-Test-File virus

การทดสอบการปกป้องข้อมูลผ่านทาง SMTP

เพื่อเป็นการตรวจจับกระแสข้อมูลผ่านทาง SMTP ท่านต้องทำการโอนถ่ายข้อมูลผ่านทางระบบอีเมลที่ใช้โปรโตคอลนี้

หมายเหตุ

เราแนะนำให้ท่านทำการทดสอบกับคาร์ปาสกีแอนตี้ไวรัสในการรับมือกับเมลล์เข้าและออก รวมทั้งตัวข้อความในเมลล์และเอกสารแนบ ในการทดสอบการตรวจจับไวรัสในตัวข้อความ ให้ทำสำเนาข้อความของการทดสอบไวรัสมาตรฐาน หรือไวรัสที่มีการดัดแปลงเข้าไปในตัวข้อความ

- การทดสอบการตรวจจับไวรัสผ่านทาง SMTP
1. สร้างข้อความธรรมดาโดยการใช้อีเมลที่มีการติดตั้งบนเครื่องคอมพิวเตอร์

หมายเหตุ

ข้อความที่ใช้ในการทดสอบ ต้องเป็นข้อความที่ไม่ได้มีการตรวจสอบมาก่อน หากว่ามีการสร้างในรูปแบบ RTF หรือ HTML

2. สำเนาข้อความของการทดสอบไวรัสมาตรฐาน หรือไวรัสที่มีการดัดแปลงเข้าไปในตัวข้อความ หรือแนบไฟล์การทดสอบไวรัสลงในข้อความ
3. ส่งข้อความไม่หาผู้ดูแล

โปรแกรมจะทำการตรวจจับวัตถุ ระบุว่ามีการติดเชื้อและทำการสกัดกัน

การตั้งค่าไฟล์แอนตี้ไวรัสให้สมบูรณ์

- เพื่อทำการยืนยันไฟล์แอนตี้ไวรัสให้สมบูรณ์ต้องทำการตั้งค่าให้ถูกต้องต่อไปนี้
1. สร้างโพลเดอร์ลงบนดิสก์ และสำเนาโพลเดอร์การทดสอบไวรัส EICAR ที่ได้ดาวน์โหลดลงไป และไวรัสที่คุณทำการสร้างขึ้น
 2. ตรวจสอบเหตุการณ์ที่บันทึกไว้ ไฟล์การรายงานจะเก็บสะสมเอาไว้ทั้งวัตถุที่มีความเสียหาย และวัตถุที่ไม่ได้รับการตรวจสอบเนื่องเพราะความผิดพลาด
 3. ทำการทดสอบไวรัส หรือเวอร์ชันที่มีการดัดแปลง

ไฟล์แอนตี้ไวรัสที่แทรกเข้ามาในไฟล์ ให้ทำการตรวจสอบ และดำเนินการระบุลงในการติดตั้ง โดยการเลือกการกระทำที่แตกต่างกัน เพื่อทำการตรวจจับวัตถุ ท่านสามารถเลือกดำเนินการตรวจสอบเต็มรูปแบบของการดำเนินการของส่วนประกอบ

ท่านสามารถดูข้อมูลเกี่ยวกับผลของการดำเนินการไฟล์แอนตี้ไวรัสในรายงานการดำเนินการของส่วนประกอบ

การตั้งการตรวจสอบไวรัสให้สมบูรณ์

- เพื่อเป็นการยืนยันการทำงานตรวจสอบไวรัสที่ถูกต้องการดำเนินการต่อไปนี้
 1. สร้างไฟล์เคอร์ลงบนดิสก์ และสำเนาไฟล์เคอร์ทดสอบไวรัส EICAR ที่ได้ดาวน์โหลดไป และไวรัสที่คุณทำการสร้างขึ้น
 2. สร้างงานการตรวจสอบไวรัสใหม่ และเลือกไฟล์เคอร์เพื่อการตั้งการทดสอบไวรัส ที่วัตถุตรวจสอบ
 3. ตรวจสอบเหตุการณ์ที่บันทึกไว้ ไฟล์การรายงานจะเก็บสะสมเอาไว้ทั้งวัตถุที่มีความเสียหาย และวัตถุที่ไม่ได้รับการตรวจสอบเนื่องจากความผิดพลาด
 4. ดำเนินการงานตรวจสอบไวรัส

เมื่อดำเนินการตรวจสอบงานอยู่ การกระทำได้กำหนดไว้ในการตั้งค่างานที่จะตรวจจับวัตถุที่ต้องสงสัยหรือมีการติดเชื้อ โดยการเลือกการกระทำต่างๆ เพื่อการตรวจจับวัตถุ ท่านสามารถทำการตรวจสอบการดำเนินการได้อย่างเต็มทุกส่วนประกอบ

ท่านสามารถดูข้อมูลเกี่ยวกับผลของการดำเนินการไฟล์แอนตี้ไวรัสในรายงานการดำเนินการของ
ส่วนประกอบ

การตั้งการตรวจสอบแอนตี้สแปมให้สมบูรณ์

ท่านสามารถทำการทดสอบข้อความที่ระบุว่าเป็นสแปม ได้จากการทดสอบการป้องกันแอนตี้
สแปม

ข้อความที่ใช้ในการทดสอบมีดังต่อไปนี้

Spam is bad do not send it

หลังจากเครื่องคอมพิวเตอร์ได้รับข้อความ โปรแกรมก็จะทำการตรวจสอบสถานะการทำงานของส
แปม และดำเนินการจัดการต่อสแปม

สถานะการสะสมข้อมูลทางเครือข่ายความปลอดภัยคาร์ปาสกี

บทนำ

โปรดอ่านด้วยความระมัดระวัง ข้อมูลส่วนนี้เป็นส่วนที่สำคัญที่ท่านควรรับทราบก่อนการใช้บริการ และสินค้าของเรา โดยการที่ท่านจะต้องยอมรับในข้อความการสะสมข้อมูลทางเครือข่ายความปลอดภัยคาร์ปาสกี เราขอสงวนสิทธิ์ในการเปลี่ยนแปลงข้อมูลในถ้อยแถลงนี้เมื่อใด หรือส่วนหนึ่งส่วนใดก็ได้ โปรดตรวจสอบวันที่ในการปรับปรุงการถ้อยแถลงนี้ด้านล่าง เพื่อการตัดสินใจหากว่ามีการเปลี่ยนแปลงนโยบายใดๆ ในตอนที่ท่านทบทวนดูครั้งล่าสุด การใช้งานส่วนหนึ่งส่วนใดของการบริการคาร์ปาสกีแลป

คาร์ปาสกีแลปและบริษัทในเครือ (เรียกว่า “คาร์ปาสกีแลป”) สร้างถ้อยแถลงการสะสมข้อมูล เพื่อแจ้งและเปิดเผยข้อมูลร่วมกันของคาร์ปาสกีแอนตี้ไวรัส และคาร์ปาสกีอินเทอร์เน็ตซีเคียวริตี้

คำจากคาร์ปาสกีแลป

คาร์ปาสกีมีการตกลงร่วมกันอย่างจริงจังในเรื่องของการให้บริการที่เหนือกว่า แก่ลูกค้าของเรา ทั้งหมด และมีเคารพในความกังวลของการเก็บข้อมูล เราเข้าใจดีว่า ท่านอาจมีคำถามในเรื่องของวิธีการในการเก็บข้อมูลเครือข่ายความปลอดภัยของเรา และหลักการในกขเก็บข้อมูล การใช้ข้อมูลที่เป็นของเครือข่ายความปลอดภัย (“ถ้อยแถลงการสะสมข้อมูล” หรือ “ถ้อยแถลง”)

ถ้อยแถลงการสะสมข้อมูลนี้ ประกอบไปด้วยจำนวนรายละเอียดทางเทคนิคและวิธีการ เกี่ยวกับขั้นตอนของการสะสมข้อมูล เรามีการจัดการเพื่อการสะสมข้อมูลที่มีชั้นตอหลัก เพื่อให้ท่านสามารถให้ข้อมูลที่ท่านสนใจ ส่วนสำคัญที่สุดคือ การได้เข้าถึงในสิ่งที่ท่านต้องการ และแบบความคาดหวังของทุกสิ่งที่เราทำเพื่อการสะสมข้อมูล

รายละเอียดและข้อมูลรวบรวมโดยทางคาร์ปาสกีแลป หากท่านมีปัญหาหรือข้อสงสัยสามารถสอบถามได้ที่ support@kaspersky.com

