ทำนาย 10 ภัยคุกคามทางอินเตอร์เน็ท 2008

ใกล้ หมดปีไปอีกครั้งแล้วนะครับ ใครตั้งใจจะทำอะไรไว้ ยังไม่ได้ทำภายในปีนี้ก็ขอให้เรียบๆทำกันไว้ เวลานั้นไม่เคยคอยใคร พอใกล้หมดปี ก็มักจะมีคำทำนายในเรื่องต่างๆ เช่นกันในปีหน้า ภัยคุกคามในรูปแบบใหม่ๆ ที่อาจจะเกิดขึ้นในปี 2008 จะเป็นอย่างไรบ้างลองรับฟังกันดูเผื่อไว้ว่าจะช่วยในการป้องกัน กันได้ทัน
เท่าที่ผ่านมาได้ค้นหาข้อมูลเกี่ยวกับภัยคุกคามทางอินเตอร์เน็ทในรูปแบบ ใหม่ๆ และคิดว่าในปี 2008 ภัยคุกคาม จะเน้นในเรื่องความเป็นส่วนตัวมากขึ้น ข้อมูลที่เป็นข้อมูลส่วนบุคคล ความประมาทในการใช้งานของ User รวมถึงอาชญากรรมคอมพิวเตอร์ ในรูปแบบต่างๆ ที่ทวีความซับซ้อน จะแบ่งหมวดหมู่ภัยคุกคามได้ดังนี้ครับ

กลุ่มภัยคุกคามที่พบในปี 2008

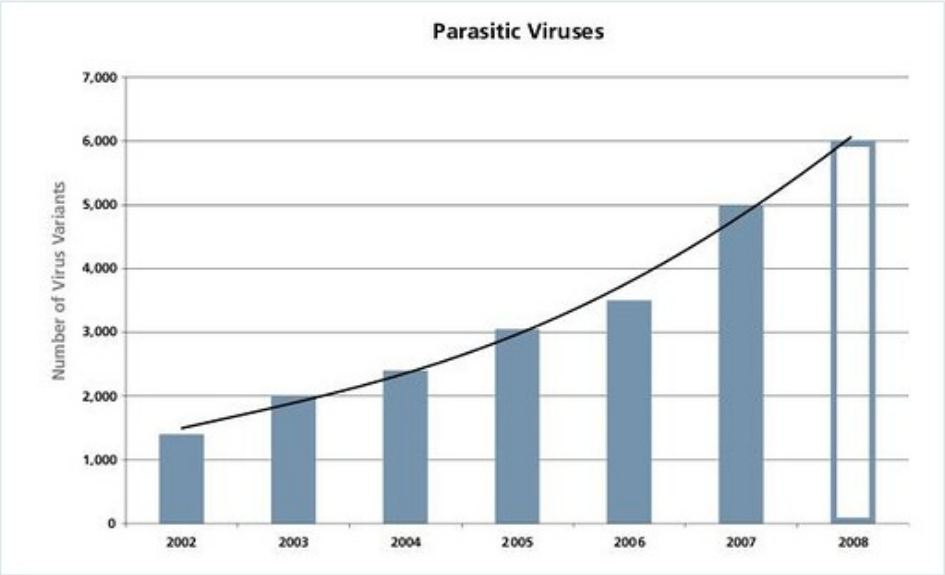
กลุ่มที่ 1 กองทัพ botnet ตัวกลางเชื่อมต่อภัยคุกคามในรูปแบบต่างๆ

กลุ่มที่ 2 ช่องโหว่ของระบบปฏิบัติการ
กลุ่มที่ 3 ภัยคุกคามจากความประมาทจากการใช้ข้อมูลส่วนตัวบนอินเตอร์เน็ท

