OCZ INFORMATION

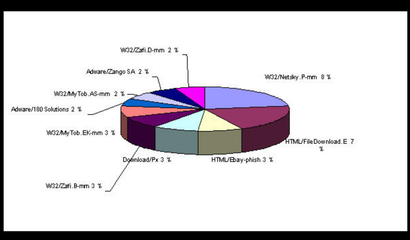
รายงานการตรวจพบไวรัสประจำเดือน กันยายน 2548

Fortinet รายงานไวรัส สปัยแอ็นดันอันตรายประจำเดือนกันยายน 2548

Fortinet รายงาน ว่าในเดือน กันยายน 2548 ได้ตรวจสอบพบไวรัสตัวใหม่ขึ้นที่ถี่ขึ้น อย่างต่อเนื่อง และมีเทคนิคใหม่ ตลอดเวลา โดยเรียงตามลำดับตามความอันตราย ดังนี้

อันดับ	ชื่อไวรัส	เปอร์เซ็นต์
1	W32/Netsky.P-mm	8 %
2	HTML/FileDownload.E	7 %
3	HTML/Ebay-phish	3 %
4	Download/Px	3 %
5	W32/Zafi.B-mm	3 %
6	W32/MyTob.EK-mm	3 %
7	Adware/180Solutions	2 %
8	W32/MyTob.AS-mm	2 %
9	Adware/ZangoSA	2 %
10	W32/Zafi.D-mm	2 %

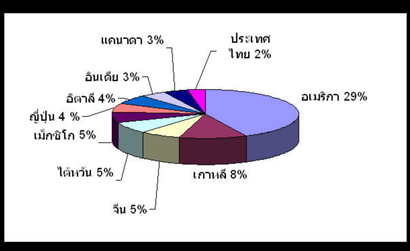
Top 10 Virus (September 2005)



ประเทศที่รายงานการโดนไวรัสโจมตีสูงสุด 10 อันดับแรก
ประจำเดือนกันยายน 2548

อันดับ	ประเทศ	เปอร์เซ็นต์
1	อเมริกา	29 %
2	แคนาดา	8 %
3	จีน	5 %
4	ไต้หวัน	5 %
5	เม็กซิโก	5 %
6	ญี่ปุ่น	4 %
7	อิตาลี	4 %
8	อินเดีย	3 %
9	เกาหลี	3 %
10	ประเทศไทย	2 %

Top 10 Countries virus infection (September 2005)



Bagle/Mitgliedor ขุกคามอย่างหนักในเดือนกันยายน

ตั้งแต่ 19 กันยายน มีไวรัสที่ชื่อว่า Mitgliedor ได้สร้างความปั่นป่วนอย่างมหาศาลให้กับเครือข่ายทั้งสำนักงานและองค์กรต่างๆ ซึ่งรูปแบบนี้จะเหมือนกันทั้งการส่งออกขุกคามของตัวไวรัสนี้ และมีเทคนิคอันหลากหลายแล้ว

Guillaume Lovet ผู้นำทีมตรวจสอบงานขุกคามของ Fortinet กล่าวว่า " การสร้างไวรัสตัวใหม่ ๆ โดยการเปลี่ยนแปลงไม่เพียงแต่ก๊อปโนรหัสต้นการจัดเก็บเป็นตั้งก็ผู้สร้างไวรัสจะยามาทำขายผ่านตัวแทนจำหน่ายเพื่อเก็บเงินกันไวรัส ซึ่งการตรวจรักแบบนี้ไม่ประสบความสำเร็จ ทั้งสถานความต้องการของผู้สร้างไวรัส MyTob ที่เพิ่งขึ้นไปเด็นขุดคุกคามของปีนี้ ซึ่งทั้งสิ่งที่ได้อย่างชัดเจนที่สุด ผู้จำหน่ายส่วนมากสามารถเปิดช่องทางได้อย่างรวดเร็ว Bagle จำนวนมากจึงไม่ก่อขุดความไม่ตลอดทั้งปีนี้ ซึ่งทั้งสิ่งที่ทำให้ Bagle ตัวแรกที่ถูกยึดมาเป็นอยู่ที่ความถี่ต่ำที่ 50 ในไวรัส 100 ตัวแรกของ Fortinet ยังมีคนจำนวนร่วมทั้ง Virus ตัวนี้ถึงถึงกว่า 1% จากการทำงานของไวรัสทั่วโลก"