เครือข่ายความปลอดภัยของคาร์ปาสกีคืออะไร

การบริการเครือข่ายคาร์ปาสกีทำให้ผู้ใช้งานสินค้าคาร์ปาสกีแลป มีความสะดวกสบายและลดการเสียเวลาที่จะเกิดจากความเสียหายชนิดใหม่ๆ ที่มุ่งเป้ามายังเครื่องคอมพิวเตอร์ของท่าน เพื่อการระบุถึงภัยคุกคามใหม่ๆ และเพื่อการปรับปรุงการทำงานด้านความปลอดภัยของเรา รวมทั้งการทำงานของสินค้าเครือข่ายความปลอดภัยคาร์ปาสกี รวบรวมความปลอดภัยและข้อมูล โปรแกรมเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้นได้ต่อเครื่องคอมพิวเตอร์ของท่าน และการยอมรับการวิเคราะห์ข้อมูลของคาร์ปาสกีแลป

ข้อมูลเหล่านี้ประกอบไปด้วย ข้อมูลการแสดงผลเกี่ยวกับผู้ใช้ เพื่อประโยชน์ต่อคาร์ปาสกีแลปที่ไม่ได้เพื่อวัตถุประสงค์อื่นใด แต่เพื่อการเพิ่มประสิทธิภาพทางด้านความปลอดภัยให้แก่สินค้า และการปรับปรุงอันดีขึ้นไปต่อโปรแกรมมั่งร้าย ภัยคุกคามและไวรัส คาร์ปาสกีแลป จะเก็บรักษาและปกป้องข้อมูลไว้ในถ้อยแถลงเครือข่ายความปลอดภัย

การรวบรวมข้อมูลทำให้ท่านเป็นส่วนหนึ่งของเครือข่ายความปลอดภัยคาร์ปาสกี ที่มาจากทั่วทุกมุมโลกอย่างปลอดภัย

เกี่ยวกับกฎหมาย

เครือข่ายความปลอดภัยคาร์ปาสกีเกี่ยวข้องกับกฎหมายบางประการ เนื่องจากอาจมีใช้ขอบเขตการตัดสินใจของอำนาจกฎหมายที่แตกต่างกันในแต่ละแห่ง รวมทั้งในสหรัฐอเมริกา คาร์ปาสกีแลปอาจเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากการยินยอมของท่านหากเป็นความต้องการทางกฎหมาย หรือความจำเป็นในการสืบสวนสอบสวน เพื่อป้องกันกษกระทำอันเป็นสิ่งอันตราย ต่อผู้เข้าร่วม ผู้มาเยือน ผู้เกี่ยวข้อง หรือทรัพย์สินของคาร์ปาสกีแลป ตัวอย่างเช่น หากว่าทางสหภาพยุโรปต้องการทราบข้อมูลส่วนบุคคล เพื่อต้องการเก็บรวบรวมข้อมูล การติดต่อทางอิเล็กทรอนิกส์หรือความเป็นส่วนตัว แต่ไม่รวมถึง คำสั่งที่ 2002/58/EC แห่งสภายุโรป และ Council of 12 July 2002 ที่เกี่ยวข้องกับกระบวนการในการเก็บรวบรวมข้อมูลส่วนบุคคล และการป้องกันความเป็นส่วนบุคคลในส่วนของ การติดต่อสื่อสารทางอิเล็กทรอนิกส์ และ คำสั่งที่ 95/46/EC แห่งสภายุโรป และ Council of 24 October 1995 ในเรื่องของการป้องกันความเป็นส่วนบุคคลอันเนื่องมาจากกระบวนการในการเก็บข้อมูล และการเคลื่อนไหวโดยอิสระ ของข้อมูลตามลำดับที่

ออกตามตัวบทกฎหมายในสมาชิกสหภาพยุโรป คำตัดสินของคณะกรรมาธิการยุโรป 497/2001/EC ในเรื่องของการมาตรการทางสัญญามาตรฐาน (การโอนถ่ายข้อมูลส่วนบุคคลไปยังประเทศที่สาม) ที่ออกตามตัวบทกฎหมายในสมาชิกสหภาพยุโรป

เครือข่ายความปลอดภัยคาร์ปาสก็์จะทำการแจ้งให้ผู้ใช้ทราบ ตั้งแต่เริ่มต้นการรวบรวมข้อมูลที่กำลังมา แล้วข้างต้น เพื่อใช้ในการพัฒนาทางธุรกิจ หรือการแบ่งปันข้อมูลใดๆ และอนุญาตให้ผู้ใช้เหล่านี้เลือกที่จะเข้าร่วม (ในสมาชิกสหภาพยุโรปและประเทศอื่นๆ ที่มีความต้องการเข้าร่วมกระบวนการนี้) หรือเลือกที่จะไม่เข้าร่วม (สำหรับประเทศอื่นๆทั้งหมด) ออนไลน์จากการใช้งานข้อมูลเหล่านี้ทางการค้า และ/หรือการโอนถ่ายข้อมูลให้กับบุคคลที่สาม

คาร์ปาสก็์แลปมีผลบังคับด้วยตัวกฎหมาย หรือคำตัดสินอื่นใดทางกฎหมาย ในเรื่องความสามารถในการระบุตัวตนเพื่อให้ถูกต้องตามอำนาจแห่งการปกครอง หากมีกฎหมายหรือคำตัดสินทางกฎหมายบังคับให้ทำการจัดหาข้อมูลเหล่านี้ เพื่อความถูกต้องทางด้านเอกสาร คาร์ปาสก็์แลปอาจต้องจัดหาข้อมูลเหล่านี้เพื่อให้เป็นไปตามอำนาจบังคับของกฎหมาย ในการปกป้องสิทธิ สุขภาพความปลอดภัยของบุคคลตามกฎหมายแห่งสหภาพยุโรป การบริการเครือข่ายคาร์ปาสก็์ที่เข้าถึงเกี่ยวกับประกาศ

ข้อมูลที่รวบรวม

ข้อมูลที่เราเก็บรวบรวม

การบริการเครือข่ายความปลอดภัยคาร์ปาสก็์จะเก็บข้อมูลที่ได้รับมาครั้งแรก และข้อมูลเพิ่มเติมที่คาร์ปาสก็์แลป เกี่ยวกับเรื่องของความเสียหายความปลอดภัยที่อาจเกิดขึ้นได้ต่อเครื่องคอมพิวเตอร์ท่าน

ข้อมูลที่ได้รับมาในครั้งแรก

- ข้อมูลเกี่ยวกับซอฟต์แวร์ ฮาร์ดแวร์ และเครื่องคอมพิวเตอร์ของท่าน ประกอบไปด้วยระบบปฏิบัติการ และแพ็คเกจบริการที่ติดตั้ง เคอเนล ไดรเวอร์ เซอร์วิส ส่วนขยาย Internet Explorer การพิมพ์ Window Explorer ไฟล์ที่ทำการดาวน์โหลด ตัวติดตั้งกำลังทำงาน ส่วน

ควบคุมแพ่ง บันทึกการลงทะเบียนและโฮสต์ IP address บราวเซอร์ โปรแกรมบริการอีเมล และเวอร์ชันของคาร์ปาสกี เป็นข้อมูลทั่วไปที่ไม่ใช่ข้อมูลส่วนบุคคล

- เลขประจำตัวเฉพาะ ที่สร้างขึ้นจากผลิตภัณฑ์ของคาร์ปาสกี เพื่อระบุตัวตนของเครื่องมือ โดยไม่มีการระบุผู้ใช้และไม่มีข้อมูลส่วนบุคคล
- ข้อมูลเกี่ยวกับสถานะของการป้องกันไวรัสของเครื่องคอมพิวเตอร์ของท่าน และข้อมูลไฟล์ใดๆ หรือกิจกรรมที่น่าสงสัยว่าจะเป็นโปรแกรมมัลแวร์ (เช่น ชื่อไวรัส วันที่ เวลาของการตรวจจับได้ ชื่อและขนาดของไฟล์ IP หรือพอร์ทที่ถูกโจมตี ชื่อของโปรแกรมที่สงสัยว่าจะเป็นโปรแกรมมัลแวร์) ข้อมูลที่เก็บรวบรวมข้างต้นไม่ได้มีข้อมูลที่มีการระบุผู้ใช้และไม่มีข้อมูลส่วนบุคคล

ข้อมูลขยาย

- ข้อมูลเกี่ยวกับโปรแกรมที่ทำการดาวน์โหลดโดยผู้ใช้ (URL, ขนาดไฟล์, ชื่อสกุล)
- ข้อมูลเกี่ยวกับโปรแกรมทำการ (ขนาด รายละเอียดของข้อมูล วันที่สร้าง ข้อมูลเกี่ยวกับ PE headers ภูมิภาค ชื่อ สถานที่ โปรแกรมบีบอัดที่ใช้)