กลุ่มที่ 1 กองทัพ Botnet ตัวกลางเชื่อมต่อภัยคุกคามในรูปแบบต่างๆ

ภัยคุกคามอันดับที่ 1 Storm Worm : อาชญกรทางคอมพิวเตอร์ จะใช้เทคนิคการสร้าง Storm Worm เพื่อกลบเกลื่อนร่องรอย สร้างสายพันธ์ของ worm ในการเปลี่ยนโค้ดที่ทำให้ระบบซอฟต์แวร์ Anti virus ไม่สามารถตรวจจับได้ ซึ่งการเกิด Storm Worm นั้นเป็นการติดโปรแกรมไม่พึงประสงค์ บนเจตนาของผู้บุกรุกที่สร้างขึ้น โปรแกรมไม่พึงสงค์เรียกอีกอย่างหนึ่งว่า “malware” คือซอฟต์แวร์ที่สูญเสีย C (Confidentiality) I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือ ทั้งหมด จนทำให้เกิดเป็น Virus , Worm , Trojan , Spyware , Backdoor และ Rootkit ซึ่ง Storm worm เป็นลักษณะการแพร่กระจายสายพันธ์ ที่มีการเปลี่ยนแปลงโค้ด ทำให้เกิดความเสียหายกับเครื่องที่ติด worm เหล่านี้ ผลลัพธ์ของ Storm worm คือเครื่องที่ติด worm ชนิดเหล่านี้จะถูกเรียกว่า “Zombie” ที่พร้อมที่จะควบคุมให้ทำการใดการหนึ่ง เช่น การส่ง Spam , การโจมตีชนิดที่เรียกว่า DDoS/DoS เป็นต้น หาก Zombie จำนวนมากกว่า 1 เครื่อง ก็เรียกว่า Botnet นั้นเอง ในปี 2008 กองทัพ Botnet ที่พร้อมใช้งานจะมีอัตราที่สูงขึ้น และอาจมีการซื้อขาย กองทัพ Botnet ในกลุ่มอาชญกรคอมพิวเตอร์ เพื่อใช้โจมตีเครือข่ายเครือข่ายขนาดใหญ่ ได้ต่อไป

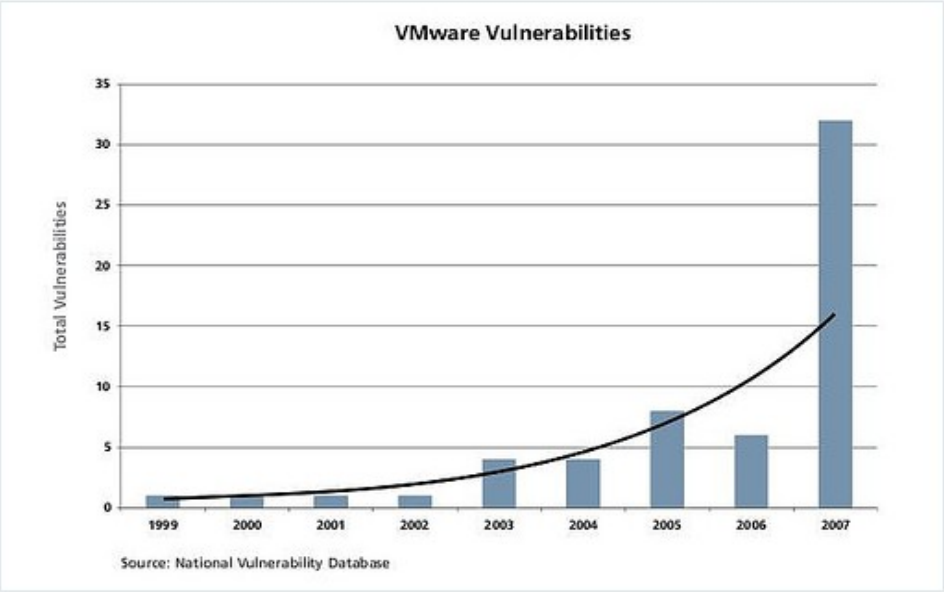
ภัยคุกคามอันดับที่ 2 : Parasitics Malware เป็นไวรัสที่แก้ไขไฟล์ที่อยู่ในดิสก์ และใส่โค้ดเข้าไปในไฟล์ ในปีที่ผ่านมาจะพบว่าผู้เขียนไวรัสจะใช้วิธีนี้สร้างไวรัสชนิดต่างๆ ตัวอย่างเช่น Grum , Virut และ Almanahe คาดว่าจะมี Parasitics Malware เติบโตขึ้นในปี 2008 และการฝังโค้ดเข้าไปในไฟล์ จากเดิมเน้นการทำลายเครื่องให้เกิดความผิดปกติ ก็จะทำฝังตัวควบคุมเครื่อง อาจเป็น Backdoor , Trojan , หรือ Script บางอย่างที่ทำให้เครื่องติด Parasitic Malware ตกเป็นทาส (Zombie) ได้ซึ่งการเกิด Zombie หลายๆเครื่อง ก็จะกลายเป็นกองทัพ Botnet ที่พร้อมใช้งานในการโจมตีต่อไป