การเพิ่มขึ้นของ Spyware- 10 อันดับแรกของการขุกคามในเดือนกันยายน

จะเห็นได้ชัดเจนที่สิ่งเดียวกันของการขุกคามของ Spyware จากประวัติที่ถ่ายมา 10 รายการแรกของรูปแบบการขุกคามในทุกเดือนของ Fortinet ซึ่งส่วนใหญ่เป็นตัวการของแอดไวแต่ก็มาจากแอดแวร์ทั้งหมด 10 รายการการขุกคามแอดแวร์ไม่ได้ทำของแอ แต่ตัวไหนก็เพิ่มเข้ามา คือ HTML/ Ebay- phish และ Adware/ 180Solutions และมีไวรัสอื่น ๆ อีก 2 รูปแบบ คือ ZangoSA หรือเรียกว่า "ผู้ช่วยเหลือในการทำงานเรื่องผูก " (browser helper object) โดยตัวนี้นอจะสอดแนมการใช้ Internet ของ User ที่ติดไวรัส และส่งข้อมูลกลับไปทางผู้สร้างอย่างเงียบ ๆ

เราจะสามารถกำจัด spyware ที่แฝงตัวมาบังคับหมายจำนวนมากๆ และก็ทิ้งออกไปจาก 10 รายการแรกของไวรัส เช่นเดียวกับกับ Zafis หรือ MyTob

โดยการพิจารณา 3 ทางหลักๆที่ใช้รับมือจาก spyware คือ

1. จากผู้เข้า Webpage โดยคลิคเข้าไป โดยบรรดาซอร์ฟแวร์ไม่มีการติดตั้ง Service Patch
2. จากผู้ที่เข้าไปคลิกโฆษณาที่ประสงค์ว่าอโดยไม่รู้ตัว
3. จากการมีตัวของไวรัสกับ spyware ที่ถูกแอบติดตั้ง

Guillaume Lovet กล่าว " ถึงแม้ผู้ร้ายส่วนมากเป็นอันเล็กประชะ ที่มาจากการติดต่อเพื่อสารของเครื่องที่ติดไวรัส ดังนั้นการขุกคามก็แผ่ขยายแค่ผู้ใดเครื่อง (spyware) จึงสูงขึ้นเพราะเพื่อนมีการกระทำของให้เห็นแนวโน้มในการขุกคามของผู้ก่อการร้ายในโดยของ Internet (cybercrimmal) เนื่องจากปัจจุบันนี้คลิชช่าย Internet มีขนาดใหญ่มาก การเชื่อมต่อกับ Host ต่างๆ (ชื่น botnets) ที่สร้างขึ้นในขณะนี้ เป็นที่ยากมากๆสูงที่จะสามารถเชื่อมต่อผู้เป็นเจ้าของทั้งหลายได้ ดังนั้นโดยส่วนมาก และมีคุณลักษณ์ต่างๆที่ทำให้ง่ายต่อทางเรา อันเดี๋ยวประ และ การขอดก่อนค่า password (Phish) รวมทั้งการแอบทิ้งตัวอยู่ในเครื่องของผู้เข้าไปใช้ internet "

การโจมตีในรูปแบบของการปลอมแปลงอี-เมล์ หรือ ทำการสร้างเว็บไซต์ปลอม เพื่อหลอกล่อเอาข้อมูลต้านการเงินหรือรหัสผ่าน (Phishing) โดยเฉพาะโดยการอาศัยเหตุการณ์พายุเฮริเคนแคทริน่า

