BẢN TIN
AN TOÀN THÔNG TIN
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA

Số 02
tháng 5/2017

CHỊU TRÁCH NHIỆM XUẤT BẢN
ThS. Lê Xuân Lâm
Giám đốc Trung tâm CNTT&TT
Thanh Hóa

BIÊN SOẠN
Cao Việt Cường; Trần Ngọc Hưng;
Trịnh Ngọc Quỳnh; Chúc Anh Hòa

THIẾT KẾ
Chung Nguyễn

TRUNG TÂM CÔNG NGHỆ THÔNG TIN
& TRUYỀN THÔNG THANH HÓA
Địa chỉ: 73 Hàng Than, TP Thanh Hóa
Điện thoại: 02373.718.298
Fax: 02373.718.299
Website: ict.thanhhoa.gov.vn
Giấy phép xuất bản số: 10/GP-XBBT
Sở TTTT Thanh Hóa cấp ngày 23/1/2017

In 500 cuốn, khổ 19x27cm
Tại Công ty TNHH In&TBGD Thanh Huệ
In xong và nộp lưu chiểu tháng 5/2017

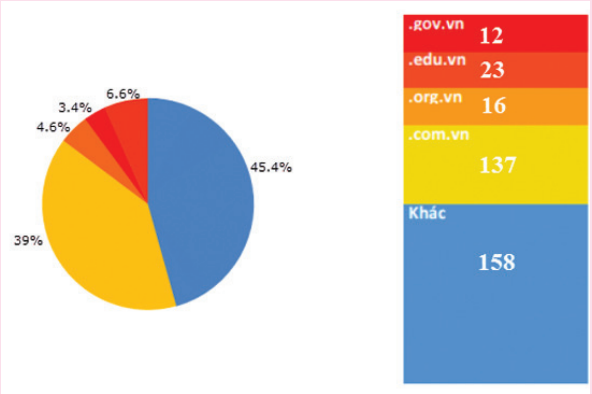
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CƠ QUAN NHÀ NƯỚC TỈNH THANH HÓA
Thách thức và giải pháp

ThS. LÊ XUÂN LÂM
Giám đốc Trung tâm CNTT&TT Thanh Hóa

Ngày nay, công nghệ thông tin (CNTT) đã góp phần không nhỏ vào công tác quản lý nhà nước của các cơ quan từ cấp trung ương đến địa phương, nhất là trong việc xử lý hồ sơ, thủ tục hành chính, quản lý ngân sách, tài chính, bảo hiểm xã hội... Việc đẩy mạnh phát triển và ứng dụng CNTT trên tất cả các lĩnh vực đã góp phần tháo gỡ nhiều khó khăn, vướng mắc, tạo thuận lợi cho người dân và doanh nghiệp, nâng cao hiệu lực, hiệu quả quản lý nhà nước.

Trong thời gian qua, tình hình mất an toàn thông tin mạng diễn biến ngày càng phức tạp, xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin nhằm phát triển KT-XH và đảm bảo QP-AN. Tuy nhiên, trong khi các cuộc tấn công mạng ở trong và ngoài nước đang gia tăng cả về quy mô, cường độ và mức độ tinh vi thì công tác bảo đảm an toàn, an ninh thông tin mạng của chúng ta lại đang bộc lộ một số bất cập về hạ tầng, nhân lực và nhận thức an toàn, an ninh thông tin. Đặc biệt, trong khoảng thời gian cuối tháng 7 đầu tháng 8 năm 2016, một loạt các hệ thống thông tin quan trọng bị tin tặc tấn công như việc tấn công thay đổi giao diện website và các hệ thống thông tin thuộc sự quản lý của Tổng công ty Hàng không Việt Nam (Vietnam Airlines) và một số đơn vị liên quan khác bị tấn công, gây ra các thiệt hại trực tiếp về kinh tế cho các đơn vị, tăng nguy cơ làm lộ, lọt các bí mật của các cơ quan đơn vị.

Tại Thanh Hóa, theo ghi nhận của bộ phận An toàn thông tin của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa, trong năm 2016 số lượng Website liên quan đến cơ quan, đơn vị nhà nước bị tin tặc tấn công là 51 website; đã tiến hành gửi công văn trực tiếp cảnh báo cho 08 đơn vị và phối hợp xử lý, khắc phục cho 16 đơn vị. Bên cạnh đó hình thức lây nhiễm mã độc, đặc biệt là mã độc mã hóa dữ liệu đòi tiền chuộc (Ransomware) có chiều hướng tăng mạnh với 11 cơ quan, đơn vị *(so với 05 đơn vị trong năm 2015)* bị lây nhiễm làm mất mát dữ liệu của các cá nhân và cơ quan.



Thống kê số lượng Website bị tấn công trên địa bàn tỉnh năm 2016.

Như vậy, tình hình an toàn thông tin xuất hiện nhiều nguy cơ đe dọa nghiêm trọng việc đẩy mạnh ứng dụng CNTT trong phát triển kinh tế - xã hội, đảm bảo quốc phòng - an ninh của cả nước nói chung và các địa phương, cơ quan, đơn vị nói riêng.

Về nguy cơ, thách thức đảm bảo an toàn thông tin

Nhận thức rõ vấn đề này, từ nhiều năm qua, Sở Thông tin và Truyền thông đã tham mưu cho UBND tỉnh triển khai nhiều giải pháp để đối phó với các nguy cơ gây mất an toàn, an ninh thông tin nói chung và công tác ứng cứu xử lý sự cố máy

tính nói riêng. Với chức năng, nhiệm vụ được Chủ tịch UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông giao trong vai trò là đầu mối tiếp nhận và xử lý ứng cứu sự cố máy tính nói chung và an toàn thông tin nói riêng; Trung tâm CNTT&TT (Trung tâm) luôn đề cao và triển khai tốt công tác phối hợp điều phối và cảnh báo sớm sự cố tới các cơ quan, tổ chức trên địa bàn tỉnh

Bên cạnh các hình thức hỗ trợ gián tiếp qua số điện thoại đường dây nóng, qua phần mềm hỗ trợ công tác ứng cứu từ xa. Trung tâm đã chủ động xây dựng kế hoạch từ đầu năm để triển khai trực tiếp hỗ trợ tại các các cơ quan, tổ chức, doanh nghiệp thực hiện các hoạt động phòng ngừa, ngăn chặn, ứng cứu, khôi phục nhằm đối phó với các loại tấn công phá hoại trên môi trường mạng cho các hệ thống thông tin của tỉnh. Trong quá trình triển khai công tác đảm bảo an toàn thông tin trên địa bàn tỉnh. Bên cạnh các nguy cơ và thách thức thường trực về mất an toàn thông tin đang hiện hữu thì Trung tâm nhận thấy có hai thách thức nổi cộm về công tác đảm bảo an toàn thông tin tại các cơ quan, đơn vị nhà nước trên địa bàn tỉnh như sau:

Một là, tại các Sở, ban, ngành và UBND cấp huyện chưa có bộ phận riêng biệt chuyên về an toàn, an ninh thông tin. Trong khi đó, nhân sự chuyên trách cũng chỉ là một vị trí kiêm nhiệm của bộ phận CNTT. Như vậy, ngay với đội ngũ phụ trách CNTT chưa thể là "chuyên gia" trong lĩnh vực này thì với người sử dụng máy tính thông thường, việc đảm bảo ATTT sẽ rất khó được chú ý. Trong khi đó với yêu cầu nhiệm vụ hiện nay, phần lớn hoạt động nghiệp vụ được sử dụng trên máy tính và môi trường mạng thì nguy cơ lộ, lọt thông tin, không đảm bảo ATTT càng lớn. Hệ thống CNTT của các Sở, ban ngành và địa phương trên địa bàn tỉnh có thể được trang bị các giải pháp, thiết bị an toàn, an ninh thông tin nhằm ngăn chặn tấn công, đe dọa từ bên ngoài. Tuy nhiên, có một điều dễ nhận thấy, dù cho hệ thống nào, máy móc nào thì con người vẫn là nhân tố sử dụng, điều khiển. Thế nên, chỉ cần người quản trị hệ thống sử dụng sơ suất, thiếu hiểu biết không tuân thủ các quy trình bảo mật thông tin cũng có thể trở thành công cụ tiếp tay cho tin tặc xâm nhập và như vậy, mức độ rủi ro, thiệt hại là rất lớn khi không chỉ thông tin cá nhân mà cả thông tin của cơ quan, đơn vị cũng có thể bị đánh cắp và phá hủy.

Hai là, qua công tác hỗ trợ và trao đổi với các cán bộ, công chức trên địa bàn tỉnh sử dụng máy tính hiện nay thì việc chú ý, quan tâm đảm bảo an toàn thông tin cho chính cá nhân và cơ quan chưa được coi trọng. Đặc biệt là nhận thức về ATTT chưa đầy đủ, dẫn đến tình trạng để lây nhiễm mã độc, sử dụng các phần mềm không có bản quyền hoặc không có nguồn gốc rõ ràng, buông lỏng trong trách nhiệm sử dụng hệ thống CNTT của cơ quan, đơn vị. Đa số người dùng chỉ tập trung vào việc ứng dụng, sử dụng các phần mềm CNTT vào hoạt động chuyên môn mà quên việc đảm bảo ATTT. Vấn đề mất an toàn thông tin trong các cán bộ, công chức thường được suy nghĩ đơn giản theo hướng máy tính làm việc bị nhiễm Virus làm hoạt động chậm hoặc cản trở việc thực hiện một vài thao tác trong công việc. Song thực tế, việc không đảm bảo ATTT gây ra những mối nguy hại rất lớn, không chỉ máy tính bị tấn công, lây nhiễm mã độc, đánh cắp thông tin, mã hóa dữ liệu, tống tiền nạn nhân mà còn ảnh hưởng tới toàn bộ hệ thống CNTT của cơ quan, đơn vị.

Về giải pháp giảm đảm bảo an toàn thông tin

Trước các nguy cơ hiện hữu về mất an toàn thông tin đặc biệt là các hoạt động lấy cắp thông tin, tấn công trên không gian mạng đang diễn ra trên diện rộng với nhiều phương thức và thủ đoạn khác nhau. Việc đảm bảo an toàn và bảo mật thông tin phải được thực hiện chặt chẽ và đồng bộ ở tất cả các phương diện: từ việc tăng cường nhận thức và ý thức của người sử dụng cho đến công tác quản lý, đầu tư, triển khai, sử dụng hệ thống công nghệ thông tin-viễn thông, hoàn thiện hành lang pháp lý về an toàn thông tin, tăng cường hợp tác, liên kết trong phạm vi quốc gia và quốc tế trong việc phòng, chống chiến tranh mạng,... phải được xem xét một cách tổng thể, nếu sơ hở hay xem nhẹ ở một khía cạnh nào đó đều có thể dẫn tới tình trạng mất an toàn thông tin, đe dọa đến an ninh quốc gia và trật tự an toàn xã hội. Trên cơ sở đó, Trung tâm đề xuất một số giải pháp đảm bảo an toàn thông tin cho

các cơ quan nhà nước trên địa bàn tỉnh như sau:

Một là, tiếp tục đẩy mạnh công tác quản lý nhà nước về an toàn thông tin trên địa bàn tỉnh. Tăng cường tuyền truyền, phổ biến, quán triệt các chủ trương, đường lối của Đảng, các chính sách, quy định của Chính phủ và của tỉnh trong hoạt động ứng dụng và phát triển CNTT. Đặc biệt là trong việc đảm bảo an toàn thông tin như Luật An toàn thông tin mạng năm 2016; Nghị quyết số 36/NQ-TW ngày 01/7/2014 của Bộ Chính trị Ban Chấp hành Trung ương Đảng Cộng sản Việt Nam về đẩy mạnh ứng dụng, phát triển CNTT đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế; Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư Trung ương Đảng (Khóa XI) về tăng cường công tác bảo đảm an toàn thông tin; Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới; Chỉ thị số 22/CT-UBND ngày 19/10/2015 của UBND tỉnh Thanh Hóa về việc tăng cường đảm bảo an ninh và an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh Thanh Hóa...

Hai là, tiếp tục triển khai hiệu quả nhằm đạt được các mục tiêu đề ra của Quyết định 893/QĐ-TTg ngày 19/6/2015 của Thủ tướng Chính phủ về phê duyệt Đề án tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020; Kế hoạch 152/KH-UBND ngày 11/11/2015 của UBND tỉnh Thanh Hóa về Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin trên địa bàn tỉnh Thanh Hóa đến năm 2020. Qua đó, tăng cường công tác tuyên truyền nâng cao nhận thức, trách nhiệm cho đội ngũ cán bộ, công chức, viên chức về công tác đảm bảo an ninh, an toàn thông tin mạng. Coi đây là nhiệm vụ quan trọng, cấp bách, thường xuyên, lâu dài của cả hệ thống chính trị.