รูปที่ 1 สัดส่วนการเจริญเติบโตจากภัยคุกคามชนิด Parasitics Malware

ภัยคุกคามอันดับที่ 3 : การยึดระบบเสมือนจริง (Virtualization) ผู้ สร้าง Malware พยายามค้นหาช่องโหว่ในระบบ Virtualization มากขึ้นการที่ได้ควบคุมระบบปฏิบัติการเสมือน ในการสร้างกองทัพ Botnet และเพื่อการแพร่กระจายการติดเชื้อแบบ Storm worm ขึ้น

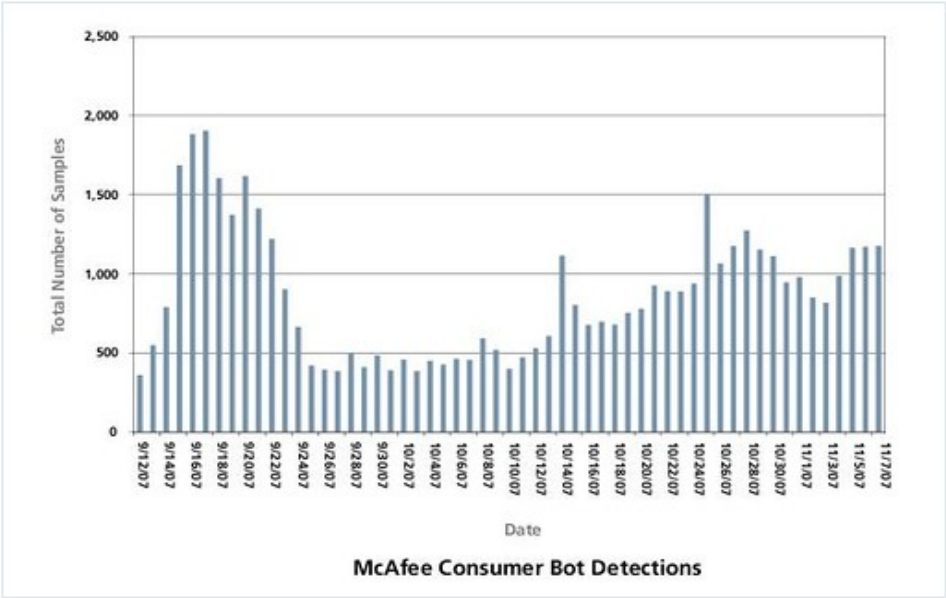
ทั้งนี้เพื่อสร้างจำนวน Zombie แบบไร้ตัวตนให้มากขึ้น Virtualization
เป็นเทคโนโลยีที่ช่วยให้สามารถแบ่งพาทิชันคอมพิวเตอร์ให้สามารถรันซอฟต์แวร์ และแอพพลิเคชันในจำนวนมากๆ
หรือแม้แต่รันระบบปฏิบัติการได้หลายๆ ตัวพร้อมกันซึ่งพื้นที่ที่แบ่งพาทิชันขึ้นนั้นมักรู้จักกันว่า "Virtual Space" หรือ "Container"
โดยปัจจุบัน Virtual lization Technology มีการใช้งานกันมากขึ้น