ความปลอดภัยของข้อมูลที่เก็บไว้และการส่งข้อมูล

คาร์ปาสกีแลปรับรองว่า จะทำการรักษาข้อมูลที่เป็นความปลอดภัย ข้อมูลที่เก็บรวบรวมจะรักษาเอาไว้ในเซิร์ฟเวอร์ที่มีการควบคุมการเข้าถึง คาร์ปาสกีแลปจะทำการรักษาข้อมูลโดยใช้ไฟร์วอลล์มาตรฐาน และระบบการป้องกันรหัสผ่าน คาร์ปาสกีแลปใช้เทคโนโลยีด้านความปลอดภัยในพิสัยกว้าง และมีวิธีการดำเนินการด้านการรักษาข้อมูลที่เก็บรวบรวมได้ คาร์ปาสกีแลป มีความมั่นใจในขั้นตอนของการดำเนินการที่มีต่อข้อมูลของท่าน ตามคำกล่าวในถ้อยแถลงนี้ แต่ไม่มีอะไรที่จะรับประกันได้เต็มร้อยถึงการรักษาความปลอดภัยของข้อมูล ไม่ว่าจะเป็นการเก็บ การส่งต่อข้อมูลจากท่านถึงเราหรือจากที่เราส่งบริการไปหาท่าน รวมทั้งขีดจำกัดทางด้านความปลอดภัยของการให้บริการเครือข่ายคาร์ปาสกี ที่อาจต้องได้รับความเสียหายที่เกิดขึ้นได้

ข้อมูลที่ทำกรเก็บรวบรวมนี้ จะเป็นไว้ในเซิร์ฟเวอร์ของคาร์ปาสกีแลป และคาร์ปาสกีแลป ไม่จำเป็นต้องทำการเตือนล่วงหน้าในเรื่องของความปลอดภัยต่อข้อมูล หากว่าการส่งข้อมูลที่ได้รับมีระดับการป้องกันที่เหมาะสม เราเก็บรักษาข้อมูลเอาไว้ในฐานะที่เป็นข้อมูลความลับ วิธีการในการรักษาความลับและนโยบายการทำงานของบริษัทเกี่ยวกับเรื่องของการป้องกันและการใช้งานของข้อมูลที่เป็นความลับ หลังจากได้ทำการรวบรวมข้อมูลแล้ว เซิร์ฟเวอร์จะมีการเก็บรักษาเอาไว้ทั้งทางกายภาพและทางอิเล็กทรอนิกส์ ที่มีกระบวนการใช้งานรหัสผ่านและบัญชีเข้ารหัส รวมทั้งการรักษาด้วยไฟลัวอลที่กั้นการเข้าถึงโดยไม่ได้รับอนุญาตจากภายนอก ข้อมูลที่ทำกรสะสมโดยเครือข่ายความปลอดภัยคาร์ปาสกี คำนินการและเก็บรวบรวมไว้ที่สหรัฐอเมริกา และทางกฎหมายอื่นๆ และรวมถึงประเทศอื่นๆที่คาร์ปาสกีแลปเข้าไปทำธุรกิจ พนักงานของคาร์ปาสกีทั้งหมดตระหนักดีถึงนโยบายความปลอดภัย ข้อมูลของท่านที่พนักงานเหล่านั้นเข้าถึง จะต้องมาจากการเข้าถึงในหน้าที่การงาน ข้อมูลที่รวบรวมเอาไว้จะไม่มีการเชื่อมโยงไปยังข้อมูลส่วนบุคคล คาร์ปาสกีแลปจะไม่รวมเอาข้อมูลเหล่านั้นมาไว้ด้วยกันไม่ว่าจะเป็น รายการติดต่อ ข้อมูลการเป็นสมาชิก ที่รวบรวมโดยคาร์ปาสกีแลปเพื่อวัตถุประสงค์อื่น

การใช้งานข้อมูลที่เก็บรวบรวม

เราใช้ข้อมูลส่วนบุคคลท่านอย่างไร

คาร์ปาสกีแลป ทำการเก็บรวบรวมข้อมูลของท่าน เพื่อการวิเคราะห์ ระบุแหล่งของการเกิดความเสียหายต่อความปลอดภัย และปรับปรุงความสามารถในการทำงานของผลิตภัณฑ์คาร์ปาสกีแลป เพื่อการสืบค้นพฤติกรรมมั่วร้าย เว็บไซต์หลอกลวง โปรแกรมอาชญากร และภัยคุกคามประเภทอื่นบนอินเทอร์เน็ต ในระดับที่ดีที่สุดเพื่อการปกป้องของคาร์ปาสกีแลปในอนาคต

การเปิดเผยข้อมูลให้แก่บุคคลที่สาม

คาร์ปาสกีแลปอาจเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากการยินยอมของท่านหากเป็นความต้องการทางกฎหมาย หรือความจำเป็นในการสืบสวนสอบสวน เพื่อป้องกันการกระทำอันเป็นอันตรายต่อผู้เข้าร่วม ผู้มาเยือน ผู้เกี่ยวข้องหรือทรัพย์สินของคาร์ปาสกีแลป ในส่วนของเงื่อนไขและข้อตกลงกับทางบริษัท หรือปกป้องความปลอดภัยแก่ผู้ใช้ และสาธารณะหรือภายใต้ข้อตกลงทางลิขสิทธิ์กับบุคคลที่สาม ที่

เข้าร่วมการพัฒนา ปฏิบัติการ หรือรักษาเครือข่ายความปลอดภัยคาร์ปาสกี เพื่อการส่งเสริมการตระหนักรู้ การค้นหาและการป้องกันภัยทางอินเทอร์เน็ต คาร์ปาสกีแลกเปลี่ยนอาจต้องทำการแบ่งปันข้อมูลกับองค์กรการวิจัย และผู้ขายซอฟต์แวร์อื่นๆ คาร์ปาสกีแลกเปลี่ยนอาจใช้สถิติที่ได้จากข้อมูลที่เก็บรวบรวมและทำการตีพิมพ์รายงาน แนวโน้มความเสี่ยงด้านความปลอดภัย

ทางเลือกของท่าน

ท่านมีสิทธิเลือกในการเข้าร่วมเป็นส่วนหนึ่งของเครือข่ายความปลอดภัยคาร์ปาสกี คุณสามารถทำการเริ่มต้นหรือเลิกได้ตลอดเวลา โดยการเข้าไปยังส่วนการตั้งค่าตอบกลับ ในตัวเลือกบนหน้าของคาร์ปาสกีแลกเปลี่ยน

เมื่อระยะเวลาของการบริการของคาร์ปาสกีแลกเปลี่ยนสิ้นสุดลง การทำงานของคาร์ปาสกีซอฟต์แวร์อาจดำเนินต่อไปในบางอย่าง แต่การส่งข้อมูลถึงคาร์ปาสกีแลกเปลี่ยนจะสิ้นสุดลง

เรามีสิทธิที่จะส่งข้อความเตือนไปยังผู้ใช้เพื่อแจ้งการเปลี่ยนแปลงเฉพาะ ที่อาจเกิดผลกระทบต่อความสามารถในการทำงานและการบริการของเรา ที่มีอยู่ก่อนหน้านี้ เรามีสิทธิในการติดต่อกับท่านในส่วนการดำเนินการทางด้านกฎหมาย การฝ่าฝืนในเรื่องของการใช้งานทางลิขสิทธิ์ การรับประกันและสัญญาการซ้ขาย

คาร์ปาสกีแลกเปลี่ยนสงวนรักษาสิทธิ์เนื่องมาจากข้อจำกัดบางกรณี ที่อาจทำการติดต่อกับท่านอันเป็นสิ่งสำคัญสำหรับท่าน อันไม่เกี่ยวกับด้านการตลาดและการออกคำสั่งที่ไม่ค่อยมีการติดต่อสื่อสาร

การสะสมข้อมูลในเรื่องของคำถามและข้อติชม

คาร์ปาสกีแลกเปลี่ยนมีความตั้งใจจริงในอันที่จะรับฟังข้อคิดเห็น คำถาม หรือคำติชมจากผู้ใช้งาน โดยการส่งอีเมลเรื่องข้อคิดเห็น คำถาม หรือคำติชม ที่เกี่ยวกับคาร์ปาสกีแลกเปลี่ยนมาที่ support@kaspersky.com

อธิบายข้อความรายละเอียดให้ชัดเจนที่สุด เราจะทำการตอบในทุกข้อคิดเห็น คำถาม หรือคำติชม