Ba là, kiến nghị các Sở, ban ngành và UBND cấp huyện thành lập hoặc chỉ định bộ phận chuyên trách về an toàn, an ninh thông tin tại nội bộ các cơ quan, đơn vị. Tăng cường đào tạo, tập huấn bồi dưỡng kiến thức chuyên sâu về an toàn, bảo mật thông tin cho đối tượng cán bộ chuyên trách này để làm hạt nhân triển khai các giải pháp, quy trình đảm bảo an toàn trong đơn vị./.

Thị xã Bỉm Sơn là đơn vị hành chính nằm ở phía Bắc tỉnh Thanh Hoá, được xác định là đô thị hạt nhân của vùng kinh tế động lực của tỉnh, diện tích tự nhiên: 6.628,52 ha, có 8 đơn vị hành chính gồm 6 phường và 2 xã. Dân số trên toàn đô thị hơn 70.000 người. Để đảm bảo phát triển KT-XH, QP-AN trên mọi mặt, UBND Thị xã Bỉm Sơn đã xác định xây dựng một nền hành chính công theo hướng Chính phủ điện tử, đáp ứng thời kỳ công nghiệp hóa, hiện đại hóa đất nước. Vì vậy thị xã đã chọn khâu đột phá trong QLNN nói chung và chỉ đạo điều hành nói riêng đó chính và việc ứng dụng CNTT trong hoạt động cơ quan hành chính nhà nước trên địa bàn.

Từ năm 2004, UBND thị xã Bỉm Sơn đã xây dựng hệ thống mạng LAN với 10 máy tính nối mạng, đến nay hệ thống đã phát triển với hơn 100 máy tính và nhiều thiết bị CNTT khác kết nối mạng LAN, WAN và Internet một cách đồng bộ. Hiện tại hệ thống mạng đang sử dụng dịch vụ cáp quang FTTH với băng thông lớn và sử dụng đường truyền số liệu chuyên dụng nên việc khai thác và ứng dụng CNTT khá hiệu quả.

Việc ứng dụng CNTT trong các hoạt động phát triển kinh tế, dịch vụ, thương mại, sản xuất kinh doanh, an ninh quốc phòng... gắn liền với việc đảm bảo an toàn thông tin mạng. Thời gian qua, tình hình mất an toàn, an ninh mạng diễn ra hết sức nghiêm trọng, nhất là việc lộ lọt bí mật Nhà nước trên hệ thống thông tin trọng yếu của Đảng, Nhà nước, các doanh nghiệp tài chính, ngân hàng. Các thế lực thù địch đã lợi dụng Internet để tuyên truyền, phá hoại tư tưởng, tấn công xâm nhập, phát tán virus, cài cắm phần mềm gián điệp, làm tê liệt hoạt động của các hệ thống mạng trọng yếu, gây thiệt hại lớn cho nhiều cơ quan, tổ chức, cá nhân... Theo Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) trong năm 2016, VNCERT đã ghi nhận tổng cộng 134.375 sự cố tấn công mạng của cả 3 loại hình Phishing (lừa đảo), Malware (mã độc) và Deface (thay đổi giao diện), tăng hơn 4,2 lần so với

Công tác đảm bảo an toàn thông tin
TẠI UBND THỊ XÃ BỈM SƠN

LÊ THỊ LAN
Phó CVP UBND Thị xã Bỉm Sơn

năm 2015 (tổng số sự cố tấn công mạng năm 2015 là 31.585 sự cố). Đặc biệt cuộc tấn công chiều ngày 29/7/2016 vào hệ thống Vietnam Airlines đã cảnh báo về tình hình mất an toàn thông tin tại Việt Nam.

Trước tình hình mất an toàn thông tin đang hiện hữu, trong thời gian qua, UBND Thị xã Bỉm Sơn cũng như nhiều đơn vị khác trong và ngoài tỉnh coi trọng công tác đảm bảo ATTT - đây là yếu tố quan trọng trong thời đại bùng nổ công nghệ

Bộ phận Tiếp nhận và Trả kết quả đang tiếp nhận hồ sơ giải quyết TTHC của nhân dân.

khoa học hiện nay. Thực hiện Kế hoạch số 152/KH-UBND, ngày 11/11/2015 của UBND tỉnh ban hành về việc tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin trên địa bàn tỉnh Thanh Hóa đến năm 2020. Để thực hiện tốt Kế hoạch trên, UBND thị xã Bỉm Sơn đã ban hành các văn bản có liên quan như: Kế hoạch số 1881/KH-UBND, ngày 02/12/2015 về việc tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin trên địa bàn Thị xã đến năm 2020; Công văn số 1909/UBND-VP, ngày 08/12/2015 về việc tăng cường công tác đảm bảo an toàn thông tin mạng trong thời gian Đại hội Đảng toàn quốc lần thức XII; Kế hoạch số 629/KH-UBND, ngày 05/4/2016 về việc tổ chức hội nghị tập huấn tuyên truyền nâng cao nhận thức và trách nhiệm về an toàn thông tin cho cán bộ công chức. Trong đó hướng dẫn Cán bộ, Công chức, Viên chức, Người lao động trong cơ quan UBND Thị xã Bỉm Sơn, các cơ quan, tổ chức, đơn vị, doanh nghiệp, trường học và UBND các xã phường các phương pháp sử dụng mạng, máy tính an toàn và biện pháp khắc phục cơ bản nhằm đảm bảo ATTT, bảo mật thông tin cho hệ thống thuộc đơn vị quản lý.

Cùng với việc quán triệt, triển khai các văn bản về an toàn thông tin mạng, UBND thị xã Bỉm Sơn đã quan tâm đầu tư cơ sở hạ tầng, trang thiết bị nhằm đảm bào an toàn thông tin mạng cho hệ thống mạng UBND Thị xã như đường truyền số liệu, thiết bị tường lửa, định tuyến... chống xâm nhập từ bên ngoài, đồng thời thường xuyên thực hiện bảo trì, cập nhật vá lỗi các phần mềm và cài đặt phần mềm diệt virus có bản quyền cho tất cả máy tính trong hệ thống mạng LAN. Do đó, đã hạn chế tối đa sự cố về mất ATTT trong hệ thống đảm bảo cho việc hệ thống hoạt động thông suốt để nâng cao yêu cầu ứng dụng CNTT trong công tác chỉ đạo điều hành và thực hiện nhiệm vụ chuyên môn của các phòng ban, đơn vị. Hiện tại, cán bộ chuyên trách về quản trị mạng của UBND Thị xã Bỉm Sơn có khả năng vận hành, quản lý, xử lý các sự cố đảm bảo hệ thống mạng, máy tính được thông suốt.

Để công tác đảm bảo an toàn thông tin được triển khai sâu rộng đến toàn dân đặc biệt là trong các cơ quan Nhà nước nói chung và thị xã Bỉm Sơn nói riêng, theo tôi cần thực hiện tốt các giải pháp sau:

- *Một là,* nâng cao nhận thức của cán bộ lãnh đạo các đơn vị về tầm quan trọng của công tác bảo đảm an toàn thông tin. Lãnh đạo phải là người đi đầu trong công tác đảm bảo an toàn thông tin đồng thời kiên quyết và có biện pháp xử lý đối với CB, CC, VC, người lao động không tuân thủ các quy định của cơ quan về việc đảm bảo an toàn thông tin.

- *Hai là,* tăng cường công tác tuyên truyền, phổ biến nâng cao nhận thức và trách nhiệm về an toàn thông tin cho cán bộ, công chức nói riêng và nhân dân nói chung. Bên cạnh đó cũng cần phải hướng dẫn kỹ năng cơ bản về an toàn thông tin khi sử dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

- *Ba là,* Cán bộ, công chức phải nêu cao vai trò trong việc tiếp nhận, chắt lọc các thông tin, nắm bắt được các nguy cơ, rủi ro mất an toàn thông tin có thể xảy ra, các nguồn thông tin độc hại, không chính thống, các kỹ năng cơ bản để tự bảo vệ bản thân, bảo vệ tổ chức, nâng cao tinh thần cảnh giác... khi sử dụng Internet và luôn tiên phong đi đầu, thường xuyên trau dồi kiến thức, trình độ chuyên môn kỹ thuật để cập nhật thường xuyên các thao tác xử lý cũng như bảo mật thông tin.

- *Bốn là,* quan tâm đầu tư trang thiết bị phần cứng, phần mềm nhằm hạn chế được các rủi ro về mất an toàn thông tin.

- *Năm là,* đào tạo nâng cao trình độ, kỹ năng cho cán bộ chuyên trách về CNTT tại các sở ban ngành và UBND cấp huyện về các biện pháp phòng, chống các nguy cơ mất an toàn thông tin mạng và các phương pháp xử lý các sự cố khi xảy ra mất an toàn thông tin.

Với việc xác định tầm quan trọng của ứng dụng công nghệ thông tin trong quản lý hành chính nói chung và chỉ đạo điều hành nói riêng, UBND Thị xã Bỉm Sơn đã chú trọng đến việc đảm bảo ATTT mạng và xem đây là yếu tố then chốt đảm bảo cho việc ứng dụng CNTT trong cơ quan QLNN nói chung và UBND Thị xã nói riêng ngày một hiện đại đáp ứng yêu cầu tiến tới Chính phủ điện tử theo chủ trương của Đảng và Nhà nước./.

Mã độc đòi tiền chuộc tác hại và cách phòng tránh

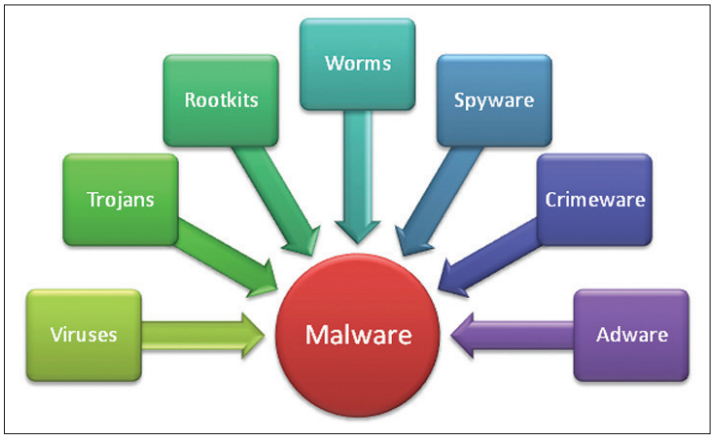
TRẦN NGỌC HƯNG
Phó Trưởng phòng Quản trị Hệ thống
Trung tâm CNTT&TT Thanh Hóa

Mã độc là gì?

Mã độc là một khái niệm chung dùng để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán (hoặc không lây lan, phát tán) trên hệ thống máy tính và internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức. Thực hiện các hành vi trục lợi cá nhân, kinh tế, chính trị hoặc đơn giản là để thỏa mãn ý tưởng và sở thích của người viết.

Phân loại và đặc tính

Tuỳ thuộc vào cơ chế, hình thức lây nhiễm và phương pháp phá hoại mà người ta phân biệt mã độc thành nhiều loại khác nhau: virus, trojan, backdoor, adware, spyware... Đặc điểm chung của mã độc là thực hiện các hành vi không hợp pháp (hoặc có thể hợp pháp, ví dụ như các ***addon*** quảng cáo được thực thi một cách hợp pháp trên máy tính người dùng) nhưng không theo ý muốn của người sử dụng máy tính. Dưới đây chúng ta sẽ phân loại các mã độc theo các hành vi nguy hiểm mà nó thường xuyên thực hiện:



Trojan/ Backdoors: không tự tái tạo, không gắn vào một tập tin như virus, thay vào đó được cài đặt vào hệ thống bằng cách giả làm một phần mềm hợp lệ và vô hại sau đó cho phép tin tặc điều khiển máy tính từ xa. Một trong những mục đích phổ biến nhất của trojan là biến máy tính thành một phần của mạng máy tính ma (Botnet).

Spyware: là phần mềm cài đặt trên máy tính người dùng nhằm thu thập các thông tin người dùng một cách bí mật, không được sự cho phép của người dùng.

Adware: phần mềm quảng cáo, hỗ trợ quảng

cáo, là các phần mềm tự động tải, pop up, hiển thị hình ảnh và các thông tin quảng cáo để ép người dùng đọc, xem các thông tin quảng cáo. Các phần mềm này không có tính phá hoại nhưng nó làm ảnh hưởng tới hiệu năng của thiết bị và gây khó chịu cho người dùng.

Ransomware: đây là phần mềm khi lây nhiễm vào máy tính sẽ kiểm soát dữ liệu hoặc chiếm quyền điều khiển máy tính và yêu cầu nạn nhân phải trả tiền để có thể khôi phục lại dữ liệu hoặc quyền kiểm soát với hệ thống.

Virus: là phần mềm có khả năng lây nhiễm trong cùng một hệ thống máy tính hoặc từ máy tính này sang máy tính khác dưới nhiều hình thức khác nhau. Quá trình lây lan được thực hiện qua hành vi lây file. Ngoài ra, virus cũng có thể thực hiện các hành vi phá hoại, lấy cắp thông tin...