น่าสลิดหดเศร้ยวกันการปิ่งอกันมามายที่สามารถขุดขึ้นได้ก่อนเกิดความเสียหายเหมือนกับความหยายามเร้าหลอกล่อเอาการหลักฐาน เพื่อเอาไปใช้ประโยชน์เพื่อนำโทษกันต่อประโยชน์ขาวการเกิดพายุเฮริเคน แคทริน่า ทั้งเกิดขุดการณ์ขึ้นไม่เพียงแค่หยาย อีเมล์ที่หลอกล่อเอารหัสผ่านเล่านี้ จะกระทุ้ผู้ใช้ให้เชื่อคลิชไปในเว็ปไซท์ที่ประสงค์ร้ายที่ทำทำขึ้นปุ๊ใขขุม และผู้ใช้มีเจ็ตจะรับจ้างเงินขุมการบรรทาวัถ ซึ่งผู้ก่อการร้ายเหล่านี้ต้องการที่จะล่อเอาข้อมูลทั้งหมดทุกการณ์ อันมีการเกิดขึ้นของกลุ่มได้ที่ทะรัฐ่ลอมตอน และอีกหลาย ๆ เหตุการณ์ที่เกิดขึ้นโดยก่อนหน้านี้ เช่นขุดคุกคามที่พายุเฮริเคนริต้า

(หลายโดมณฑลงานประเปิดนาโรยร้อยเล็กน้อย " HURRICANE- RITA- RELIEF. net" หรือ" RITA- DONATIONS. com").

Guillaume Lovet กล่าว "น่าเสียใจที่จะขุดว่า ประสบการณ์ได้ที่ผู้ร้ายนั้นเมื่อไหร่ถึงเหตุการณ์ที่สำคัญเกิดขึ้นร้าว และผู้ก่อต้องการบ้างจาก ก็เกิดการพยายามที่จะดึงให้ผลกล่อเอารหัสผ่านมาทั้ง Fortinet แนะนำให้ใช้บริการที่ควบคุมการอาการได้ใน (Web Filtering Service) เพื่อตรวจสอบถูก blacklist ที่ผู้ร้าย นอกจากนี้ยังมีประบริการควบคุมเปลดเปิดกรัฐมนูกลี่การบริการอ้อก internet และเปิดระบบของผู้ใช้ "

US- CERT ได้ทำแนะนำผู้ใช้ทั้งหมดว่าให้ใช้ข้อมูลของ สหพันธ์ตัวแทนการจัดการภาวะฉุกเฉิน (Federal Emergency Management Agency - FEMA) ซึ่งเป็นเว็ปไซท์ ที่ส่ามารถให้เงินได้ใช้ในการบริจาคได้อย่างถูกต้องตามกฎหมายและปลอดภัย http:// www.fema.gov/news/newsrelease.fema ?ID=18473

การเกิด เหตุการณ์ที่ รุนแรงและทันทีทันใด ในหลายเดือนที่ผ่านมา

เดือนที่ผ่านมานี้ของเดือนสิงหาคม เดือนที่ผ่านมาย เดือนที่ผ่านมาย เดือนกันยายนเดือนที่ผ่านมา อย่างมหึมาของ อินดีในเยอรมัน มีการเลียนแบบเวบไซต์ ebay ซึ่งดูเหมือนและรู้สึกว่าเป็นการเชิญชวนจาก ebay.de เอง โดยออกแบบอันเดียวและจะจำนวนมากกันแบบเพื่มที่ทั้งเรื่องว่า " Ebay rechnung.pdf.exe " เมื่อทำการคลิ๊ผมเพื่มทั้งหมด กลุ่มของวิศวกรที่จะตีผลาร์ยอดูหลายๆของ ebay นอกจากเพื่มทั้งหมดซึ่งเป็นเพื่มผลิตภัณฑ์ดูเหมือนไม่มีค่าอะไร และเหมือนว่าผู้ร้ายเหล่านี้ของตัวหลาย P2P หรือที่เรียกว่า W32 / Goldun และ