รูปที่ 2 ช่องโหว่ที่ค้นพบบนระบบเสมือน

ภัยคุกคามอันดับที่ 4 FastFlux เป็น เทคนิคทาง DNS ที่ใช้โดย Botnet เพื่อซ่อนเว็บไซต์ที่ทำหน้าที่ให้บริการ Phisihing และมัลแวร์ที่อยู่เบื้องหลังเครือข่ายของโฮสต์ที่ถูกบุกรุกทำตัวเป็น Proxy ที่มีการเปลี่ยนแปลงตลอดเวลา รวมถึงเครือข่ายแบบ Peer-to-Peer รวมกันหลายเครือข่าย ใช้เทคนิคต่างๆ ได้แก่ การใช้คำสั่งและการควบคุมแบบกระจาย (Distributed) การใช้ Load Balancing และการเปลี่ยนเส้นทาง proxy เพื่อทำให้การเครือข่ายมัลแวร์ยากต่อการถูกตรวจพบและการป้องกัน Storm Worm เป็นหนึ่งในมัลแวร์ที่ใช้เทคนิคเหล่านี้ผู้ใช้อินเทอร์เน็ตอาจพบการใช้ fast flux ในการโจมตี phishing ที่มีเชื่อมโยงกับกลุ่มอาชญากร รวมถึงการโจมตี MySpace ด้วยในปี 2008 นี้

ในปี 2008 อาจมีอาชีพใหม่ ในการค้าขาย กองทัพ botnet ในตลาดอินเตอร์เน็ทก็เป็นได้ ทั้งนี้กองทัพ botnet อาจจะมีมากในประเทศที่พึ่งมีการเชื่อมต่ออินเตอร์เน็ท และระบบเครือข่ายใหม่ๆ ที่ยังขาดการป้องกันภัยที่ดี อีกทั้งจะมีจำนวนมากขึ้นสำหรับประเทศที่ยังไม่มีกฎหมายเอาผิดกับผู้ใช้ botnet ซึ่งผลที่เกิดจากการโจมตีของ Botnet ไม่ใช่แค่เพียงการส่ง Spam , DDoS/DoS , Virus/worm อีกต่อไป แต่เป็นภัยคุกคามอื่น ที่คาดไม่ถึงว่าจะเกิดขึ้นก็เป็นไปได้