Rootkit: là một kỹ thuật cho phép phần mềm có khả năng che giấu danh tính của bản thân nó trong hệ thống, các phần mềm antivirus từ đó nó có thể hỗ trợ các module khác tấn công, khai thác hệ thống.

Worm: có khả năng tự nhân bản trên chính nó mà không cần cấy vào một tập tin lưu trữ. Chúng còn thường sử dụng Internet để lây lan, do đó gây thiệt hại nghiêm trọng cho một mạng lưới về tổng thể, trong khi virus thường chỉ nhắm vào các tập tin trên máy tính bị nhiễm. Worm lây lan chủ yếu là do các lỗ hổng bảo mật của hệ thống

Keylogger: có khả năng ghi lại mọi phím bấm mà người dùng đã nhấn trên bàn phím. Tổng hợp kết quả của các tổ hợp phím này, kẻ cài đặt keylogger có thể thu được tin nhắn cá nhân, nội dung email, số thẻ tín dụng và dĩ nhiên nguy hiểm nhất là mọi loại mật khẩu của người dùng.

Tìm hiểu về mã độc đòi tiền chuộc

Khi đến cơ quan làm việc, bạn bật máy tính để bắt đầu thực hiện các công việc đang làm. Tuy nhiên bạn nhận thấy vấn đề đang xảy ra với mình là toàn bộ các dữ liệu mà bạn đang lưu trữ trên máy tính đã bị thay đổi và không thể xem được nội dung. Tiếp theo bạn thấy xuất hiện các cảnh báo về việc thực hiện các chỉ dẫn để lấy lại các file văn bản này bằng cách truy cập vào các trang web để nộp tiền cho người gây ra vấn đề này. Mã độc gây ra hiện tượng trên cho dữ liệu của bạn gọi là Mã độc đòi tiền chuộc (Ransomware). Đây là một loại phần mềm độc hại trong đó hạn chế quyền truy cập vào hệ thống máy tính mà nó lây nhiễm, và yêu cầu một khoản tiền chuộc trả cho các tác giả của phần mềm độc hại để các hạn chế được loại bỏ. Với trường hợp mã độc mã hóa tài liệu thì mã độc sẽ tiến hành mã hoá nội dung toàn bộ các dữ liệu trên máy nạn nhân với thuật toán mã hóa mạnh để không thể giải mã được với mục đích bắt cóc dữ liệu trên máy để tống tiền nạn nhân.

Phương thức lây nhiễm:

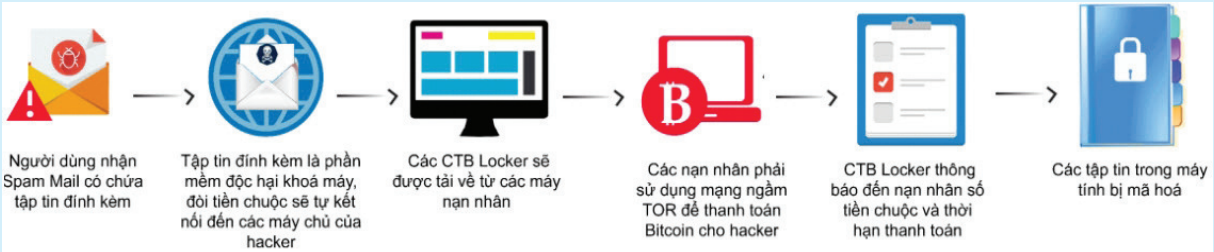
Theo cảnh báo của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) trong thời gian qua, Trung tâm ghi nhận cách thức tấn công mới của tin tặc nhằm vào các cơ quan tổ chức có sử dụng các hòm thư điện tử nội bộ. Theo đó, tin tặc sẽ giả mạo một địa chỉ điện tử có địa chỉ giống với địa chỉ thư điện tử trong cơ quan đó để gửi thư điện tử có kèm mã độc đến các người dùng nhằm qua mặt các hệ thống dò quét mã độc, các mã độc thường được nén lại dưới định dạng .zip hoặc .zar. Với việc giả mạo chính các địa chỉ thư điện tử của đơn vị sẽ làm cho người dùng khó phát hiện các thư giả mạo dẫn đến số lượng các máy tính bị lây nhiễm mã độc mã hóa dữ liệu có thể tăng cao.

Phương thức lây nhiễm chủ yếu của mã độc này là gửi tập tin đính kèm thư điện tử, khi người dùng mở tập tin thì mã độc sẽ tự động lây nhiễm vào máy tính người dùng. Gửi thư điện tử hoặc tin nhắn điện tử có chứa đường dẫn đến mã độc và yêu cầu người dùng tải về và cài đặt. Ngoài ra máy tính còn có thể bị lây nhiễm thông qua đường khác như qua các thiết bị lưu trữ, qua quá trình cài đặt phần mềm không rõ nguồn gốc, sao chép dữ liệu từ máy nhiễm,...!

Dấu hiệu nhận biết của loại mã độc sau khi máy tính bị nhiễm là các tài liệu, văn bản sẽ bị thay đổi nội dung và đổi tên phần mở rộng, phổ biến là các tập tin có định dạng: .doc, .docx, .pdf, .xls, .xlsx, .jpg, .txt, .ppt, .pptx,...một số loại còn khoá máy tính không cho sử dụng và đòi tiền chuộc.

Biện pháp phòng tránh

Trước đây, mã độc thường lây nhiễm vào máy tính của nạn nhân thông qua các phần mềm tiện ích, gần đây thủ đoạn lây nhiễm có thay đổi và



Quy trình lây nhiễm mã độc Ransomware thông qua Email

phức tạp hơn. Do vậy, để phòng ngừa, hạn chế tối đa khả năng bị nhiễm mã độc mã hóa dữ liệu trong hoạt động công vụ, các cơ quan, đơn vị cần thực hiện một số nội dung sau:

Tăng cường phòng ngừa để hạn chế tối đa khả năng bị nhiễm mã độc:

Phân quyền hợp lý cho các loại tài khoản người dùng, bảo vệ các tập tin không cho phép xoá, sửa nội dung các tập tin quan trọng; Cài đặt và thường xuyên cập nhật cho hệ điều hành, phần mềm chống mã độc như Kaspersky, Symantec, Avast, AVG, MSE, Bkav, CMC,... cho tất cả các máy tính của cán bộ, công chức, viên chức nhằm đảm bảo bảo mật, an toàn thông tin trên môi trường mạng; đồng thời, chú ý cảnh giác với các tập tin đính kèm, các đường liên kết ẩn được gửi đến thư điện tử người dùng, kể cả người gửi từ trong nội bộ; tuyệt đối không bấm vào các đường liên kết nhận được qua các tin nhắn trên mạng xã hội hay mở những thư điện tử không rõ nguồn gốc, nếu mở thì cần liên lạc với người gửi thông tin để xác thực hoặc mở các tập tin đính kèm trong các email đó trong môi trường cách ly an toàn (Safe Run) của các phần mềm diệt Virus và thực hiện các biện pháp kỹ thuật nhằm kiểm tra xác thực người dùng trên máy chủ gửi email của đơn vị, tránh bị giả mạo người gửi từ nội bộ; tắt các chế độ tự động mở, chạy tập tin đính kèm theo thư điện tử.

Thực hiện sao lưu dữ liệu định kỳ:

Sử dụng các ổ đĩa lưu trữ như Ổ cứng cắm ngoài, ổ đĩa USB để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong đưa ra cất giữ riêng; sử dụng các công cụ, giải pháp chuyên dụng để sao lưu dữ liệu như: các máy chủ quản lý tập tin, máy chủ sao lưu từ xa, các công cụ lưu trữ đám mây cho phép khôi phục lịch sử thay đổi của tập tin.

Xử lý khi phát hiện lây nhiễm mã độc:

Khi mã độc lây nhiễm vào máy tính, mã độc sẽ tiến hành quét và mã hoá các tập tin trong một khoảng thời gian. Do đó, việc phản ứng nhanh khi phát hiện ra sự cố có thể giúp giảm thiểu thiệt hại cho dữ liệu trên máy tính và tăng khả năng khôi phục dữ liệu bị mã hoá. Cụ thể cần thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính bằng cách ngắt nguồn điện trực tiếp.

- Không được khởi động lại máy tính theo cách thông thường mà phải khởi động từ hệ điều hành sạch khác (khuyến nghị hệ điều hành Linux) như từ ổ đĩa CD, USB,... sau đó thực hiện kiểm tra các tập tin dữ liệu và sao lưu các dữ liệu chưa bị mã hoá.

- Các tập tin đã bị mã hoá tương đối khó để giải mã, tuy nhiên trong một số trường hợp có thể sử dụng các phần mềm khôi phục dữ liệu như FTK, EaseUs, R-STUDIO,... để khôi phục các tập tin nguyên bản đã bị xoá.

- Cài đặt lại toàn bộ hệ thống, cài đặt phần mềm diệt virus đồng thời thiết lập chế độ cập nhật phiên bản tự động.

Để giúp các cơ quan chức năng theo dõi, phân tích và phản ứng nhanh chóng với các loại mã độc mới, ngay khi phát hiện xảy ra sự cố về mã độc Ransomware cần nhanh chóng thông báo về ***Tổ Ứng cứu sự cố mạng máy tính*** của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa theo địa chỉ dưới đây, để được hỗ trợ, xử lý kịp thời, hạn chế tối đa các nguy cơ mất an toàn thông tin mạng.

Thông tin liên hệ:
Điện thoại: (0237) 3718699;
Fax (037) 3718299.
Email: ungcuusuco@thanhhoa.gov.vn

RANSOMWARE - THÔNG TIN LIÊN QUAN

LÊ VĂN TUẤN
Trung tâm CNTT&TT Thanh Hóa

1. Mẫu Ransomware đầu tiên được phát hiện vào năm 2005

2. Ransomware được thiết kế để kiếm được lợi nhuận nhanh nhất có thể. 04 loại Ransomware mang lại nhiều lợi nhuận nhất là: Locker Ransomware; Crypto Ransomware; Ransomware giả mạo chương trình Antivirus; Ransomware đưa ra các cảnh báo giả mạo.

3. Mã độc tống tiền đã trải qua 04 sự thay đổi quan trọng để nâng cấp. Qua mỗi lần thay đổi, mã độc tống tiền đã chuyển từ loại mã độc này sang loại mã độc khác với cấp độ tinh vi hơn như tại thời điểm hiện tại.

4. Lợi nhuận trung bình của Ransomware là 300$ cho một lần lây nhiễm thành công và hình thức thanh toán được tội phạm ưa chuộc là sử dụng đồng tiền ảo Bitcon.

5. Giữa năm 2013 và 2014 cho thấy sự bùng nổ của Ransomware mã hóa dữ liệu trên không gian mạng với tốc độ tăng trưởng lên tới 250%.

6. Các nhóm tội phạm đứng sau Ransomware đang liên tục đổi mới về phương thức lây nhiễm và cách thức tấn công.

RANSOMWARE là gì?

Ransomware hay "mã độc tống tiền" là một loại phần mềm độc hại sử dụng hệ thống mật mã để mã hóa dữ liệu thuộc về một cá nhân hay tổ chức và ngăn chặn người dùng hợp pháp truy cập và sử dụng. Nạn nhân thường phải nộp một khoản tiền chuộc nếu muốn lấy lại dữ liệu hoặc đơn giản nhất là truy cập lại máy tính của mình.

PHÂN LOẠI RANSOMWARE

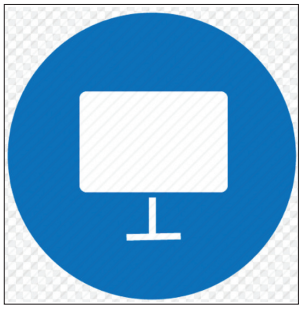
Locker Ransomware: Ngăn chặn người dùng truy cập vào máy tính hoặc thiết bị

Crypto Ransomware: Ngăn chặn người dùng truy cập dữ liệu hoặc tập tin, sử dụng hệ mật mã mạnh như AES, RSA để mã hóa dữ liệu người dùng.

Hai loại mã độc này được thiết kế để ngăn chặn người dùng truy cập vào chính các thông tin cá nhân quan trọng của họ và từ đó yêu cầu người dùng phải nộp một khoản tiền chuộc để có thể truy cập lại dữ liệu đã bị tin tặc mã hóa.

CÁC THIẾT BỊ DỄ BỊ ẢNH HƯỞNG

Thiết bị di động thông minh: Mặc dù Android chiếm tới 80% thiết bị di động trên toàn cầu nhưng lại có sự khác biệt lớn về bảo mật giữa iOS và Android. iOS sẽ là mục tiêu ít bị tấn công bởi Ransomware do iOS là một hệ điều hành đóng, mỗi ứng dụng trước khi phát hành đều được kiểm duyệt kỹ càng. Ngược lại, do tính chất của một nền tảng mở, Android là miếng mồi ngon cho nhiều phần mềm độc hại trong đó có Ransomware.