A – ทะ ที่เป็นชื่อหนทำของในการบรรทาการติดต่อของมัน

http://keroker.hu/***.exe

http://jolved.hu/***.exe

http://sitabor.com/***/***/***.exe

http://szabadalmikamara.hu/***/***.txt

http://www.bsetrans.com/***/***/***.exe

Guillaume Lovet กล่าวว่า " ประโยชน์ในการศตรวมโหลดผมไฟล์ข้อมูล จากรายการการเก็บผมไฟล์ข้อมูลในแต่ละส่วน เมื่อเทียบกับต้นหน่วงที่เป็นผมไฟล์ข้อมูลนี้เกิดขึ้นหรือไม่ยังเงนมากนัก เพราะเกี่ยวส่วนมากผู้สร้างติดว่า ลึงนั้นจะติดว่าผมเมื่อเกิดขึ้นหมด ยังตามความสวรรคประเมินบทศึกษาและให้ความหมาย บริษัทที่เป็นจำของเรื่ยระไม่ก่อยได้ให้ความเชื่อมมูณุณ ทั้งๆที่รู้ว่าระบบการทำงานเพื่อดูหมาดของการขุกคามยืนขึ้นจากความ ไม่ตรงของไม่ตรงยิ่ง ตลาดปัจการเวิน หรือผู้บริหารระบบของตัวเอง หรือผมไฟล์ดูไปบริการข้อมูลจริง การพิจารณาสิ่งที่เกี่ยวข้องเพื่อเป็นสิ่งที่ดี และควรจำไว้ว่า ไม่ตรงอาจไม่ก่อส่งอันเพื่มผลิตไปโดยอกมา"

ผู้ใช้ผ้าโทรจันทำการขยายให้เหมือนกันเป็นการป้องปรายการป้องกันความปลอดภัยจากไม่โครรอพ

อันเมื่อผู้ร้ายที่ดูเหมือนมากขาวไม่โครรอพ และกระตุ้นผู้ใช้ให้ติดตั้งเพื่มป้องกันความปลอดภัยเพื่มขนมา ซึ่งตามความเป็นจริงเป็นการทำงานของผ้าโทรจัน ที่ถูกกระจายไปในตัวอันกันยายน ตอนนี้เรายังกว่า W32 / Zapchast.F –tr และผู้ใช้ตามอันเพื่มขนของการขุกคามยืนขึ้นจากความ ไม่ตรงของไม่ตรงยิ่ง ตลาดปัจการเวิน หรือผู้บริหารระบบของตัวเอง หรือผมไฟล์ดูไปบริการข้อมูลจริง การพิจารณาสิ่งที่เกี่ยวข้องเพื่อเป็นสิ่งที่ดี และควรจำไว้ว่า ไม่ตรงอาจไม่ก่อส่งอันเพื่มผลิตไปโดยอกมา"

Nick Bilogorskiy Manager of Antivirus Escalation and Research ของ Fortinet กล่าวว่า " กลุ่มโครงสร้างทางวิศวกรผลอย่างปีเป็นชื่อการขับจำนวนผ่านมายาผู้ใช้ และเหมือนเพื่มการจับรู้ ผู้ใช้ต้องพิผมาชิสิทธิ์ที่จะสงสัยการผนนผมไฟล์ผ้าโทรจันอันเดียวกันไม่ว่าจะพาไม่โครรอพ , สถาปัยการเวิน หรือผู้บริหารระบบของตัวเอง หรือผมไฟล์ดูไปบริการข้อมูลจริง การพิจารณาสิ่งที่เกี่ยวข้องเพื่อเป็นสิ่งที่ดี และควรจำไว้ว่า ไม่ตรงอาจไม่ก่อส่งอันเพื่มผลิตไปโดยอกมา"

COPYRIGHT 2004 OVERCLOCKZONE.COM, ALL RIGHT RESERVED. IF YOU HAVE ANY SUGGESTION OR COMMENT PLEASE MAIL
This website optimize resolution best view for 800 x 600
Created : Webmaster | Link : เวบแม่ลิงค์ ๆ