รูปที่ 3 จำนวน botnet ในแต่ละวัน

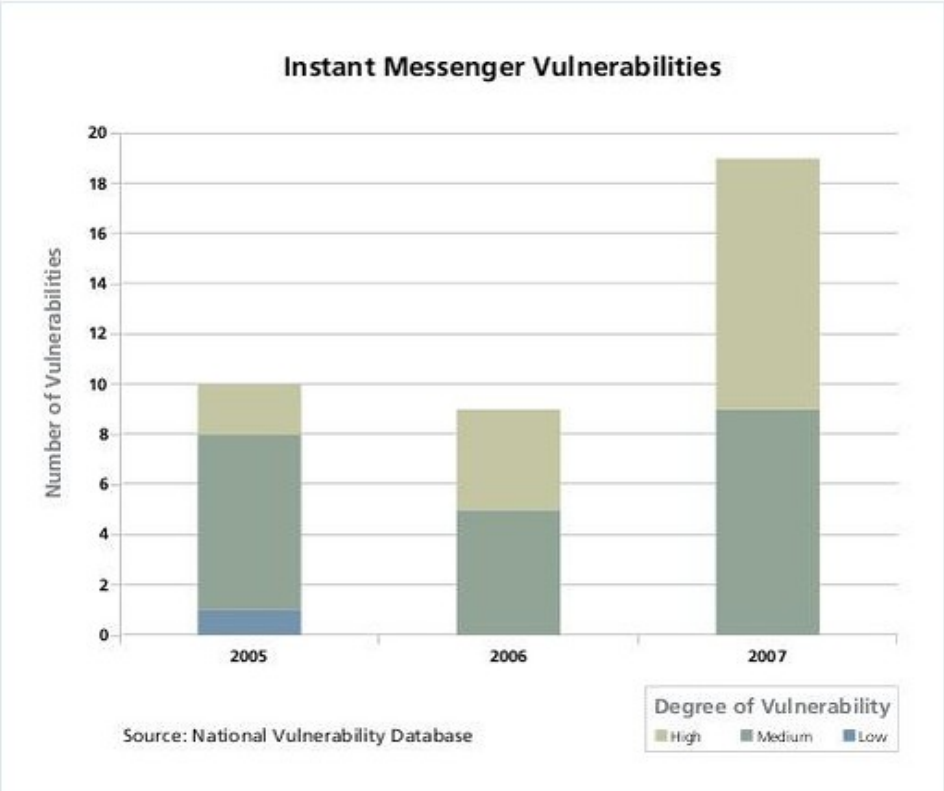
กลุ่มที่ 2 ภัยคุกคามจากช่องโหวที่พบบนระบบปฏิบัติการ

ภัยคุกคามอันดับ 5 : Operating System Vulnerability : ระบบปฏิบัติการที่เรารู้จักกันดี ไม่ว่าเป็น Linux / BSD , MaC OS หรือ Windows Microsoft นำไปใช้บน Appliance ต่างๆ รวมไปถึงระบบมือถือ ที่ในปีหน้า 2008 นี้เองจะเห็นว่าคนทั่วไปพกมือถือที่มีมัลติมีเดีย และสามารถท่องโลกอินเตอร์เน็ทได้ สามารถทำอะไรๆ ที่ต้องการได้ ทำงานแทน Notebook ได้ ไม่ว่าเป็นมือถือที่ระบบปฏิบัติการของ Mac ที่ชื่อว่า iPhone หรือพวก Windows Mobile ซึ่งในปีหน้าอาจพบช่องโหว่ต่างๆ ที่เกิดขึ้นบนเครื่องมือถือมากขึ้น ไม่ว่าเป็นพวก Virus/worm, Spam เหล่านี้สร้างความเสียหายไม่น้อยกว่าเครื่อง PC ที่ใช้กันทั่วไป ที่เป็นเช่นนี้ก็เนื่องจาก Application ที่มากขึ้น บนตัวระบบ Operating System ทำให้ภาพรวมการใช้งาน จะพบช่องโหว่มากขึ้น หลายคนยังตั้งข้อสังเกตถึงระบบปฏิบัติการใหม่ของ Windows Microsoft ที่ชื่อว่า Vista ที่ยังมีช่องโหว่และไม่ได้รับการแก้ไขให้ทันเวลา ซึ่งจะขยายผลก่อให้เกิดภัยคุกคามใหม่ที่ฝังเข้าสู่ระบบ และสร้างเป็น Zombie ต่อไปได้เช่นกัน