Máy tính cá nhân: Hiện nay có nhiều Ransomware được thiết kế nhắm mục tiêu tấn công tới máy tính cá nhân chạy Windows. Điều này là hiển nhiên khi Windows chiếm thị phần tới 89% và phần còn lại dành cho Mac OSX và Linux. Ransomware được thiết kế để mang lại lợi nhuận cho tội phạm mạng nhiều nhất nên không ngạc nhiên khi máy tính cá nhân chạy hệ điều hành Windows có nguy cơ bị tấn công cao hơn các hệ điều hành còn lại.

Hệ thống máy chủ: Máy chủ khác với toàn bộ mục tiêu còn lại của Ransomware. Máy chủ có nhiều khả năng chứa dữ liệu quan trọng ảnh hưởng tới toàn bộ hoạt động của tổ chức. Máy chủ có thể là trung tâm dữ liệu lưu trữ toàn bộ tài liệu, dữ liệu quan trọng của cơ quan, đơn vị và làm cho nó trở thành mục tiêu tiềm năng có giá trị cao đối với những tên tội phạm.

ĐỐI TƯỢNG TẤN CÔNG

Những kẻ tấn công đứng đằng sau Ransomware thực sự không quan tâm tới mục tiêu tấn công của chúng là ai miễn sao nạn nhân trả tiền chuộc. Chính vì lý do đó, những kẻ tấn công thường thực hiện một chiến dịch phát tán Ransomware liên tục trên một phạm vi rộng lớn nhằm tới mọi người dùng máy tính. Chỉ cần một phần nhỏ đối tượng đồng ý trả tiền chuộc cũng đủ để đạt được mục đích của tội phạm mạng và là động cơ để chúng tiếp tục thực hiện các cuộc tấn công tiếp theo...

HÌNH THỨC LÂY NHIỄM

Một trong những câu hỏi mà nhiều nạn nhân thắc mắc là "Ransomware đã lây nhiễm lên máy của mình như thế nào" Câu hỏi này không có một câu trả lời rõ ràng khi những kẻ tấn công có rất nhiều cách thức để phát tán mã độc lên máy nạn nhân.

Quảng cáo độc hại

Thư rác/ Thư giả mạo

Lổ hổng bảo mật

Botnet/ Downloader

CÁCH PHÒNG TRÁNH

Sao lưu dữ liệu thường xuyên: Bạn nên thực hiện sao lưu dữ liệu thường xuyên và sử dụng nhiều môi trường khác nhau để lưu trữ dữ liệu như điện toán đám mây, ổ đĩa di động... Đây là cách phòng chống hiệu quả nhất.

Cập nhật thường xuyên phần mềm: Tin tặc có thể lợi dụng các lỗ hổng từ các phần mềm, ứng dụng trên thiết bị để cài mã độc. Hãy đảm bảo rằng thiết bị của bạn được cập nhật các phần mềm với các bản vá lỗi mới nhất.

Kiểm tra nguồn gốc các Email được gửi tới: Hãy kiểm tra để xác thực nguồn gốc và độ tin cậy của các email trước khi bạn mở, click vào đường dẫn hay tải các file chứa trong email đó.

Cảnh giác với các Website giả mạo: Bạn nên chỉ truy cập và các website tin cậy, chính thống và tuyệt đối cảnh giác với các đường link quảng cáo không rõ nguồn gốc.

XỬ LÝ KHI BỊ LÂY NHIỄM

Một khi hệ thống của bạn bị tấn công bởi Ransomware, hãy thực hiện sao lưu ngày lập tức. Nếu không thể backup, bạn cần phải cố gắng lấy lại các tập tin như sau:

1. Tìm hiểu về loại Ransomware đang lây nhiễm và tìm kiếm biện pháp và công cụ gỡ bỏ trên Internet.

2. Sử dụng các công cụ khôi phục tập tin được cung cấp bởi các nhà cung cấp phần mềm khôi phục đáng tin cậy.

3. Liên hệ với các đơn vị chuyên trách về xử lý sự cố để có biện pháp xử lý nhanh nhất./.

CÁC KỸ NĂNG NÂNG CAO HIỆU QUẢ PHÒNG CHỐNG MÃ ĐỘC HẠI

HOÀNG ANH TUẤN
Trung tâm CNTT&TT Thanh Hóa

Mã độc (Malware) viết tắt của từ ***Malicious Software***: Là những chương trình phần mềm được thiết kế để gây hại hoặc làm những hành động không mong muốn đối với người dùng trên hệ thống máy tính.

Như vậy: Mã độc bản chất là một phần mềm như những phần mềm khác trên máy tính mà chúng ta vẫn sử dụng hằng ngày, nó có đầy đủ những đặc điểm, tính chất của một phần mềm bình thường chỉ khác là nó có thêm tính độc hại (malicious)

Việc phòng tránh mã độc cần được thực hiện đồng bộ trên tất các thành phần trong hệ thống thông tin của các cơ quan, đơn vị. Sau đây là hướng dẫn các kỹ năng nâng cao trong việc phòng chống hiệu quả các loại mã độc thông thường đang hoạt động hiện nay.

Bước 1. Kiểm tra, phát hiện các tiến trình độc hại đang chạy trên máy tính.

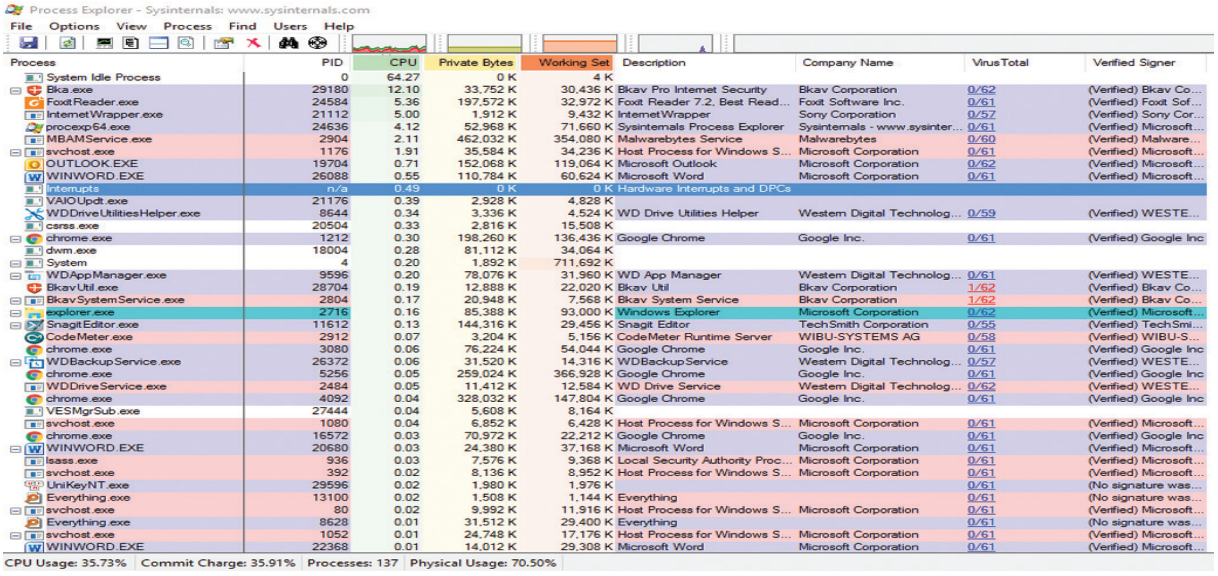
Một trong những chức năng quan trọng thường có ở các mã độc là khả năng ẩn mình trên hệ thống bị lây nhiễm. Trong đó các tiến trình của mã độc thường sử dụng các tên gần giống hoặc giống hoàn thoàn với các tiến trình thật của máy tính.

Để người dùng phát hiện ra các tiến trình nghi ngờ là tiến trình của mã độc qua đó xác định và thực hiện các biện pháp bóc tách và loại bỏ mã độc này ra khỏi máy tính.

Trên máy tính chạy hệ điều hành Windows, người dùng có thể sử dụng chức năng Task Manager để thực hiện liệt kê các tiến trình đang chạy trong hệ thống. Tuy nhiên ứng dụng này thường chỉ cung cấp các thông tin cơ bản liên quan đến tiến trình mà thiếu đi các thông tin quan trọng khác phục vụ việc phân biệt rõ ràng đâu là tiến trình an toàn của hệ thống, đâu là tiến trình của mã độc.

Để khắc phục nhược điểm của ứng dụng có sẵn Task Manager. Chúng ta sử dụng 01 công cụ miễn phí khác là ***Process Explorer*** của hãng Microsoft. Công cụ này cung cấp nhiều hơn thông tin liên quan đến các tiến trình trên hệ thống cho người dùng và được download trực tiếp từ Website của Microsoft theo đường dẫn sau:

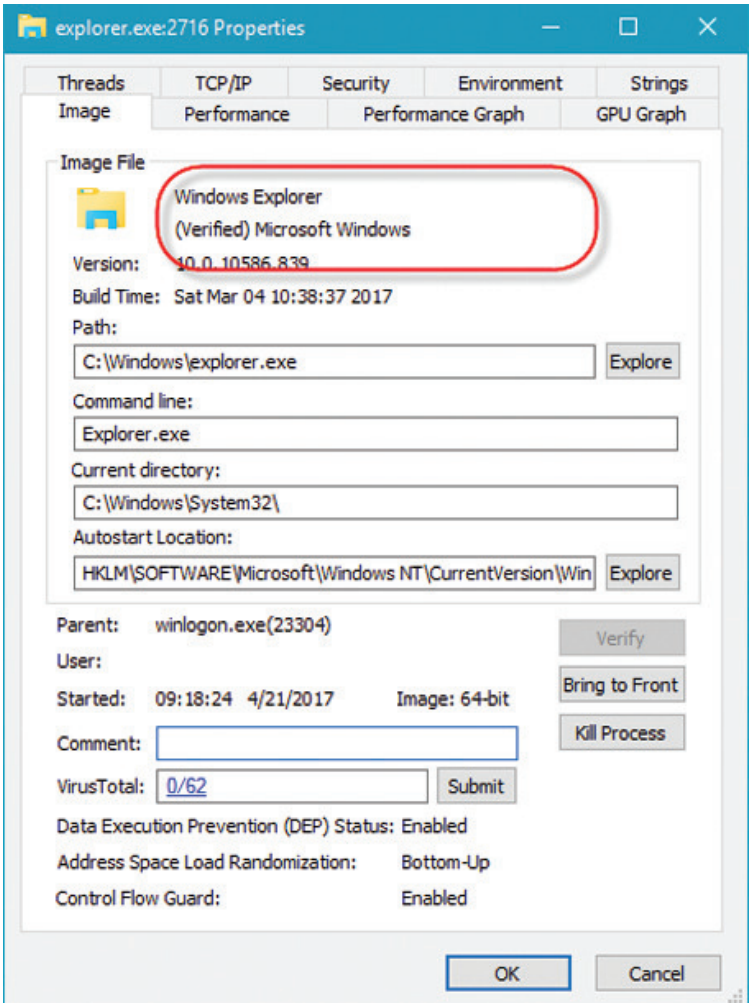
https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx



Process	PID	CPU	Private Bytes	Working Set	Description	Company Name	VirusTotal	Verified Signer
System Idle Process	0	64.27	0 K	4 K				
Bka.exe	29180	12.10	33,752 K	30,436 K	Bkav Pro Internet Security	Bkav Corporation	0/62	(Verified) Bkav Co...
FoxitReader.exe	24584	5.36	197,572 K	32,972 K	Foxit Reader 7.2. Best Read...	Foxit Software Inc.	0/61	(Verified) Foxit Sof...
InternetWrapper.exe	21112	5.00	1,912 K	9,432 K	InternetWrapper	Sony Corporation	0/57	(Verified) Sony Cor...
procexp64.exe	24636	4.12	52,968 K	71,660 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...	0/61	(Verified) Microsoft...
MBAMService.exe	2904	2.11	462,032 K	354,080 K	Malwarebytes Service	Malwarebytes	0/60	(Verified) Malware...
svchost.exe	1176	1.91	35,584 K	34,236 K	Host Process for Windows S...	Microsoft Corporation	0/61	(Verified) Microsoft...
OUTLOOK.EXE	19704	0.71	152,068 K	119,064 K	Microsoft Outlook	Microsoft Corporation	0/62	(Verified) Microsoft...
WINWORD.EXE	26088	0.55	110,784 K	60,624 K	Microsoft Word	Microsoft Corporation	0/61	(Verified) Microsoft...
Interrupts	n/a	0.49	0 K	0 K	Hardware Interrupts and DPCs			
VAIOUpdt.exe	21176	0.39	2,928 K	4,828 K				
WDDriveUtilitiesHelper.exe	8644	0.34	3,336 K	4,524 K	WD Drive Utilities Helper	Western Digital Technolog...	0/59	(Verified) WESTE...
csrss.exe	20504	0.33	2,816 K	15,508 K				
chrome.exe	1212	0.30	198,260 K	136,436 K	Google Chrome	Google Inc.	0/61	(Verified) Google Inc
dwm.exe	18004	0.28	81,112 K	34,064 K				
System	4	0.20	1,892 K	711,692 K				
WDAppManager.exe	9596	0.20	78,076 K	31,960 K	WD App Manager	Western Digital Technolog...	0/61	(Verified) WESTE...
BkavUtil.exe	28704	0.19	12,888 K	22,020 K	Bkav Util	Bkav Corporation	1/62	(Verified) Bkav Co...
BkavSystemService.exe	2804	0.17	20,948 K	7,568 K	Bkav System Service	Bkav Corporation	1/62	(Verified) Bkav Co...
explorer.exe	2716	0.16	85,388 K	93,000 K	Windows Explorer	Microsoft Corporation	0/62	(Verified) Microsoft...
SnagitEditor.exe	11612	0.13	144,316 K	29,456 K	Snagit Editor	TechSmith Corporation	0/55	(Verified) TechSmi...
CodeMeter.exe	2912	0.07	3,204 K	5,156 K	CodeMeter Runtime Server	WIBU-SYSTEMS AG	0/58	(Verified) WIBU-S...
chrome.exe	3080	0.06	76,224 K	54,044 K	Google Chrome	Google Inc.	0/61	(Verified) Google Inc
WDBackupService.exe	26372	0.06	31,520 K	14,316 K	WDBackupService	Western Digital Technolog...	0/57	(Verified) WESTE...
chrome.exe	5256	0.05	259,024 K	366,928 K	Google Chrome	Google Inc.	0/61	(Verified) Google Inc
WDDriveService.exe	2484	0.05	11,412 K	12,584 K	WD Drive Service	Western Digital Technolog...	0/62	(Verified) WESTE...
chrome.exe	4092	0.04	328,032 K	147,804 K	Google Chrome	Google Inc.	0/61	(Verified) Google Inc
VESMgrSub.exe	27444	0.04	5,608 K	8,164 K				
svchost.exe	1080	0.04	6,852 K	6,428 K	Host Process for Windows S...	Microsoft Corporation	0/61	(Verified) Microsoft...
chrome.exe	15572	0.03	70,972 K	22,212 K	Google Chrome	Google Inc.	0/61	(Verified) Google Inc
WINWORD.EXE	20680	0.03	24,380 K	37,168 K	Microsoft Word	Microsoft Corporation	0/61	(Verified) Microsoft...
lsass.exe	936	0.03	7,576 K	9,368 K	Local Security Authority Proc...	Microsoft Corporation	0/61	(Verified) Microsoft...
svchost.exe	392	0.02	8,136 K	8,952 K	Host Process for Windows S...	Microsoft Corporation	0/61	(Verified) Microsoft...
UniKeyNT.exe	29596	0.02	1,980 K	1,976 K			0/61	(No signature was...
Everything.exe	13100	0.02	1,508 K	1,144 K	Everything		0/61	(No signature was...
svchost.exe	80	0.02	9,992 K	11,916 K	Host Process for Windows S...	Microsoft Corporation	0/61	(Verified) Microsoft...
Everything.exe	8628	0.01	31,512 K	29,400 K	Everything		0/61	(No signature was...
svchost.exe	1052	0.01	24,748 K	17,176 K	Host Process for Windows S...	Microsoft Corporation	0/61	(Verified) Microsoft...
WINWORD.EXE	22368	0.01	14,012 K	29,308 K	Microsoft Word	Microsoft Corporation	0/61	(Verified) Microsoft...

Thông qua chạy công cụ này, người dùng có thể thu thập được nhiều thông tin hơn về một tiến trình đang chạy trên hệ thống, bao gồm:

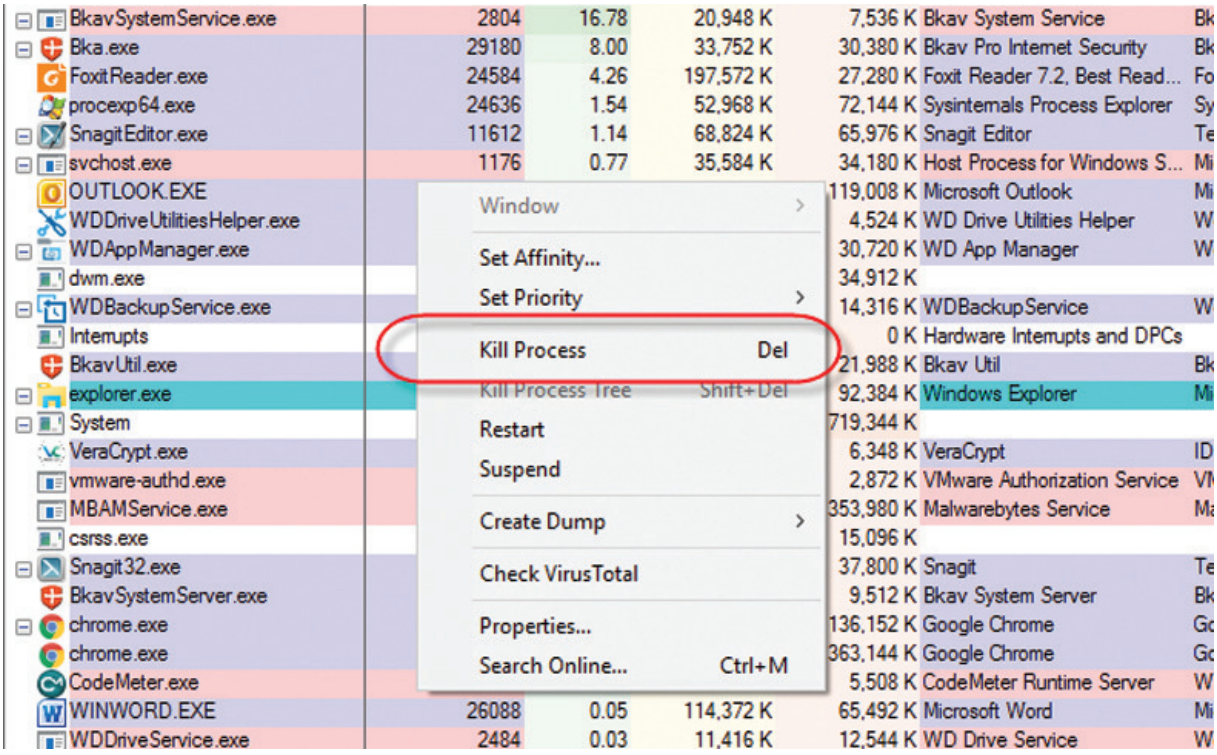
- Các tiến trình đang chạy
- Các thư viện "dll" mà tiến trình sử dụng
- Cây tiến trình để xác định tiến trình gốc khởi tạo
- Trạng thái của từng tiến trình
- Tài nguyên hệ thống mà tiến trình đang sử dụng
- Và nhiều thông tin liên quan khác



Để xác định một tiến trình bất thường, người dùng chú ý một số đặc điểm như sau:

- Tiến trình không có phần mô tả từ nhà sản xuất (Description)
- Tiến trình không có thông tin từ nhà sản suất (Company Name)
- Tiến trình có các hoạt động bất thường trên nền TCP/IP
- Tiến trình không thể xác thực chữ ký số của nhà sản xuất (Verified Signer)
- Kiểm tra tiến trình thông qua dịch vụ kiểm tra mã độc Virus Total được liên kết trực tiếp trên giao diện của công cụ.

Trong trường hợp xác định hoặc nghi ngờ tiến trình là mã độc. Người dùng tiến hành chức năng loại bỏ tạm thời tiến trình thông qua chức năng "kill" của công cụ.

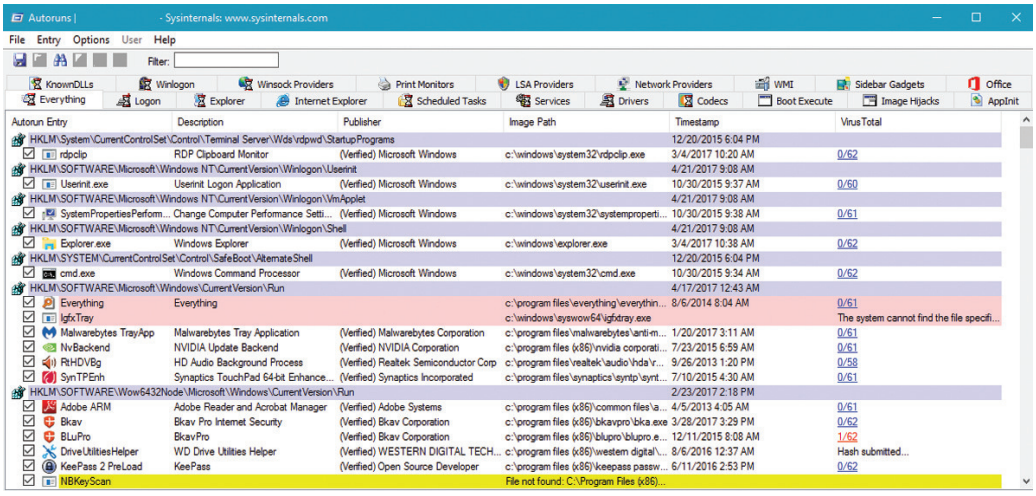


Bước 2. Kiểm tra, phát hiện các tiến trình tự động khởi động của mã độc

Sau khi kiểm tra, phát hiện các tiến trình nghi ngờ là mã độc hại đang tồn tại trên hệ thống. Ngoài việc sử dụng tính năng "Kill" để tạm thời loại bỏ tiến trình ở bước 1. Chúng ta cần thực hiện kiểm tra, phát hiện các mã độc chạy tự động khi hệ thống khởi động. Bởi vì, ngoài khả năng che dấu bản thân theo tên các tiến trình thông thường, mã độc còn có khả năng thiết lập các cơ chế tự động khởi tạo theo hệ thống khi hệ thống khởi động.

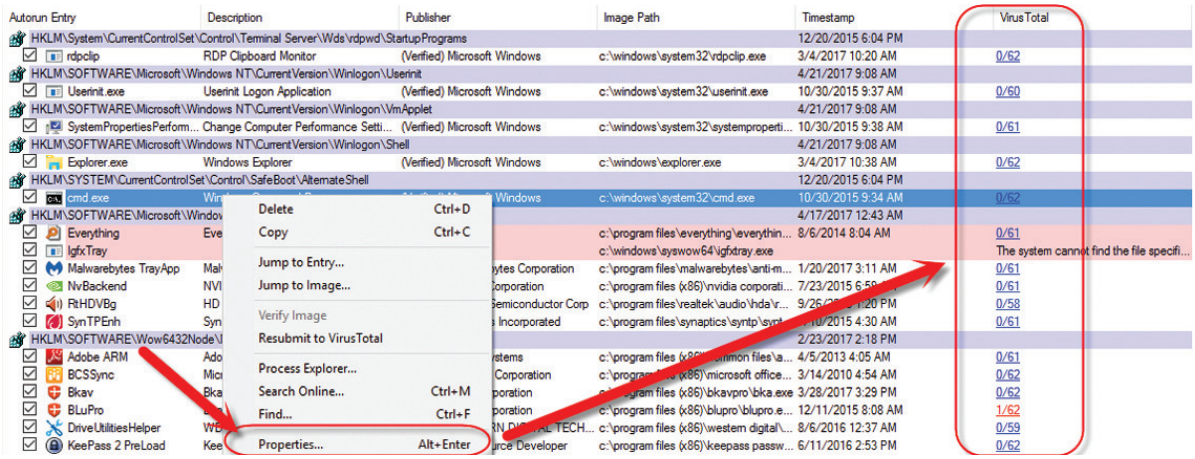
Để có thể phân tích các tiến trình tự khởi động cùng hệ thống. Chúng ta sử dụng công cụ thứ 2 là ***Autoruns*** cũng do Microsoft phát triển. Công cụ này cung cấp nhiều thông tin hữu ích hơn so với ứng dụng ***Startup*** được tích hợp sẵn trong Windows và được tải trực tiếp từ Website của Microsoft theo đường dẫn sau:

https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx



Với việc sử dụng công cụ này, chúng ta có thể liệt kê tất cả các cơ chế tái khởi động của các tiến trình như sau:

- Các dịch vụ (Services) tự động khởi động cùng hệ thống
- Các tác vụ (tasks) đã được đặt lịch cùng hệ thống
- Các phần mở rộng (addons) của ứng dụng được đăng ký tự động khởi tạo.
- Và các thông tin khác



Tương tự như với ứng dụng ***Process Explorer***, đối với ứng dụng ***Autoruns***, người dùng cần chú ý đến các ứng dụng đã được đăng ký tái khởi động cùng hệ thống nhưng không có các đặc điểm sau đây để qua đó xác định các tiến trình nghi ngờ là mã độc:

- Tiến trình không có xác thực chữ ký số của nhà sản xuất (Verified Signer)
- Tiến trình không có phần mô tả từ nhà sản xuất (Description)
- Tiến trình không có thông tin từ nhà sản suất (Company Name)

Sau khi xác định được các tiến trình nghi ngờ, chúng ta có thể sử dụng các thông tin được cung cấp từ công cụ này để tìm đến đường dẫn đầy đủ của các ứng dụng sử dụng các tiến trình này và dò quét bằng dịch vụ VirusTotal để xác định ứng dụng có phải mã độc hay không.