ผู้ใช้งานสามารถยกเลิกการใช้งานด้านการสะสมข้อมูลได้ตลอดเวลา โดยการเข้าไปยังส่วนของ "Feedback" บนหน้า "Settings" ของผลิตภัณฑ์คาร์ปาสกีใดๆ

สงวนลิขสิทธิ์ 2008 คาร์ปาสกีแลป

คาร์ปาสกีแลป

คาร์ปาสกีแลปผู้นำแห่งเทคโนโลยีความปลอดภัยทางด้านข้อมูล ก่อตั้งขึ้นเมื่อปี 2540 ผลิตซอฟต์แวร์ที่มีประสิทธิภาพสูงในการทำงานเป็น แอนตี้ไวรัส แอนตี้สแปม และแอนตี้ระบบแฮกเกอร์

คาร์ปาสกีแลปเป็นบริษัทนานาชาติ สำนักงานใหญ่อยู่ที่สหพันธรัฐรัสเซีย มีสำนักงานอยู่ที่ สหราชอาณาจักร ฝรั่งเศส เยอรมัน ญี่ปุ่น เบนลักซ์ จีน โปแลนด์ โรมาเนีย และสหรัฐอเมริกา (แคลิฟอร์เนีย) สำนักงานใหม่เป็นสำนักงานการวิจัยแอนตี้ไวรัส ในประเทศฝรั่งเศส มีกว่า 500 ประเทศจากทั่วโลกที่เป็นพันธมิตรกับคาร์ปาสกี

ปัจจุบันนี้ พนักงานในคาร์ปาสกีแลปกว่า 450 คนที่ เป็นผู้เชี่ยวชาญ ในระดับปริญญาโทกว่าสิบคน ปริญญาเอก 16 คน ผู้เชี่ยวชาญในคาร์ปาสกีแลปส่วนหนึ่งเป็นสมาชิกอาวุโสขององค์กรนักวิจัยแอนตี้ไวรัส คอมพิวเตอร์ (CARO)

สินทรัพย์ของเราคือผู้เชี่ยวชาญที่ร่วมกันทำงานต่อต้านไวรัสมากกว่า 14 ปี การวิเคราะห์ไวรัส คอมพิวเตอร์ ตลอดจนการวิเคราะห์กิจกรรมของไวรัสโดยผู้ชำนาญการของบริษัท ที่มองเห็นเหตุการณ์ ล่วงหน้าของการพัฒนาทางด้านโปรแกรมมิ่งร้าย การต่อต้านการรุกรานในอนาคตที่เป็นพื้นฐานของสินค้า คาร์ปาสกี สินค้าของบริษัทยังคงส่งต่อไปยังผู้ค้าเพื่อทำการคุ้มครองลูกค้าของเรา

ตลอดหลายปีที่ทำงานหนักเพื่อให้บริษัทก้าวเป็นบริษัทแอนตี้ไวรัสอันดับหนึ่งของโลก คาร์ปาสกี แลปเป็นบริษัทแห่งแรกที่ทำ การพัฒนาทางด้านซอฟต์แวร์แอนตี้ไวรัสที่มีมาตรฐานทันสมัย เป้าหมายสำคัญ ของบริษัทคาร์ปาสกี คือการผลิตสินค้าที่เต็มไปด้วยมาตรฐานแห่งการป้องกัน แก่เครือข่ายและสถานีการทำงาน ไฟล์เซิร์ฟเวอร์ ระบบเมล์ ไฟร์วอลล์ ช่องทางอินเทอร์เน็ต และคอมพิวเตอร์พกพา ให้ง่ายต่อการ จัดการสำหรับเครื่องคอมพิวเตอร์และเครือข่าย ผู้ผลิตที่มีชื่อเสียงจำนวนมากเลือกใช้งานคาร์ปาสกี อย่างเช่น Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybaris (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada)

ลูกค้าของคาร์ปาสกีแลป ได้รับบริการเสริมเพิ่มเติมที่มั่นคง ในบริษัทที่มั่นคง ผลิตภัณฑ์ของบริษัท ตามความต้องการของธุรกิจ เราออกแบบให้มีการทำงานและสนับสนุนการใช้งานแอนติไวรัสในที่อัน ซับซ้อน ฐานข้อมูลของคาร์ปาสกีแลปมีการอัปเดตทุกชั่วโมง รวมทั้งการมีหน่วยสนับสนุนทางเทคนิค ตลอด 24 ชั่วโมง

เนื้อหาในส่วนนี้ประกอบไปด้วย

ผลิตภัณฑ์อื่นๆ ของคาร์ปาสกี

ติดต่อเรา

ผลิตภัณฑ์อื่นๆ ของคาร์ปาสกี

หน่วยข่าวของคาร์ปาสกีแลป

โปรแกรมหน่วยข่าวของคาร์ปาสกีแลปเป็นการดำเนินการด้านข่าวสารที่รวดเร็วของคาร์ปาสกีแลป ในอันที่จะแจ้งให้ทราบถึงเรื่องของการเกิดไวรัส และเหตุการณ์ล่าสุด โปรแกรมทำการอ่านรายการช่องข่าว ที่มีอยู่และข้อมูลที่ประกอบขึ้น จากเซิร์ฟเวอร์ข่าวคาร์ปาสกีที่มีช่วงเวลาเหตุการณ์

นอกจากนี้หน่วยงานยังให้ผู้ใช้ทำได้ต่อไปนี้

- มองเห็นสภาพของไวรัสในระบบแพคเกจควบคุม
- บอกรับหรือปฏิเสธการรับข่าวจากช่องทางของคาร์ปาสกีแลป
- รับข่าวในแต่ละช่องทางที่บอกรับด้วยการเลือกจากความถี่ในการบอกรับ หรือการเลือกเพิ่มเติมสำหรับข่าวที่ยังไม่ได้อ่าน
- ดูข่าวบนช่องทางที่บอกรับ
- ดูรายการของช่องทางบนสถานะของช่องทาง

- เปิดหน้าบราวเซอร์เพื่อดูรายละเอียดของข่าว

หน่วยข่าวสามารถทำงานได้บน **Microsoft Windows** และยังสามารถลงบนโปรแกรมเดี่ยวอื่นๆ อีก รวมทั้งการแก้ปัญหาที่รวมกันของคาร์ปาสกีแลป

Kaspersky® Online Scanner

โปรแกรมนี้เป็นโปรแกรมฟรีใช้กับผู้ที่เข้ามาเยี่ยมชมเว็บไซต์ของบริษัท แล้วโปรแกรมจะทำการตรวจจับไวรัสที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ของผู้ที่เข้ามาเยี่ยมชม และทำการกำจัดไวรัสเหล่านั้นออนไลน์ Kaspersky® Online Scanner ทำงานบนบราวเซอร์ และทำการตัดสินใจว่ามีใครเป็นโปรแกรมมุงร้าย ในการตรวจจับผู้ใช้งานสามารถทำได้ดังต่อไปนี้

- แยกตัวเก็บและฐานข้อมูลของแม่ล่ออกจากการตรวจสอบ
- ใช้ฐานข้อมูลมาตรฐานและฐานข้อมูลเพิ่มเติมในการตรวจสอบ
- บันทึกผลการตรวจจับไว้ในไฟล์txt หรือ html

Kaspersky® Online Scanner Pro

โปรแกรมนี้เป็นโปรแกรมบอกรับเป็นสมาชิก ใช้กับผู้ที่เข้ามาเยี่ยมชมเว็บไซต์ของบริษัท แล้วโปรแกรมจะทำการตรวจจับไวรัสที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ของผู้ที่เข้ามาเยี่ยมชม และทำการกำจัดไวรัสเหล่านั้นออนไลน์ Kaspersky® Online Scanner Pro ทำงานได้โดยตรงบนบราวเซอร์ ในการตรวจจับผู้ใช้งานสามารถทำได้ดังต่อไปนี้

- แยกตัวเก็บและฐานข้อมูลของแม่ล่ออกจากการตรวจสอบ
- ใช้ฐานข้อมูลมาตรฐานและฐานข้อมูลเพิ่มเติมในการตรวจสอบ
- ทำการกำจัดไวรัสเมื่อพบการติดเชื้อ
- บันทึกผลการตรวจจับไว้ในไฟล์txt หรือ html

Kaspersky Anti-Virus® Mobile

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

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

Kaspersky Anti-Virus for File Servers

ชุดซอฟต์แวร์นี้ เพื่อให้ความมั่นใจในการปกป้องโปรแกรมมัลแวร์สำหรับระบบไฟล์ของเซิร์ฟเวอร์ ที่ดำเนินการบน Microsoft Windows, Novell NetWare และระบบปฏิบัติการ Linux ชุดซอฟต์แวร์นี้ ประกอบไปด้วย