กลุ่มที่ 3 ภัยคุกคามจากความประมาทจากการใช้ข้อมูลส่วนตัวบนอินเตอร์เน็ท

กลุ่มที่ 3 ภัยคุกคามจากความประมาทจากการใช้ข้อมูลส่วนตัวบนอินเตอร์เน็ท ซึ่งส่วนตัวผมถือว่าเป็นกลุ่มภัยคุกคามประจำปี 2008 เนื่องจากการเจริญเติบโตการใช้งานอินเตอร์เน็ทที่มากขึ้นและความซับซ้อนของ รูปแบบการใช้งาน มีผลให้เกิดอาชญกรรมเกี่ยวกับการขโมยข้อมูลส่วนตัว การนำข้อมูลส่วนตัวมาเผยแพร่ โดยไม่ได้รับอนุญาติ และการหลอกหลวงทางเทคโนโลยีต่างๆ ที่เกี่ยวข้องกับการใช้งาานอินเตอร์เน็ท ส่วนบุคคลมากขึ้นนั่นเอง สรุปว่ากลุ่มนี้ เหยื่อมักเกิดจาก ความรู้เท่าไม่ถึงการณ์ การทำนายภัยคุกคามที่อาจเกิดขึ้นในปี 2008 ในกลุ่มที่ 3 นี้ก็เพื่อป้องกันไม่สิ่งเหล่านี้เกิดกับตนเอง และคนใกล้ตัวให้พึ่งระวังได้

ภัยคุกคามอันดับที่ 6 : ซอฟต์แวร์ไม่พึ่งประสงค์จากการใช้สนทนาออนไลท์ (Instant Malware)
เป็นการใช้งานที่ประมาทของผู้ใช้เอง ที่อาจจะดาวโหลดซอฟต์แวร์จาก คู่สนทนาที่ไม่รู้จัก หรือรู้จัก มีไฟล์แนบมา หรือที่พบมากขึ้นคือ ในรูปแบบของ Flash ที่สามารถเอ็กซิคิวท์ตัวเองได้ มาพร้อมกับโปรแกรมประเภท Instant Messaging



รูปที่ 4 ช่องโหว่ที่ค้นพบจากการใช้งาน IM ในแต่ละปี

ภัยคุกคามอันดับที่ 7 : บริการเกมส์ออนไลน์ (Online Gaming) ผู้ใช้บริการอาจตกเป็นเหยื่อ
เนื่องจากของในเกมส์สามารถซื้อขายกันเงินจริงๆได้ ตัวอย่างเห็นได้จากโทรจันที่ขโมยรหัสผ่านของบริการเกมส์ออนไลน์ ในปี 2007 จะมีอัตราเติบโตเร็วกว่าจำนวนของโทรจันที่มีเป้าหมายกับผู้ใช้บริการของ ธนาคาร