Trong trường hợp xác định ứng dụng đó là mã độc, chúng ta có thể gỡ bỏ ứng dụng đó khỏi hệ thống đồng thời loại bỏ các tiến trình này trong việc tái khởi động cùng hệ thống ở những lần khởi động tiếp theo.

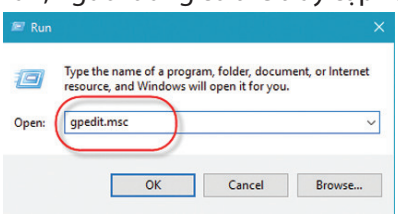
Bước 3. Thiết lập việc sử dụng USB, thiết bị lưu trữ ngoài

Các thiết bị lưu trữ bên ngoài cũng như USB là một trong những nguyên nhân chủ yếu gây ra việc lây lan mã độc trong môi trường mạng. Do đó, cần có các thiết lập đảm bảo an toàn thông tin cho việc sử dụng thiết bị lưu trữ ngoài trong hệ thống như:

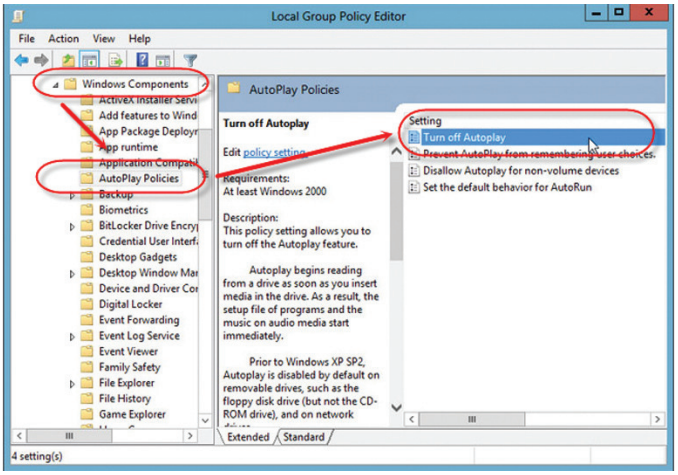
Bước 3.1. Ngăn chặn chức năng tự chạy (Autorun) đối với thiết bị lưu trữ USB:

Thông thường, mã độc thường sử dụng chức năng Autorun để lây lan thông qua các thiết bị lưu trữ gắn ngoài như USB, các ổ cứng gắn ngoài... Việc cấu hình này giúp ngăn chặn chức năng Autorun cho các thiết bị lưu trữ gắn ngoài là công việc đơn giản, nhưng hữu hiệu trong việc phòng chống mã độc tại các máy tính cá nhân trong cơ quan, đơn vị.

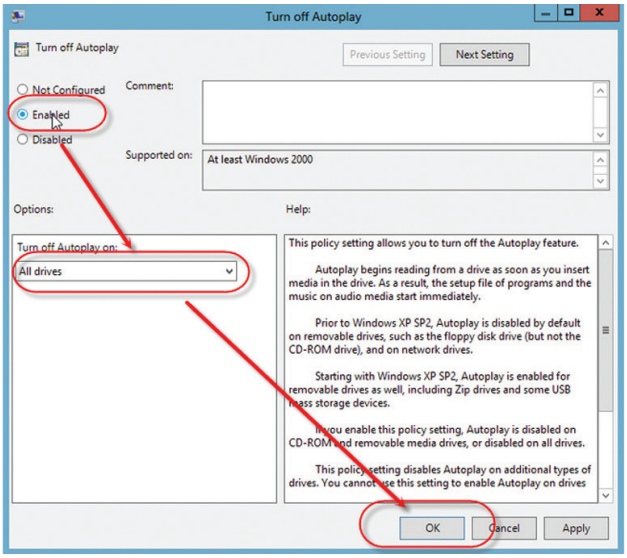
Để vô hiệu hóa chức năng Autorun, người dùng có thể truy cập vào: ***Windows -> Run -> gpedit.msc***



Sau đó vào phần ***Computer Configuration -> Administrative Templates -> Windows Components -> Autoplay Policies:***



Mở chức năng ***Turn off Autoplay*** và chọn Enable cũng như tùy chọn ***All driver*** để xác nhận:



Bước 3.2. Dò quét mã độc trước khi sử dụng thiết bị:

Ngoài việc loại bỏ chức năng Autorun đối với các thiết bị lưu trữ, người sử dụng cần hình thành thói quen sử dụng chương trình diệt Virus để dò quét mã độc trước khi sử dụng thiết bị.

Trong trường hợp, trên máy tính chưa được trang bị phần mềm diệt Virus có bản quyền. Người dùng có thể sử dụng các phần mềm diệt Virus phiên bản miễn phí. Sau đây là danh sách các phần mềm miễn phí để chúng ta lựa chọn cài đặt./.

Name	Avast Free Antivirus 2017	AVG AntiVirus Free (2017)	Bitdefender Antivirus Free Edition (2017)	Check Point ZoneAlarm Free Antivirus+ 2017	Sophos Home	Avira Antivirus (2017)	adaware antivirus free 12	Comodo Antivirus 10	Panda Free Antivirus (2017)	Qihoo 360 Total Security 8.6
Lowest Price	Free AVAST Software	Free AVG Technologies	Free Bitdefender	Free ZoneAlarm	Free Sophos	Free Avira	$0.00 MSRP	$0.00 MSRP	Free Panda Security	$0.00 MSRP

AN TOÀN THÔNG TIN
KHI SỬ DỤNG MẠNG KHÔNG DÂY

(Nguồn Cục An toàn thông tin - Bộ Thông tin và Truyền thông)

Trong những năm gần đây, mạng không dây ngày càng trở nên phổ biến, giá thành thấp và dễ sử dụng. Người dung có thể lắp đặt để truy cập mạng không dây tại nhà hoặc sử dụng máy tính xách tay, thiết bị di động thông minh để truy cập tại những nơi công cộng như quán café, sân bay, khách sạn...

Việc sử dụng mạng không dây sẽ rất tiện lợi và đơn giản nhưng nó cũng tiềm ẩn rất nhiều nguy cơ mất an toàn thông tin.

Nếu mạng không dây được bảo vệ đúng mức thì bất cứ một máy tính nào có hỗ trợ truy cập không dây nằm trong vùng phủ sóng của thiết bị phát sóng đều có thể kết nối để truy cập Internet. Ở ngoài trời, phạm vi này có thể đạt tới 300m. Vì vậy, bất cứ ai ở xung quanh cũng có thể dễ dàng truy cập vào thiết bị phát sóng này.

CÁC NGUY CƠ CÓ THỂ XẢY RA:

• **Bị xâm phạm dịch vụ**: dung lượng, số lượng kết nối... có thể vượt quá giới hạn mà nhà cung cấp dịch vụ cho phép, tốc độ có thể rất chậm do bị chiếm dụng băng thông.

• **Bị lợi dụng**: một số người có thể lợi dụng hệ thống để thực thi những hành động bất hợp pháp.

• **Bị theo dõi**: các hoạt động trên internet có thể bị theo dõi, những thông tin nhạy cảm (mật khẩu, số thẻ tín dụng có thể bị đánh cắp).

• **Bị tấn công**: các tệp tin trên máy tính có thể bị truy cập trái phép, máy tính có thể bị cài spyware và các chương trình độc hại khác.

Những việc cần làm khi truy cập Internet bằng mạng không dây công cộng

1. Sử dụng mạng riêng ảo

Yếu tố đầu tiên phải kể đến trong mặt tối của mạng không dây là sự tiện lợi, dễ dàng sử dụng mà không cần phải thiết lập hay cấu hình gì quá phức tạp. Tuy nhiên, yếu tố an ninh trong mạng không dây thường vẫn bị cho qua.

Khi đã kết nối laptop hay điện thoại của mình vào một mạng không dây nào đó, thì tất cả những thiết bị trong cùng mạng này có thể nhìn thấy nhau. Đây là điều hoàn toàn có lợi cho những kẻ xấu đang kết nối vào cùng mạng không dây, chúng có thể đánh cắp thông tin tài khoản hay xem trộm dữ liệu cá nhân của người dùng trong mạng.

Do vậy, ưu tiên số một khi sử dụng mạng không dây là nên cài đặt mạng riêng ảo (VPN - Virtual Private Network) cho truy cập của mình.

Khi sử dụng VPN để truy cập Internet, nó sẽ tự động thiết lập một kết nối mạng dựa trên chính nền tảng mạng không dây nhưng đã được mã hóa các gói tin truyền đi và nhận về, đồng thời

chuyển hướng truy cập giúp người dùng ẩn danh dễ dàng trên Internet. Tuy nhiên, chính vì yếu tố bảo mật cao này mà VPN sẽ làm suy giảm một phần tốc mạng.

2. Sử dụng xác thực 2 bước:

Để tiện cho người dùng truy cập vào mạng không dây, những người quản trị mạng ít khi thiết lập bảo mật nghiêm ngặt cho mạng không dây. Đa phần chỉ chọn cách đặt mật khẩu đơn giản là những chuỗi số dễ nhớ, hay một cụm từ. Tức là, người dùng nào cũng có thể ghi nhớ và thuận tiện truy cập lại cho lần sử dụng tiếp theo.

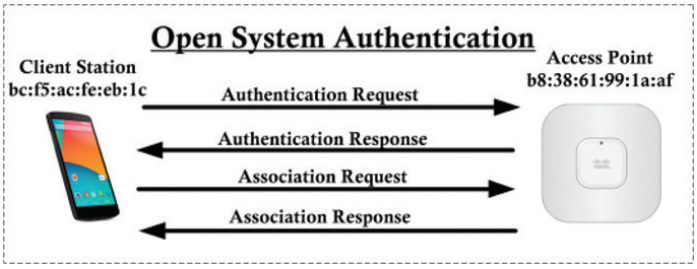
Thông thường, khi đã truy cập vào mạng Internet, đa số người dùng đều đăng nhập vào các tài khoản chứa nhiều thông tin cá nhân, ví dụ như email. Do đó, nếu đã không chọn sử dụng kết nối VPN, và nếu tài khoản email thiết lập lỏng lẻo, thì điều này chẳng khác nào mời gọi những kẻ xấu tìm đến!

Do đó, luôn sử dụng cơ chế xác thực 2 bước cho những tài khoản của mình. Thậm chí, để an toàn hơn, nên chọn cách xác thực bằng số điện thoại cá nhân, thay vì những câu hỏi bí mật đơn giản.

Ví dụ, nếu chọn kích hoạt xác thực 2 bước cho tài khoản Gmail, thì sau khi nhập đúng mật khẩu bạn vẫn phải chờ Gmail gửi thêm một tin nhắn SMS đến điện thoại của người dùng. Tin nhắn đó sẽ cung cấp số mật mã từ phía Google để nhập vào rồi mới đi vào được hộp thư.

3. Cẩn thận với tính năng tự động kết nối mạng không dây.

Một trong những mặt tốt và cũng là nguy cơ tiềm ẩn biến người sử dụng trở thành miếng mồi ngon cho kẻ xấu chính là cơ chế ghi nhớ kết nối mạng không dây của điện thoại, máy tính. Mặc định, khi dùng thiết bị kết nối vào một mạng không dây nào trước đó, thì điện thoại hay laptop sẽ tự động kết nối cho lần sau. Thật vậy, sau này, mỗi khi thiết bị đó ở trong phạm vi của mạng không dây đó thì nó sẽ dò và kết nối vào một cách tự động. Lợi dụng cơ chế này, kẻ xấu có thể đoán biết thói quen này của người dùng để lấy cắp dữ liệu mà người dùng không ngờ đến.



Bên cạnh đó, cũng có những mạng không dây không đặt mật khẩu truy cập, chỉ cần chọn mạng không dây là kết nối vào. Khi đó, việc tấn công sẽ trở nên đơn giản và dễ dàng hơn rất nhiều.

4. Xác minh mạng không dây

Hãy luôn là người dùng thông minh bằng cách kiểm chứng tên kết nối trước khi truy cập. Kẻ xấu có thể đặt tên cho mạng không dây giả của họ gần giống, hay giống hoàn toàn như tên mạng mà bạn thường sử dụng. Nếu không cẩn thận, người dùng sẽ hướng luồng truy cập của mình tới nhầm hướng; khi đó, những gì người dùng gửi đi cũng như nhận lại sẽ bị ghi nhận lại.

Cách tốt nhất là hãy kích hoạt mạng riêng ảo trong mọi tình huống và tỉnh táo hơn nếu nhận thấy có dấu hiệu bất thường từ khâu kết nối. Nên liên lạc với quản trị của mạng không dây đó để xác thực cho chắc chắn hơn nữa.