- 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

ความสามารถในการทำงานและประโยชน์

- การปกป้องแบบเรียลไทม์แก่ระบบไฟล์ของเซิร์ฟเวอร์ ไฟล์ของเซิร์ฟเวอร์ทั้งหมดจะได้รับการตรวจสอบเมื่อมีการเปิดการทำงาน หรือการบันทึกลงบนเซิร์ฟเวอร์
- การป้องกันการเกิดไวรัสแบบกระตั้นหัน
- การตรวจสอบไฟล์ระบบทั้งหมดตามความต้องการ หรือ ไฟล์หรือโพลเดอร์แยก
- ใช้เทคโนโลยีสูงสุดในการตรวจสอบวัตถุของระบบไฟล์ของเซิร์ฟเวอร์
- กู้คืนระบบหลังจากการติดเชื้อ
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- รักษาความสมดุลของการไหลคในระบบ (Load balance)
- สร้างรายการนำเชื่อถือ ต่อกิจกรรมที่เกิดขึ้นในเซิร์ฟเวอร์เพื่อไม่ต้องเฝ้าระวังในรายการนี้
- การควบคุมระยะไกล รวมทั้งการติดตั้งจากส่วนกลาง การตั้งค่าและการจัดการ
- เก็บสำเนาข้อมูลสำรองของวัตถุที่ลบทิ้งหรือติดเชื้อในกรณีต้องการกู้คืน
- แยกวัตถุที่ต้องสงสัยยังพื้นที่เก็บพิเศษ
- รักษารายงานอย่างละเอียด
- อัปเดตฐานข้อมูลอย่างอัตโนมัติของชุดซอฟต์แวร์

Kaspersky Open Space Security

Kaspersky Open Space Security เป็นชุดซอฟต์แวร์ด้านความปลอดภัยตัวใหม่ที่ตรงกับ
 เครื่องข่ายบริษัทที่มีความทันสมัยในทุกรูปแบบ และให้การปกป้องส่วนกลางของระบบข้อมูลและการ
 ควบคุมออฟฟิศระยะไกล รวมทั้งผู้ใช้งานเคลื่อนที่

ชุดซอฟต์แวร์ประกอบไปด้วย

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

คำอธิบายของแต่ละผลิตภัณฑ์มีดังต่อไปนี้

Kaspersky Work Space Security เป็นผลิตภัณฑ์ ที่ออกแบบมาเพื่อการปกป้องส่วนกลางสำหรับ
 สถานีการทำงานในเครือข่ายองค์กรและอื่นๆ เพื่อการต่อต้านภัยคุกคามทางอินเทอร์เน็ตสมัยใหม่อย่างเช่น
 ไวรัส สปายแวร์ การบุกรุก และสแปม

ความสามารถในการทำงานและประโยชน์

- ป้องกันจากไวรัส สปายแวร์ การบุกรุก และสแปม อย่างเต็มรูปแบบ
- ปกป้องก่อนการเกิด โปรแกรมมัลแวร์ร้ายตัวใหม่
- ไฟร์วอลล์ส่วนบุคคลด้วยระบบการตรวจจับผู้บุกรุก และป้องกันการจู่โจมระบบ
- ย้อนกลับไปที่ก่อนการเกิด โปรแกรมมัลแวร์ร้ายทำลายระบบ
- ปกป้องการจู่โจมแบบฟิชซิงและสแปม

- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- ตรวจสอบกราฟฟิคอีเมลล์และอินเทอร์เน็ตในแบบเรียลไทม์
- สกัดกั้นหน้าต่างแสดงโฆษณาและแบนเนอร์อินเทอร์เน็ต
- ให้ความปลอดภัยด้านการทำงานกับเครือข่าย ประเภทไวไฟ
- มีเครื่องมือในการกู้ข้อมูลหลังจากการโจรกรรมจากไวรัส
- ระบบที่พัฒนาเต็มรูปแบบในการรายงานเกี่ยวกับสถานะการปกป้อง
- อัปเดตฐานข้อมูลช่องอัต โนมัติ
- 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 ป้องกันการเกิดไวรัสแบบกระตั้นหัน และความมั่นใจต่อความปลอดภัยของข้อมูล และการเข้าถึงแหล่งทรัพยากรเครือข่ายในทันที

ความสามารถในการทำงานและประโยชน์

- ระบบการจัดการระยะไกลของโปรแกรม ทำให้สามารถจัดการ และตั้งค่า รวมทั้งติดตั้งโปรแกรมได้ในระยะไกล
- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- ปกป้องสถานีการทำงานและไฟล์เซิร์ฟเวอร์จากภัยคุกคามทางอินเทอร์เน็ตทุกประเภท
- กระจายการ โหลดระหว่างตัวดำเนินการของเซิร์ฟเวอร์
- แยกโปรแกรมมุ่งร้ายออกไปเก็บที่พิเศษ
- กู้คืนระบบหลังจากการติดเชื้
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- รักษาความสมดุลของการโหลดในระบบ (Load balance)
- สร้างรายการนำเชื่อถือ ต่อกิจกรรมที่เกิดขึ้นในเซิร์ฟเวอร์เพื่อไม่ต้องเฝ้าระวังในรายการนี้
- การควบคุมระยะไกล รวมทั้งการติดตั้งจากส่วนกลาง การตั้งค่าและการจัดการ
- เก็บสำเนาข้อมูลสำรองของวัตถุที่ลบทิ้งหรือติดเชื้ในกรณีต้องการกู้คืน
- แยกวัตถุที่ต้องสงสัยยังพื้นที่เก็บพิเศษ
- รักษารายงานอย่างละเอียด
- อัปเดตฐานข้อมูลอย่างอัตโนมัติของชุดซอฟต์แวร์

Kaspersky Enterprise Space Security

โปรแกรมนี้ใช้เพื่อการปกป้องสถานีการทำงาน และกลุ่มเซิร์ฟเวอร์เพื่อป้องกันประเภทของไวรัส โปรแกรมโทรจันและหนอนอินเทอร์เน็ต ป้องกันการเกิดไวรัสแบบกระตั้นหัน และความมั่นใจต่อความปลอดภัยของข้อมูล และการเข้าถึงแหล่งทรัพยากรเครือข่ายในทันที

ความสามารถในการทำงานและประโยชน์

- ปกป้องสถานีการทำงาน และกลุ่มเซิร์ฟเวอร์เพื่อป้องกันประเภทของไวรัส โปรแกรมโทรจันและหนอนอินเทอร์เน็ต ป้องกันการเกิดไวรัสแบบกระตั้นหัน
- ปกป้องซอฟต์แวร์เมลเซิร์ฟเวอร์ รวมทั้งSendmail, Qmail, Postfix และ Exim
- ตรวจสอบข้อความทั้งหมดในMicrosoft Exchange server รวมทั้งโพลเดอรร่วม
- ดำเนินการกับข้อความ ฐานข้อมูล และวัตถุอื่นๆของLotus Domino servers
- ป้องกันการเกิดฟิชชิ่งและสแปม
- ป้องกันการเกิดมัลแวร์และไวรัสกระตั้นหัน
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- ระบบการจัดการระยะไกลของโปรแกรม ทำให้สามารถจัดการ และตั้งค่า รวมทั้งติดตั้งโปรแกรมได้ในระยะไกล
- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- ไฟร์วอลล์ส่วนบุคคลด้วยระบบการตรวจจับผู้บุกรุก และป้องกันการโจมตีระบบ
- ให้ความปลอดภัยภายในเครือข่ายระบบไร้สายไวไฟ

- ตรวจสอบกราฟฟิกลงในอินเทอร์เน็ตแบบเรียลไทม์
- คุ้มกันระบบหลังจากการติดเชื้อ
- จัดสรรพื้นที่แบบไดนามิกแก่แหล่งทรัพยากรระหว่างการตรวจสอบ
- แยกโปรแกรมมัลแวร์ออกไปเก็บที่พิเศษ
- ระบบที่พัฒนาเต็มรูปแบบในการรายงานเกี่ยวกับสถานะการปกป้อง
- อัปเดตฐานข้อมูลของแฮกเกอร์อัตโนมัติ

Kaspersky Total Space Security

โปรแกรมนี้เป็นที่ควบคุมกระแสเข้าออกของข้อมูล อีเมลล์ กราฟฟิกลงเว็บ และการปฏิสัมพันธ์การทำงานทั้งหมดของเครือข่าย มีส่วนผสมของการปกป้องสถานีการทำงานและอุปกรณ์เคลื่อนที่ เพื่อความมั่นใจในความปลอดภัยของผู้ใช้ในองค์กรบนอินเทอร์เน็ต และรับประกันได้ถึงความมั่นใจในการสื่อสารทางเมลล์