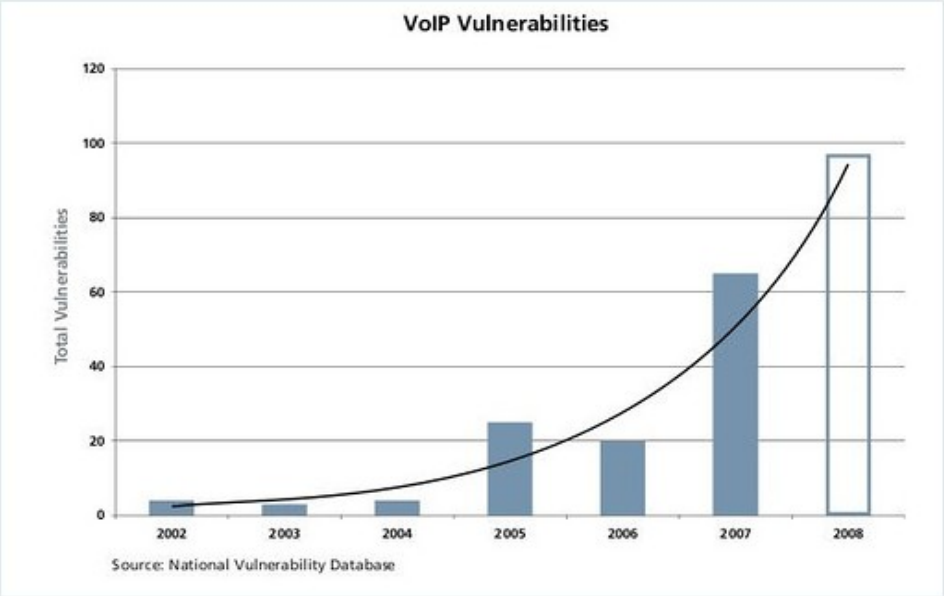
ภัยคุกคามอันดับที่ 8 : สังคมออนไลท์แบบเปิด (Social Networking) กับการใช้ข้อมูลบน Web 2.0
เป็นที่รู้กันว่าสังคมแบบเปิดบนโลกอินเตอร์เน็ทมีจำนวนมากขึ้นจากเทคโนโลยี Web 2.0 สิ่งที่ตามมา เป็นเรื่องยาก
เพื่อเนื้อหาเกิดจากผู้ใช้งานทุกคน ทุกคนมีส่วนร่วมในการสร้างเนื้อบนเว็บไซต์ การควบคุมเรื่องนี้เป็นเรื่องยาก
เรามักได้ยินข่าวการโพสเรื่องราวการหมิ่นประมาทสิทธิส่วนบุคคล การกล่าวร้าย การกล่าวเท็จ ปิดเบือนข้อเท็จจริง บน Web 2.0 รวมถึงพวก Web Board อยู่ตลอดทั้งปี ไม่ว่าเป็น Youtube , Camfroge , Myspace.com เป็นต้น
หรือแม้เว็บไทยของเราก็มีจำนวนไม่น้อยที่เกิดเรื่องเหล่านี้ การควบคุมทัศนะคติแต่บุคคลที่เข้ามา Post
เนื้อหาในเว็บเป็นเรื่องที่ควบคุมลำบาก แต่เป็นเรื่องไม่ยากในการทราบที่มาที่ไปของการ Post สิ่งเหล่านี้
จึงทำให้มีการหลอกหลวงจากความรู้เท่าไม่ถึงการณ์จากการใช้งาน Web 2.0 มากขึ้น
และผลการคาดการแล้วพบว่าอาจเกิดมีผู้โจมตีจะใช้เวบไซต์ที่ใช้เทคโนโลยี Web 2.0 เพื่อแพร่กระจายมัลแวร์และรวบรวมข้อมูลต่าง ๆ ที่ต้องการจากเว็บเพื่อค้นหาข้อมูลที่ผู้ใช้แชร์ไว้เพื่อทำให้การโจมตีดู เหมือนจริงมากยิ่งขึ้น

ภัยคุกคามอันดับที่ 9 การหลอกลวงจากการใช้เทคโนโลยี VoIP : ในปีคศ.2007 จำนวนของช่องโหว่ที่รายงานเกี่ยวกับ VoIP มากกว่ารายงานช่องโหว่ในปีคศ.2006 ถึงสองเท่า นอกจากนี้ยังมีรายงานเกี่ยวกับการโจมตีที่เรียกว่า vishing และ phreaking ซึ่งอาจเกิด Spam บน VoIP และการหลอกลวงจาก Botnet ที่เป็นเสียงมากับมือถือโดยใช้เทคนิค (Social Engineering) ได้เช่นกัน

VoIP-Voice Over IP หรือที่เรียกกันว่า "VoIP Gateway" หมายถึง การส่งเสียงบนเครือข่ายไอพี
เป็นระบบที่แปลงสัญญาณเสียงในรูปของสัญญาณไฟฟ้ามาเปลี่ยนเป็นสัญญาณดิจิตอล คือ นำข้อมูลเสียงมาบีบอัดและบรรจุลงเป็นแพ็กเก็ตไอพี (IP) แล้วส่งไปโดยมีเราเตอร์ (Router) ที่เป็นตัวรับสัญญาณแพ็กเก็ต และแก้ปัญหาบางอย่างให้ เช่น
การบีบอัดสัญญาณเสียงให้มีขนาดเล็กลง การแก้ปัญหาเมื่อมีบางแพ็กเก็ตสูญหาย หรือได้มาล่าช้า
(delay)การสื่อสารผ่านทางเครือข่ายไอพีต้องมีเราเตอร์ (Router) ที่ทำหน้าที่พิเศษเพื่อประกันคุณภาพช่องสัญญาณไอพีนี้
เพื่อให้ข้อมูลไปถึง ปลายทางหรือกลับมาได้อย่างถูกต้องและอาจมีการให้สิทธิพิเศษก่อนแพ็กเก็ตไอพี อื่น (Quality of Service : QoS)
เพื่อการให้บริการที่ทำให้เสียงมีคุณภาพ