5. Hạn chế việc đăng nhập.

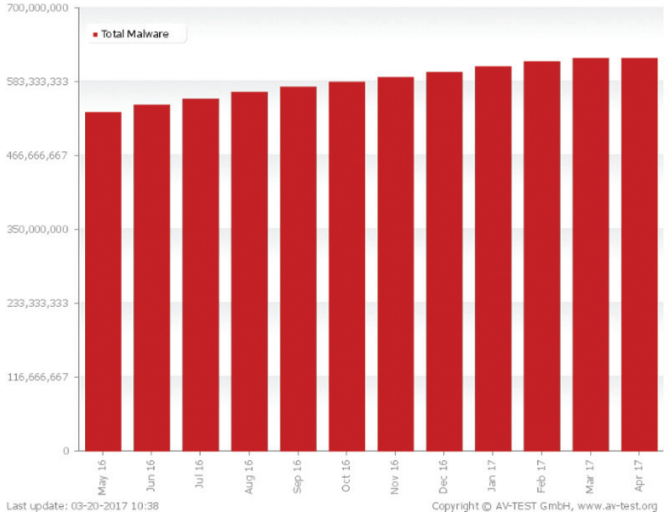
Đây có lẽ là yêu cầu khó thực hiện nhất, khi mà thời đại bùng nổ thông tin. Để an toàn, hãy tập thói quen hạn chế truy cập vào các tài khoản cá nhân khi đang dùng mạng không dây. Tức là, chỉ sử dụng mạng không dây để đọc báo, lướt web.

Nếu bắt buộc phải truy cập vào mail hay tài khoản mạng xã hội, hoặc giao dịch mua bán bất kỳ, hãy kích hoạt mạng VPN lên trước, đồng thời chỉ sử dụng các dịch vụ hỗ trợ giao thức HTTPS mà thôi. Với giao thức này, mọi thông tin của bạn sẽ được an toàn hơn nhờ cơ chế mã hóa mà HTTPS hỗ trợ./.

THỐNG KÊ TÌNH HÌNH AN TOÀN THÔNG TIN

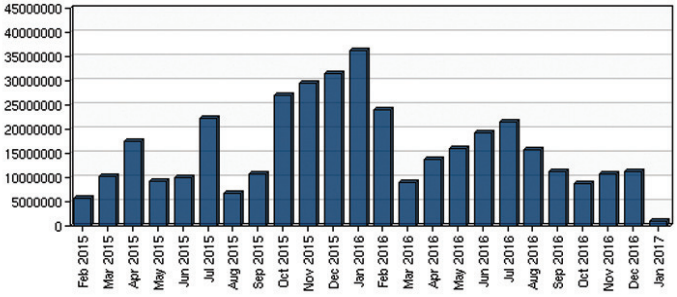
I. TÌNH HÌNH AN TOÀN THÔNG TIN QUÝ I NĂM 2017 TRONG NƯỚC VÀ QUỐC TẾ

1. Tình hình tổng hợp mã độc: Từ tháng 5/2016 đến tháng 4/2017



Nguồn: AV-TEST

2. Tình hình mẫu mã độc xuất hiện mới trong từng tháng



Nguồn: shadowserver

3. Tình hình Spam trong Quý I

Top ten countries | Complete List

Last 14 days

Country	Last 14 days
India	16.7%
Vietnam	16.6%
Iran	5.6%
China	5.5%
United States	5.1%

Last 60 days

Country	Last 60 days
Vietnam	14.2%
India	12.7%
China	9.1%
United States	6.9%
Brazil	3.4%

Last 180 days

Country	Last 180 days
United States	12.6%
India	12.1%
Vietnam	10.9%
China	5.1%
Brazil	4.9%

Nguồn: AV-TEST

4. Hơn 75.000 máy tính tại Việt Nam nhiễm mã độc giả mạo file văn bản

Đây là kết quả thống kê của Tập đoàn công nghệ Bkav và con số này vẫn tiếp tục tăng. Mã độc "ăn" file văn bản, có tên W32.FakeDoc.Worm, phát tán mạnh qua USB.

W32.FakeDoc.Worm có cơ chế phát tán rất tinh vi, virus này tìm các file văn bản Word (có đuôi .doc, .docx), Excel (.xls, .xlsx), PowerPoint (.ppt, .pptx) hay PDF (.pdf) trên các ổ đĩa USB, giấu các file này đi, sau đó sinh ra các file giả mạo chứa mã độc để thay thế vào. File giả mạo có tên và biểu tượng (icon) giống hệt các file văn bản gốc khiến người sử dụng rất khó phát hiện. Khi người dùng mở các file giả mạo vẫn đọc được nội dung gốc của văn bản nhưng đồng thời cũng kích hoạt cả mã độc của virus, nhờ đó virus có thể tiếp tục lây lan từ USB sang máy tính khác.

5. Sự cố các website cảng hàng không: Không phải là tấn công APT như vụ Vietnam Airlines

Đầu tháng 3, một số website của các cảng hàng không như: Tân Sơn Nhất, Rạch Giá, Tuy Hòa bị hacker tấn công. Tuy nhiên, đây chỉ đơn thuần là khai thác lỗ hổng website chứ không phải là tấn công APT như vụ việc của Vietnam Airlines. Vụ việc một lần nữa dấy lên hồi chuông cảnh báo việc đảm bảo an ninh mạng cho ngành hàng không vẫn còn yếu kém và việc đầu tư chưa tương xứng với tầm quan trọng của hệ thống.

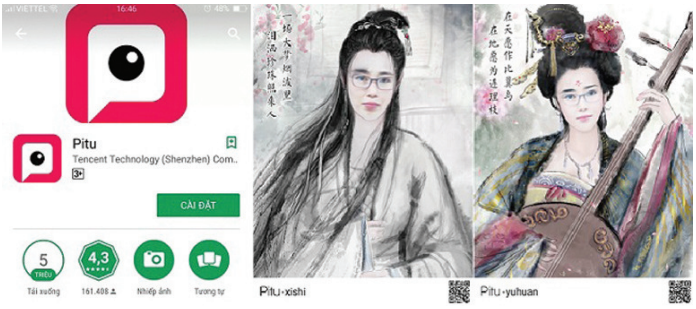
6. Lỗ hổng 0-Day ảnh hưởng đến hơn 300 mẫu switch của Cisco

Lỗ hổng nằm trong mã xử lý CMP - giao thức truyền tải thông tin bằng Telnet hoặc SSH - trong các sản phẩm IOS và IOS XE của Cisco. Lỗi cho phép hacker khởi động lại và thực thi mã từ xa nhằm kiểm soát thiết bị. Hiện tại, lỗ hổng vẫn chưa được vá và người dùng được khuyến cáo vô hiệu hóa kết nối Telnet và SSH với các thiết bị switch cho đến khi có bản vá.

7. Ứng dụng chỉnh ảnh cổ trang thu thập thông tin nhạy cảm của người dùng

Với khả năng chỉnh sửa ảnh thành các nhân vật trong phim cổ trang Trung Quốc, Pitu trở thành ứng dụng miễn phí thu hút người dùng

vào trung tuần tháng 2/2017. Tuy nhiên, ứng dụng này đã bị phát hiện thu thập dữ liệu nhạy cảm của người dùng khi đòi" một số quyền ưu tiên trong quá trình cài đặt. Dữ liệu thu thập được gửi tới các server đặt tại Trung Quốc. Theo khuyến cáo của chuyên gia an toàn thông tin, ngoài thông tin về nhà sản xuất, người dùng cần đặc biệt lưu ý đến các quyền mà ứng dụng đòi hỏi khi cài đặt.



8. Hàng nghìn site WordPress bị hack bằng lỗ hổng mới được tiết lộ

Lỗ hổng này nằm trong Wordpress REST API cho phép hacker không có đặc quyền có thể xóa page hoặc sửa đổi tất cả các page trên trang web chưa được vá, sau đó hướng người dùng tới mã độc hại và các cuộc tấn công. Ngay sau đó, WordPress phát hành một tính năng mặc định tự động cập nhật các trang web chưa được vá đồng thời gửi khuyến cáo tới các quản trị viên nhằm đảm bảo đã cập nhật WordPress lên phiên bản mới nhất là 4.7.2 để được an toàn.

9. Phát hành công cụ giải mã 15 mã độc ransomware miễn phí

Khởi đầu từ liên minh cảnh sát Châu Âu, cảnh sát Hà Lan, Interl Security và Kaspersky Lab, dự án No More Ransom (NRM) là một tổ chức chống mã độc tống tiền toàn cầu giúp nạn nhân khôi phục dữ liệu mà không phải trả tiền cho tin tặc.

Trang web củaNRMkhông chỉ giáo dục người dùng máy tính nâng cao nhận thức và cách thức tự bảo vệ bản thân mà còn cung cấp hàng loạt công cụ giải mã miễn phí. Kể từ tháng 11 năm ngoái, hơn 10.000 nạn nhân trên khắp thế giới đã có thể tự giải mã thiết bị bị khóa mà không tốn bất cứ khoản tiền nào.

NRM hiện tại có sẵn 14 ngôn ngữ và lưu trữ 40 công cụ giải mã miễn phí cung cấp bởi nhiều tổ chức thành viên khác nhau.

MRCR Decryptor	Rakhni Decryptor (updated 2-3-2017 with Dharma)		
Globe3 Decryptor	Rannoh Decryptor (updated 20-12-2016 with CryptXXX v3)		
Derialock Decryptor	Damage Decryptor	FenixLocker Decryptor	
PHP Ransomware Decryptor	Crypton Decryptor	Philadelphia Decryptor	Marlboro Decryptor
WildFire Decryptor	Merry X-Mas Decryptor	Stampado Decryptor	GlobeImposter Dec
Chimera Decryptor	BarRax Decryptor	Xorist Decryptor	Globe Decryptor
Teslacrypt Decryptor	Alcatraz Decryptor	Nemucod Decryptor	Globe2 Decryptor
Shade Decryptor	Bart Decryptor	Gomasom Decryptor	
CoinVault Decryptor	Crypt888 Decryptor	Linux.Encoder Decryptor	
Jigsaw Decryptor	HiddenTear Decryptor	NMoreira Decryptor	CryptoMix Decrypt
TM Ransomware File Decrypto	Noobcrypt Decryptor	Ozozalocker Decryptor	Popcorn Decryptor

10. Hàng ngàn máy tính Windows đang bị tin tặc tấn công bằng bộ công cụ rò rỉ của NSA

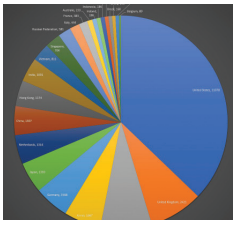
Tin tặc trên khắp thế giới đã bắt đầu khai thác bộ công cụ hacking của NSA vào cuối tuần trước. Hàng ngàn máy tính sử dụng phiên bản Windows chưa được cập nhật đã bị xâm nhập thông qua Internet.

Nhóm tin tặc bí ẩn Shadow Brokers đã chính thức phát tán bộ công cụ hacking Windows, nhắm tới Windows XP, Windows Server 2003, Windows 7 and 8, và Windows 2012 của Cơ quan tình báo quốc gia Hoa Kỳ NSA.

Microsoft ngay lập tức đã giảm thiểu nguy cơ bảo mật xuống bằng cách phát hành bản vá dành cho tất cả các lỗ hổng. Nhưng những hệ thông không còn được hỗ trợ cùng với rất nhiều thiết bị chưa được cài đặt bản cập nhật là đối tượng chính mà tin tặc nhắm tới.