ความสามารถในการทำงานและประโยชน์

- การปกป้องที่ครอบคลุมในเรื่องของไวรัส การโจมตีมัลแวร์ และสแปมในระดับของเครือข่ายบริษัท จากสถานีการทำงานถึงเกตเวย์
- ปกป้องก่อนการเกิด โปรแกรมมัลแวร์ตัวใหม่ในสถานีการทำงาน
- ปกป้องเมลล์เซิร์ฟเวอร์และแชร์เซิร์ฟเวอร์
- การตรวจสอบแบบเรียลไทม์ ของกราฟฟิกลงเว็บภายใน (HTTP / FTP)
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่

- สกัดกั้นการทำงานจากสถานีการทำงานที่ติดเชื่อ
- ป้องกันการเกิดไวรัสแบบกระตั้นหัน
- การจัดการส่วนกลางในการรายงานสถานะการป้องกัน
- ระบบการจัดการระยะไกลของโปรแกรม ทำให้สามารถจัดการ และตั้งค่า รวมทั้งติดตั้งโปรแกรมได้ในระยะไกล
- สนับสนุนการทำงานของ Cisco® NAC (การควบคุมการอนุญาตเข้าใช้เครือข่าย - Network Admission Control)
- สนับสนุน hardware proxy servers
- กรองทราฟฟิกอินเทอร์เน็ตตามรายการเซิร์ฟเวอร์ที่น่าเชื่อถือ ประเภทของวัตถุและกลุ่มของผู้ใช้
- ใช้เทคโนโลยีของiSwift เพื่อกำหนดการตรวจสอบภายในเซิร์ฟเวอร์
- จัดสรรพื้นที่แบบไดนามิกแก่แหล่งทรัพยากรระหว่างการตรวจสอบ
- ไฟร์วอลล์ส่วนบุคคลด้วยระบบการตรวจจับผู้บุกรุก และป้องกันการโจมตีระบบ
- ให้ความปลอดภัยภายในเครือข่ายระบบไร้สายไวไฟ
- ป้องกันการเกิดฟิชชิ่งและสเปม
- กำจัดไวรัสในระยะไกล(Intel® Active Management technology, component Intel® vPro™)
- กู้คืนระบบหลังจากการติดเชื่อ
- เทคโนโลยีการปกป้องตนเองของโปรแกรมที่มีต่อโปรแกรมม่งร้าย
- สนับสนุนการทำงานของระบบปฏิบัติการ64-bit

- อพเทฐานข้อมูลอย่างอัตโนมัติ

Kaspersky Security for Mail Servers

ชุดซอฟต์แวร์ตัวนี้ป้องกันเมลเซิร์ฟเวอร์และเซิร์ฟเวอร์ การปกป้องเมลเซิร์ฟเวอร์ 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.

ความสามารถในการทำงานและประโยชน์

- การปกป้องที่น่าเชื่อถือในการต่อต้านโปรแกรมมัลแวร์ และ โปรแกรมที่อันตรายทั้งหลาย
- ตัวกรองสแปม
- การตรวจสอบเมลเข้าและออกรวมทั้งไฟล์แนบ
- การตรวจสอบแอนตี้ไวรัสของข้อความทั้งหมดบน Microsoft Exchange server รวมทั้งโฟลเดอร์ที่เปิดร่วม
- การตรวจสอบข้อความ ฐานข้อมูลและวัตถุอื่นๆใน Lotus Domino servers

- การกรองข้อความที่แนบมา
- แยกโปรแกรมมัลแวร์ออกไปเก็บที่พิเศษ
- ระบบการจัดการที่สะดวก
- การป้องกันไวรัสแบบกระทันหัน
- ฝ้าดูสถานะระบบการป้องกัน โดยการแจ้งเตือน
- ระบบการรายงานเกี่ยวกับกาดำเนินการ โปรแกรม
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- อัปเดตฐานข้อมูลอย่างอัตโนมัติ

Kaspersky Security for Gateways

ชุดซอฟต์แวร์นี้ เพื่อให้เกิดความปลอดภัยต่อการเข้าถึงอินเทอร์เน็ตของพนักงานทั้งบริษัท การเคลื่อนย้ายโปรแกรมมัลแวร์อัตโนมัติ และโปรแกรมที่มีความเสี่ยงออกจากข้อมูลที่ได้รับผ่านทางเครือข่าย โปรโตคอล HTTP/FTP การแก้ปัญหาที่ประกอบด้วย

- 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

- การปกป้องที่น่าเชื่อถือในการต่อต้านโปรแกรมมัลแวร์ และ โปรแกรมที่อันตรายทั้งหลาย
- ตรวจสอบทราฟฟิกอินเทอร์เน็ต HTTP/FTP ในโหมดเรียลไทม์

- กรองทราฟฟิกอินเทอร์เน็ต ตามรายการเซิร์ฟเวอร์ที่น่าเชื่อถือ ประเภทของวัตถุและกลุ่มของผู้ใช้
- แยกวัตถุที่ต้องสงสัยไว้ในโพลเดอร์พิเศษ
- ระบบการควบคุมที่สะดวก
- ระบบการรายงานเกี่ยวกับการดำเนินการของโปรแกรม
- สนับสนุนการทำงาน hardware proxy servers
- สามารถเพิ่มหรือลดผลิตภัณฑ์เพื่อให้เหมาะสมกับทรัพยากรของระบบที่มีอยู่
- อพเทชันข้อมูลอย่างอัตโนมัติ

Kaspersky® Anti-Spam

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

Kaspersky® Anti-Spam มีการกระทำที่เรียกว่าการกรองทางเข้า ของเครือข่ายบริษัท ทำการตรวจสอบข้อความเข้าเพื่อหาสแปม โดยสามารถทำงานร่วมกับเครือข่ายของผู้ใช้ที่มีการติดตั้งเมลเซิร์ฟเวอร์เอาไว้

ประสิทธิภาพสูงของโปรแกรม ช่วยให้สามารถทำการอัปเดตได้ทุกวัน กับฐานข้อมูลการกรองเนื้อหา โดยการใช้ตัวอย่าง ที่จัดขึ้นโดยผู้เชี่ยวชาญกว่าสี่ล้านที่ออกมาทุก20 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
ในข้อความเมลล์เข้าและออก

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

เพื่อการสร้างและยืนยันลายเซ็นดิจิทัล คาร์ปาสกีแอนตี้ไวรัสจึงใช้ 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 อันเป็นข้อมูลความลับ ที่ได้รับการออกอนุญาตที่ No. SF/114-0901 เมื่อวันที่ 1 กรกฎาคม 2549

เทคโนโลยีในการเข้ารหัส ถอดรหัส ของขนาดข้อมูลที่มีการกำหนดขอบเขตมีดังต่อไปนี้

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

รูปแบบของไลบรารีจะอยู่ใน ANSI มาตรฐาน C และสามารถเข้าสู่โปรแกรมได้ทั้งรหัสโหนดเคลื่อนไหวและคงที่ ประกอบไปด้วย x86, x86-64, Ultra SPARC II และแพลตฟอร์มที่ทำงานร่วมกันได้ที่

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
ติดต่อทางอีเมลที่ info@cryptoex.ru

มูลนิธิ มอซิลลา

Library Gecko SDK ver. 1.8 ใช้เพื่อการพัฒนาส่วนประกอบของโปรแกรม

โปรแกรมนี้ใช้ตามเงื่อนไขและข้อตกลงของลิขสิทธิ์ MPL 1.1 Public Mozilla Foundation license <http://www.mozilla.org/MPL>.