นอก จากนั้น Voice over IP (VoIP) ยังเป็นการส่งข้อมูลเสียงแบบ 2 ทางบนระบบเครือข่ายแบบ packet-switched IP network.
ซึ่งข้อมูลนี้จะถูกส่งผ่านเครือข่ายอินเตอร์เน็ตสาธารณะเพื่อสื่อสารระหว่าง VoIP ด้วยกัน โดยที่ยังคงความเป็นส่วนตัวไว้ได้

เทคโนโลยีนี้ยังใหม่ และยังขาดวิธีที่ใช้ในการป้องกัน คาดว่าจะมีการโจมตี VoIP เพิ่มขึ้นร้อลละ 50 ในปีคศ.2008 หรือแม้แต่กระทั่งมัลแวร์ (Malware) ที่โจมตี VoIP แพร่กระจายสู่วงกว้าง



รูปที่ 5 อัตราภัยคุกคามจาก VoIP ในแต่ละปี

ภัยคุกคามอันดับ 10 :การติดกับดักทางข้อมูล (Information pitfall) เรื่องนี้ผมถือว่าเป็นเรื่องใหญ่
และเคยเขียนบทความเรื่องนี้ในเดือนเมษายน ปี 2007 ที่บอกว่าเป็นเรื่องใหญ่เพราะว่าเป็นการสร้างความเชื่อให้เกิดขึ้นกับบุคคล
การสร้างกลยุทธการตลาดเข้ามาเพื่อสร้างภาพ สร้างความเชื่อ หากเป็นความเชื่อที่เป็นสิ่งที่ถูกต้อง และมีคุณธรรม ก็ดีไป
แต่หากเป็นการสร้างความเชื่อ เพื่อหลอกหลวง ก็จะทำให้เกิดความเสียหายได้เช่นกัน ตัวอย่างเราจะพบว่า Scam Web , Phishing Web ,

Adsware ที่ติดมากับ Web ถึงแม้จะจำนวนน้อยลงเพราะคนเริ่มตะหนักถึงภัยคุกคามที่ตามจากเข้าเว็บพวกนี้
แต่ก็ยังมีจำนวนคนไม่น้อยที่ยังตกเป็นเหยื่ออยู่ตลอดทั้งปี สิ่งนี้จะจางหายไปกับกับระบบป้องกันภัยทั้งด้านระบบป้องกันภัยทางเครือข่าย (Network) และระบบป้องกันภัยระดับเครื่องคอมพิวเตอร์ (Host) ที่มีความทันสมัยและฉลาดในวิธีการป้องกันภัยมากขึ้น ถึงอย่างไรก็ตาม การสร้างค่านิยม ถือว่ามีความเกี่ยวพันกับความมั่นคงของชาติในอนาคต มันอาจเป็นเรื่องพูดได้ยากในขณะนี้ เพราะทุกคน ยินดีต้อนรับเทคโนโลยีที่มาจากต่างประเทศ โดยไม่คิดว่าผลสืบเนื่องในอนาคต ความเชื่อ จากค่านิยม ที่คิดว่าต่างประเทศดีกว่าเรา เป็นเรื่องยากที่แก้ไข แต่ไม่สายที่ดำเนินการ ถึงเวลาที่เราทุกคนต้องสร้างความเชื่อมั่นว่า คนไทยไม่แพ้ใคร ไม่ได้ด้อยไปกว่าใครในโลกนี้

สวัสดีปีใหม่ครับ

นนทวรรธนะ สาระมาน

หัวหน้าทีมพัฒนาวิจัยระบบ SRAN