สำหรับรายละเอียดเพิ่มเติมได้ที่ [library Gecko SDK](http://developer.mozilla.org/en/docs/Gecko_SDK) เว็บไซต์ http://developer.mozilla.org/en/docs/Gecko_SDK. © Mozilla Foundation

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

ข้อตกลงทางลิขสิทธิ์

ข้อตกลงทางลิขสิทธิ์กับผู้ใช้แบบมาตรฐาน

เรียนผู้ใช้ทราบว่า กรุณาอ่านอย่างละเอียดสำหรับข้อตกลงทางกฎหมาย (หรือเรียกว่า “ข้อตกลง”) สำหรับลิขสิทธิ์คาร์ปาสกีอินเทอร์เน็ตซีเคียวริตี้ (หรือเรียกว่า “ซอฟต์แวร์”) ที่ผลิตโดยคาร์ปาสกีแลป (หรือเรียกว่า “คาร์ปาสกีแลป”)

หากว่าท่านทำการซื้อซอฟต์แวร์นี้ผ่านทางอินเทอร์เน็ต โดยคลิกที่ปุ่มตกลงการซื้อ ท่าน (ทั้งที่เป็นบุคคล หรือกลุ่มคณะ) ได้ยินยอมแล้วในการเข้าร่วมเป็นส่วนหนึ่งในข้อตกลงทางลิขสิทธิ์นี้ หากว่าท่านไม่เห็นด้วยตามข้อตกลงนี้ ให้คลิกที่ปุ่ม ไม่ตกลงและไม่ต้องการติดตั้งซอฟต์แวร์นี้

หากว่าท่านทำการซื้อซอฟต์แวร์นี้ผ่านทางตัวแทนการขาย ท่าน (ทั้งที่เป็นบุคคล หรือกลุ่มคณะ) ได้ทำการเปิด CD เรียบร้อยแล้ว จะถือว่าท่านได้ยินยอมแล้วในการเข้าร่วมเป็นส่วนหนึ่งในข้อตกลงทางลิขสิทธิ์นี้ หากว่าท่านไม่เห็นด้วยตามข้อตกลงนี้ท่านจะต้องไม่ทำการเปิด CD คาว์โหนด ติดตั้ง หรือใช้งานซอฟต์แวร์

ตามบทกฎหมาย เนื่องด้วยซอฟต์แวร์คาร์ปาสกี เป็นการใช้งานส่วนบุคคล หากท่านจะซื้อผ่านทางคาร์ปาสกีแลปออนไลน์ หรือเว็บไซต์ของพันธมิตร ลูกค้าย่อมมีเวลา 14 วันหลังจากวันที่ได้รับส่งมอบของเพื่อการคืนสินค้าหรือการคืนเงิน หากยังไม่มีการใช้งานซอฟต์แวร์

เนื่องด้วยซอฟต์แวร์คาร์ปาสกี เป็นการใช้งานส่วนบุคคล หากลูกค้าไม่ได้ซื้อซอฟต์แวร์ผ่านทางออนไลน์อินเทอร์เน็ต ไม่มีการคืนสินค้ายกเว้นทางพันธมิตรมีการกระทำในกรณีตรงข้ามกัน ในกรณีนี้คาร์ปาสกีแลปจะไม่ยึดถือจากตัวบทของพันธมิตร

สิทธิของการคืนสินค้านั้นจะต้องเป็นสินค้าของดั้งเดิมเท่านั้น

การอ้างอิงทั้งหมดถึง “ซอฟต์แวร์” ถือว่ารวมไปถึงรหัสการเริ่มต้นทำงานซอฟต์แวร์ ที่ได้รับมาจากการเป็นส่วนหนึ่งของคาร์ปาสกีแอนตี้ไวรัสของคาร์ปาสกีแลป

1. การอนุญาตทางลิขสิทธิ์ ภายใต้เงื่อนไขการชำระเงินให้กับอายุของลิขสิทธิ์ และภายใต้เงื่อนไขและข้อตกลงแห่งสัญญา คาร์ปาสกีแลกเปลี่ยนยอมให้มีการใช้งานซอฟต์แวร์และเอกสารคู่มือ (“เอกสารคู่มือ”) ภายใต้เงื่อนไขของตามธุรกิจที่ท่านอาจติดตั้งโปรแกรม 1 ครั้งสำเนาของซอฟต์แวร์กับคอมพิวเตอร์เครื่องเดียว

1.1 การใช้ หากว่าซอฟต์แวร์ที่ซื้อจากสื่อกลาง ท่านมีสิทธิในการใช้ซอฟต์แวร์ในการปกป้องจำนวนของคอมพิวเตอร์ตามที่กำหนดเอาไว้ตอนซื้อ หรือตอนที่สั่งซื้อซอฟต์แวร์การปกป้อง

1.1.1 ซอฟต์แวร์ที่ใช้ในเครื่องคอมพิวเตอร์ เมื่อมีการโหลดลงในหน่วยความจำชั่วคราว (เช่นหน่วยความจำแบบสุ่ม หรือแรม) หรือมีการติดตั้งลงในหน่วยความจำถาวร (เช่น ฮาร์ดดิสก์ CD-ROM หรือหน่วยเก็บความจำอื่นๆ) ของเครื่องคอมพิวเตอร์อำนาจของลิขสิทธิ์นี้ ตามกฎหมายหากท่านมีการทำสำเนาเพื่อการสำรองข้อมูล ไว้ในที่ต่างๆ หรือการทำสำเนาส่วนหนึ่งส่วนใดของซอฟต์แวร์อันเป็นสมบัตินั้น ก็เพื่อการสำรองข้อมูลเท่านั้น ท่านจะต้องทำการเก็บรักษาสำเนาข้อมูลเหล่านั้นเพื่อการป้องกันกรนำเอาซอฟต์แวร์ไปใช้โดยไม่ได้รับอนุญาต

1.1.2 ซอฟต์แวร์ปกป้องคอมพิวเตอร์ป้องกันไวรัส ประกอบไปด้วยฐานข้อมูลในการอัปเดตหลายเซนต์ไวรัสซึ่งมีอยู่บนเซิร์ฟเวอร์ของคาร์ปาสกี

1.1.3 หากว่าท่านขายเครื่องคอมพิวเตอร์ที่มีการติดตั้งซอฟต์แวร์ ท่านต้องแน่ใจว่าได้ลบซอฟต์แวร์เวอร์ชันก่อนหน้าไปเรียบร้อยแล้ว

1.1.4 ท่านจะไม่ทำการถอดโปรแกรม แกะไขทางวิศวกร แยกหรือทำการลดส่วนใดของซอฟต์แวร์เพื่อให้บุคคลที่สามที่ไม่ได้รับอนุญาตสามารถอ่านได้ ข้อมูลจำเป็นของตัวประสานการทำงานระหว่างผู้ใช้เพื่อให้มีการทำงานร่วมกันของซอฟต์แวร์ที่ทำให้เพิ่มจำนวนโปรแกรมคอมพิวเตอร์ โดยคาร์ปาสกีมีค่าใช้จ่ายที่

สมเหตุสมผลในการดำเนินการนั้น ด้วยเหตุที่คาร์ปาสกีแลปไม่มี
แนวโน้มนำในการทำขั้นตอนให้สามารถทำงานร่วมกันได้ เราจะมี
การทำการถอดโปรแกรม แก้ไขทางวิศวกร แยกหรือทำการลด
ส่วนใดของซอฟต์แวร์โดยได้รับอนุญาตจากกฎหมายเท่านั้น

- 1.1.5 ท่านจะไม่ทำการแก้ไข เปลี่ยนแปลง แปลความหรือไม่ทำอะไร
นอกเหนือไปจากเดิมของซอฟต์แวร์ จากบุคคลที่สามผู้ที่ไม่ได้
รับอนุญาต
- 1.1.6 ท่านจะไม่ทำการให้เช่า เช่าช่วงหรือให้ยืมซอฟต์แวร์แก่บุคคลใด
และไม่ทำการโอนถ่ายลิขสิทธิ์ของท่านไปให้ใคร
- 1.1.7 ท่านจะไม่จัดหาสิทธิ์หรือรหัสให้แก่บุคคลที่สาม รหัสการเริ่มต้น
โปรแกรมนั้นถือว่าเป็นข้อมูลความลับ
- 1.1.8 คาร์ปาสกีแลปอาจขอให้ท่านทำการติดตั้งเวอร์ชันล่าสุด ของ
ซอฟต์แวร์ (เวอร์ชันล่าสุดและเวอร์ชันรักษาล่าสุด)
- 1.1.9 ท่านจะไม่ใช้โปรแกรมไปในทางการสร้างไวรัสโดยอัตโนมัติ
ทั้งอัตโนมัติหรือด้วยมือ ให้เป็นไวรัส ข้อมูลหรือรหัสใดที่เป็น
โปรแกรมมุ่งร้าย
- 1.1.10 ด้วยความยินยอมของท่านในข้อตกลงนี้ คาร์ปาสกีแลปมีสิทธิใน
การรวบรวมข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ของเครื่อง
คอมพิวเตอร์ของท่าน เพื่อนำข้อมูลเหล่านั้นมาเป็นการปรับปรุง
การทำงานของคาร์ปาสกีแลป

2. การสนับสนุน

(i) คาร์ปาสกีแพลตฟอร์มจัดหาบริการการสนับสนุน (“การบริการการสนับสนุน”) ตามระยะเวลาของลิขสิทธิ์ที่ระบุไว้ข้างล่างใน License Key File (ระยะเวลาการบริการ) ที่แสดงไว้ในหน้าต่าง “Service” จากการกระทำดังนี้

- a. การชำระเงินตามค่าการสนับสนุน และ
- b. การกรอกเอกสารการบอกรับการบริการการสนับสนุนที่ได้ให้ไว้ในข้อตกลงนี้ หรืออยู่ที่ คาร์ปาสกีเว็บไซต์ ซึ่งท่านต้องกรอกรหัสการเริ่มต้นโปรแกรม (Activation code) ที่เป็นไปตามสัญญา การตัดสินใจขั้นเด็ดขาดขึ้นอยู่กับคาร์ปาสกีแพลตฟอร์ม หรือความพอใจของท่านตามเงื่อนไขของการบริการสนับสนุน

การบริการสนับสนุนเริ่มขึ้นเมื่อมีการเริ่มต้นโปรแกรมโดยการลงทะเบียน ฝ่ายสนับสนุนทางเทคนิคของคาร์ปาสกี จะเข้าสู่ความต้องการในการสนับสนุนทางเทคนิคของท่านเพื่อทำการยืนยันการสนับสนุน

(ii) การบริการการสนับสนุนจะสิ้นสุดลงเมื่อไม่มีการต่ออายุลิขสิทธิ์โดยการชำระเงิน เมื่อมีค่าธรรมเนียมประจำปีอีกครั้งก็จะสามารถเข้าสู่แบบการขอสนับสนุนทางเทคนิคได้

(iii) “การบริการการสนับสนุน” หมายถึง

- a. การอัปเดตปกติของแอนตี้ไวรัส
- b. การอัปเดตซอฟต์แวร์ฟรี รวมถึงการอัปเดตเวอร์ชันใหม่
- c. การสนับสนุนทางเทคนิคผ่านทางอินเทอร์เน็ตและสายด้วยจากผู้ขาย
- d. การตรวจจับไวรัสและการกำจัดตลอด 24 ชั่วโมง

(iv) การบริการการสนับสนุนมีการจัดหาให้ในกรณีที่ไม่มีเวอร์ชันล่าสุด (รวมถึงการบำรุงรักษา) ที่มีอยู่บนเว็บไซต์ทางการของคาร์ปาสกี (www.thaikaspersky.com) ที่ติดตั้งบนเครื่องคอมพิวเตอร์ท่าน

3. สิทธิความเป็นเจ้าของ ซอฟต์แวร์นี้มีการปกป้องโดยทางกฎหมายสำเนาถูกต้อง ที่สงวนไว้เฉพาะผู้จำหน่ายที่ถูกต้องของคาร์ปาสกี คาร์ปาสกีขอสงวนสิทธิ์ ในชื่อและทั้งหมดในซอฟต์แวร์ รวมทั้งสำเนาถูกต้อง สิทธิบัตร การค้าและทรัพย์สินทางปัญญาอื่นๆ ความเป็นเจ้าของ การติดตั้ง หรือการใช้งานซอฟต์แวร์ที่ไม่ได้มีการโอนถ่ายทรัพย์สินทางปัญญาจากซอฟต์แวร์ไปยังท่าน และท่านไม่ได้มีสิทธิครอบครองในส่วนนี้ตามข้อตกลงนี้
4. การรักษาความลับ ท่านตกลงให้ซอฟต์แวร์และเอกสาร รวมทั้งการออกแบบโครงสร้างของโปรแกรมเฉพาะนั้นถือเป็นสมบัติของคาร์ปาสกีแลป ท่านจะได้รับมาตรการการป้องกันอย่างสมเหตุสมผล เพื่อการปกป้องข้อมูลที่เป็นความลับ แต่ไม่มีข้อจำกัด
5. การจำกัดการรับประกัน
 - (i) คาร์ปาสกีมีการรับประกันการดาวน์โหลดใน 6 เดือนแรกของการดาวน์โหลดหรือการติดตั้ง ซอฟต์แวร์ที่ซื้อจากสื่อกลาง ตามการทำงานที่อธิบายไว้ในเอกสารเมื่อมีการทำงานอย่างปกติ
 - (ii) ท่านยอมรับในความรับผิดชอบในการเลือกซอฟต์แวร์ที่ท่านต้องการ คาร์ปาสกีจะไม่รับประกันหากว่าเกิดจากการเลือกโปรแกรมที่ผิด ไม่เหมาะสมกับการใช้งาน
 - (iii) คาร์ปาสกีแลป จะไม่รับประกันเนื่องจากการรายงานผลไวรัสที่ไม่ถูกต้องหรือเกิดจากความเข้าใจผิดในส่วนที่ไม่ได้เกิดจากการติดเชื้อไวรัส
 - (iv) การรักษาหรือความรับผิดชอบทั้งหมด ของคาร์ปาสกีแลปสำหรับการทำผิดสัญญาในข้อ (i) จะเป็นตัวเลือกของคาร์ปาสกีในการซ่อม เปลี่ยน หรือคืนเงินค่าซอฟต์แวร์ หากการรายงานยังคาร์ปาสกีแลปหรือผู้ได้รับการแต่งตั้งระหว่างระยะเวลาของรับประกัน ท่านจะจัดหาข้อมูลทั้งหมดเท่าที่จำเป็นเพื่อช่วยในการแก้ปัญหา

- (v) การรับประกันในข้อ (i) จะไม่เกิดขึ้นหากว่าท่าน a) ทำหรือเป็นสาเหตุของการเปลี่ยนแปลงซอฟต์แวร์ โดยปราศจากการยินยอมของคาร์ปาสกี แลป b) ใช้ซอฟต์แวร์เพื่อการอื่นโดยไม่เจตนา c) ใช้ซอฟต์แวร์ในทางที่ไม่ได้อยู่ภายใต้ข้อตกลง
- (vi) การรับประกันและเงื่อนไข ในข้อตกลงนี้ หรือเงื่อนไขอื่นใด ที่ทำให้เกิดความผิดพลาดในซอฟต์แวร์หรือเอกสารคู่มือ (vi) มีผลระหว่างคาร์ปาสกี แลปและท่าน หรือหากว่าท่านไม่ให้ความร่วมมือในข้อตกลงนี้ หรือมีสัญญาใดที่ใกล้เคียงกันไม่ว่าจะเป็นกฎหมายอื่นใด (รวมทั้งการไม่มีข้อจำกัด เงื่อนไขเป็นนัย การรับประกันหรือเงื่อนไขอื่นใด ที่เป็นสิ่งที่เหมาะสมกับวัตถุประสงค์ที่ใช้หรือสมเหตุสมผลกับทักษะหรือการดูแล)

6. ข้อจำกัดของความรับผิดชอบ

- (i) ไม่มีสิ่งใดในข้อตกลงนี้ ที่ทางคาร์ปาสกีจะไม่รับผิดชอบสำหรับ a)
 - (a) การสูญเสียรายได้
 - (b) การสูญเสียกำไรที่แท้จริง หรือกำไรที่ควรได้ (รวมทั้งกำไรตามสัญญา);
 - (c) สูญเสียการใช้เงิน
 - (d) การสูญเสียเงินสะสม
 - (e) สูญเสียทางธุรกิจ
 - (f) สูญเสียโอกาส
 - (g) สูญเสียมิตร
- (ii) ภายใต้หัวข้อข้างบนที่กล่าวมา คาร์ปาสกีแลป จะไม่รับผิดชอบ(ไม่ว่าจะในสัญญา

(h) สูญเสียชื่อเสียง

(i) ข้อมูลสูญเสีย เสียหายหรือถูกทำลายหรือ

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

(iii) ภายใต้ข้อความ (i) ข้างต้น ความรับผิดชอบของคาร์ปาสกีแลป ขึ้นอยู่กับการเชื่อมต่อด้วยซอฟต์แวร์ที่อยู่ในสภาพแวดล้อมที่เหมาะสมและจำนวนที่เท่ากับที่ท่านจ่ายไป

7. ข้อตกลงนี้ประกอบไปด้วยความเข้าใจทั้งหมดระหว่าง ทั้งสองฝ่ายที่เกี่ยวข้องกันมาในทั้งหมดนี้ ความเข้าใจก่อนหน้านี้ที่เป็นลายลักษณ์อักษร หรือด้วยวาจาเปลวระหว่างคุณและคาร์ปาสกีแลป ซึ่งมาจากการตกลงกันระหว่างเราหรือตัวแทนของเราก่อนหน้านี้สัญญาให้ถือเป็นโมฆะทั้งหมด และมีผลตามวันที่บังคับการมีผลนี้

8. คาร์ปาสกีแลป

ผลิตภัณฑ์อื่นๆ ของคาร์ปาสกี

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