Code Name	Solution
"EternalBlue"	Addressed by MS17-010
"EmeraldThread"	Addressed by MS10-061
"EternalChampion"	Addressed by CVE-2017-0146 & CVE-2017-0147
"ErraticGopher"	Addressed prior to the release of Windows Vista
"EsikmoRoll"	Addressed by MS14-068
"EternalRomance"	Addressed by MS17-010
"EducatedScholar"	Addressed by MS09-050
"EternalSynergy"	Addressed by MS17-010
"EclipsedWing"	Addressed by MS08-067

Có khoảng hơn 36.000 địa chỉ ip trên khắp thế giới bị nhiễm Malware DoublePulsar, trong đó có 811 là ở Việt Nam



II. TÌNH HÌNH AN TOÀN THÔNG TIN TRÊN ĐỊA BÀN TỈNH TRONG QUÝ I/2016

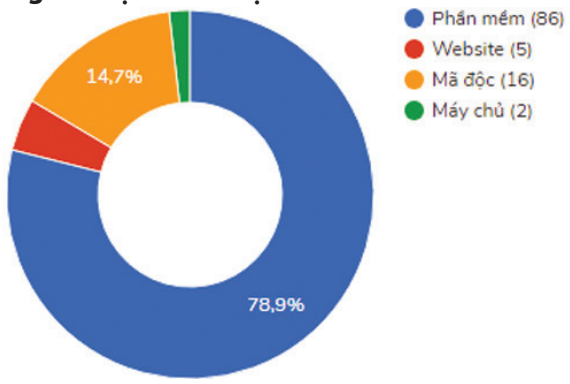
1. Thống kê các website trên địa bàn tỉnh bị tấn công

Ngày	Domain
13/01/2017	shop.vnptthanhhoa.vn
06/02/2017	otohondathanhhoa.net/honda-viet-nam-gioi-thieu-thanh-cong-civic-2017-tai-viet-nam-motor-show-2016.htm
29/02/2017	gachkhongnungthanhhoa.com/eg.html
27/3/2017	hyundaithanhhoa.net/ds.html
27/3/2017	duongsatthanhhoa.vn
28/3/2017	lamwebthanhhoa.com/o.php
31/3/2017	mitsubishithanhhoa.com.vn
10/4/2017	tmdl.edu.vn
13/4/2017	danguykhoithanhhoa.org.vn/images/tech.txt
18/4/2017	dongson.gov.vn/NewsImages/1937CNteam.txt
24/4/2017	ftcthanhhoa.com.vn/by.htm

2. Thống kê các cơ quan, đơn vị bị nhiễm mã độc tham gia mạng Botnet

Khối Sở, Ban, Ngành	Khối UBND Huyện, Thị xã, Thành phố
Sở Công thương	UBND huyện Hậu Lộc
Sở Kế hoạch và Đầu tư	UBND huyện Nga Sơn
Sở Lao động, Thương binh và Xã hội	UBND huyện Như Thanh
Sở Nông nghiệp và Phát triển nông thôn	UBND huyện Quan Hóa
Sở Văn hóa, Thể thao và Du lịch	UBND huyện Hoằng Hóa
Sở Y tế	UBND Thị xã Bỉm Sơn
	UBND huyện Quan Sơn
	UBND huyện Thiệu Hóa
	UBND huyện Yên Định
	UBND Thành phố Thanh Hóa

3. Tổng hợp tình hình ứng cứu sự cố trên địa bàn tỉnh



TIN HOẠT ĐỘNG

Triển lãm Quốc gia về An ninh bảo mật 2017 (Security World 2017) và Hội thảo Quốc gia về Chính phủ số 2017 (DGov 2017)

Ngày 04/4/2017, tại Hà Nội, Trung tâm CNTT&TT Thanh Hóa đã tham dự Triển lãm quốc gia về an ninh bảo mật 2017 (Security World 2017) với chủ đề "Chiến lược đảm bảo an ninh, an toàn thông tin trong thời kỳ cách mạng công nghiệp lần thứ 4" do Cục An toàn thông tin - Bộ Thông tin và Truyền thông phối hợp với Cục An ninh mạng - Bộ Công an và Tập đoàn Dữ liệu quốc tế (IDG) đồng tổ chức.

Cuộc cách mạng công nghiệp lần thứ 4 với sự phát triển mạnh mẽ về Khoa học - Công nghệ được dự báo sẽ tạo ra những cơ hội lớn cho Việt Nam hội nhập sâu rộng hơn và hiệu quả hơn vào nền kinh tế thế giới. Đây cũng được đánh giá là thời cơ quý giá để Việt Nam đẩy mạnh ứng dụng công nghệ thông tin, tự động hoá các quy trình kinh doanh, tăng cường khả năng kết nối qua các thiết bị di động và tiếp cận với cơ sở dữ liệu lớn, đồng thời những tính năng xử lý thông tin sẽ được nhân lên bởi những đột phá công nghệ trên nhiều lĩnh vực.

Trong bối cảnh vấn đề đó, Hội Thảo - Triển lãm Quốc gia về An ninh bảo mật (Security World 2017) sẽ đưa vào thảo luận chủ đề "Chiến lược đảm bảo An ninh, an toàn thông tin trong thời kỳ cách mạng công nghiệp lần thứ 4". Hội thảo hướng đến mục tiêu giúp các doanh nghiệp, tổ chức nắm bắt và đánh giá được các hiểm họa an toàn thông tin hiện nay, cũng như đề xuất các phương án giúp các tổ chức ứng phó kịp thời trước sự phát triển nhanh chóng của các nguy cơ bảo mật và đảm bảo tuân thủ các quy định an toàn bảo mật mới.

Sáng 5/4, tại Khách sạn Melia - Hà Nội đã diễn ra Hội thảo Quốc gia về Chính phủ điện tử 2017 với chủ đề "Phát triển Chính phủ Điện tử trong thời kỳ Cách mạng công nghiệp lần thứ 4: Tầm nhìn & Giải pháp Công nghệ". Đây là sự kiện thường niên do UBND TP. Hà Nội phối hợp với Tập đoàn Dữ liệu Quốc tế Việt Nam (IDG) tổ chức.

Tại Hội thảo, các đại biểu đã tập trung thảo luận một số vấn đề nổi bật như: Cuộc cách mạng công nghiệp lần thứ 4 và các vấn đề đặt ra đối với phát triển Chính phủ điện tử tại Việt Nam; một số vấn đề cần quan tâm trong chương trình cải cách hành chính công trong xu hướng phát triển Chính phủ điện tử hiện nay; đảm bảo xác thực và bảo mật phục vụ triển khai Chính phủ điện tử; ứng phó thách thức an ninh mạng trong bảo mật Thành phố thông minh; phát triển Giáo dục và Y tế của TP. Hà Nội hướng đến đô thị thông minh và hiện đại./.

TRẦN LÊ PHÚC

Tập huấn, bồi dưỡng kỹ năng ứng cứu sự cố về an toàn thông tin

Trong ba ngày từ 13-15/4/2017. Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa phối hợp với UBND huyện Quan Sơn tổ chức lớp tập huấn, bồi dưỡng kỹ năng ứng cứu sự cố về an toàn thông tin cho các cán bộ chuyên trách công nghệ thông tin là đầu mối tiếp nhận sự cố của các Sở, ban, ngành và UBND cấp huyện, thị xã, thành phố trên địa bàn tỉnh.

Tham dự khai mạc lớp tập huấn có đ/c Lê Xuân Lâm - Giám đốc Trung tâm CNTT&TT; đ/c Lương Tiến Thành - Ủy viên Ban thường vụ Huyện ủy, Phó Chủ tịch thường trực UBND huyện; đại diện các phòng ban liên quan của Trung tâm và UBND huyện.

Phát biểu tại buổi khai mạc lớp tập huấn, đồng chí Lê Xuân Lâm, Giám đốc Trung tâm CNTT&TT Thanh Hóa đã nhấn mạnh: Trước tình hình diễn biến phức tạp về mất an toàn thông tin hiện nay, để hoạt động ứng cứu xử lý sự cố được triển khai hiệu quả hơn nữa, đặc biệt trong kỷ nguyên cách mạng công nghiệp lần thứ 4, nguy cơ chiến tranh mạng ngày càng hiện hữu; Trung tâm CNTT&TT tổ chức lớp tập huấn với mục đích giúp cho các cán bộ trực tiếp phụ trách CNTT nói chung, an toàn thông tin nói riêng tại mỗi cơ quan, đơn vị trên địa bàn tỉnh nâng cao kỹ năng ứng cứu và xử lý các sự cố tại hệ thống thông tin của cơ quan, đơn vị mình. Để qua đó chủ động, sẵn sàng đối phó, ngăn chặn và giảm thiểu các nguy cơ đe dọa gây mất an toàn thông tin.

Tại hội nghị tập huấn, đ/c Lương Tiến Thành - Ủy viên Ban thường vụ Huyện ủy, Phó Chủ tịch thường trực UBND huyện Quan Sơn đã chia sẻ kinh nghiệm, những khó khăn vướng mắc trong triển khai ứng dụng CNTT, công tác quản lý nhà nước về Thông tin và Truyền thông và an toàn thông tin mạng tại các cơ quan nhà nước trên địa bàn huyện, bên cạnh đó cũng giới thiệu tình hình KT-XH và những tiềm năng thế mạnh của huyện.

Trong thời gian tập huấn, các học viên được giảng viên của Trung tâm Công nghệ thông tin và Truyền thông tỉnh truyền đạt những nội dung thiết thực với tình hình thực tế của cơ quan nhà nước. Giúp cán bộ chuyên trách công nghệ thông tin có thể khắc phục,

xử lý những sự cố mạng máy tính; sự cố về an toàn an ninh thông tin của Cổng/Trang thông tin điện tử; các vấn đề liên quan đến an toàn thông tin tại các cơ quan. Đồng thời, trang bị kiến thức về các kỹ năng ứng cứu sự cố, tấn công của tin tặc; các trang thiết bị phục vụ cho tin tặc; nhận biết các thông số trên hệ điều hành, phát hiện và nhận diện các nguy cơ tấn công; đánh giá các điểm yếu, triển khai hệ thống phòng chống tấn công; cấu hình hệ thống trên mạng nội bộ và mạng diện rộng, triển khai các biện pháp đảm bảo an toàn, an ninh mạng.

Bên cạnh đó nhằm tăng cường hơn nữa mối quan hệ công tác với cơ sở, các học viên được thăm quan thực tế một số xã biên giới của huyện Quan Sơn về công tác trao đổi, sử dụng văn bản điện tử trên phần mềm Quản lý văn bản và Hồ sơ công việc (TDOffice) đã được tỉnh chọn một trong 6 huyện hưởng thụ dự án thí điểm./.

TRỊNH NGỌC QUỲNH

Giao lưu chia sẻ kinh nghiệm, hợp tác cùng phát triển trong lĩnh vực CNTT&TT trong khu vực Bắc Trung bộ

Thực hiện chương trình "HỢP TÁC CÙNG PHÁT TRIỂN" giữa các Trung tâm Công nghệ thông tin và Truyền thông khu vực Bắc Trung bộ, sau sáng kiến lần thứ nhất tại Sầm Sơn, Thanh Hóa. Năm 2017, Trung tâm CNTT&TT tỉnh Nghệ An là đơn vị đăng cai địa điểm tổ chức lần thứ hai;

Trong nội dung của chương trình, lãnh đạo Trung tâm CNTT&TT các tỉnh Thanh Hóa, Nghệ An, Quảng Trị, Quảng Bình đã ký kết biên bản "Hợp tác cùng phát triển". Lễ ký kết có sự chứng kiến của lãnh đạo Sở Thông tin và Truyền thông các tỉnh Nghệ An, Quảng Trị và Giám đốc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) cũng như cán bộ, viên chức, người lao động, đoàn thanh niên Trung tâm các tỉnh tham dự.

Tiếp theo chương trình là buổi tọa đàm chia sẻ kinh nghiệm, hợp tác cùng phát triển trong lĩnh vực CNTT&TT giữa các tỉnh Bắc Trung bộ. Tại buổi tọa đàm, đ/c Nguyễn Trọng Đường, giám đốc trung tâm VNCERT cho rằng: "để đưa ngành CNTT&TT khu vực Bắc Trung bộ phát triển, các đơn vị cần thực hiện tốt nhiệm vụ được giao; Trong đó, đặc biệt quan tâm, chú trọng tuân thủ các quy định về an toàn, bảo mật thông tin; Phối hợp, liên kết với các đơn vị phát triển và hoàn thiệnhạ tầng kỹ thuật bảo đảm cho các hoạt động ứng dụng CNTT trong các cơ quan nhà nước trên môi trường mạng an toàn, hiệu quả; Tổ chức đào tạo nguồn nhân lực về CNTT&TT phục vụ yêu cầu phát triển KT-XH của tỉnh". Cũng tại buổi tọa đàm, lãnh đạo Trung tâm CNTT&TT các tỉnh khu vực Bắc Trung Bộ đã chia sẻ thêm một số kinh nghiệm trong công tác thực hiện các nhiệm vụ chuyên môn gồm: Xây dựng chính quyền điện tử, giao ban trực tuyến, chuyển giao ứng dụng CNTT, an toàn thông tin, ứng cứu sự cố, trao đổi chia sẻ trong việc tổ chức đào tạo, bồi dưỡng, tổ chức thi cấp chứng chỉ tin học "chuẩn kỹ năng sử dụng công nghệ thông tin" theo Thông tư 03/2014/TT-BTTTT của Bộ TT&TT và các nội dung trong công tác tư vấn triển khai dịch vụ và phát triển phần mềm... Đồng thời, các đại biểu đề nghị những năm tiếp theo sẽ tổ chức tọa đàm theo chủ đề, nội dung cụ thể, thiết thực hơn./.

CAO VIỆT CƯỜNG

Trung tâm CNTT&TT Thanh Hóa tổ chức thi cấp Chứng chỉ ứng dụng Công nghệ thông tin đợt 1 năm 2017

Sáng ngày 23 tháng 4 năm 2017, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa tổ chức kỳ thi sát hạch cấp Chứng chỉ công nghệ thông tin chuẩn cơ bản, đợt 1 năm 2017; Hội đồng thi được Sở Giáo dục và đào tạo thành lập gồm 14 người, bao gồm đầy đủ các Ban theo quy định về việc tổ chức thi và cấp chứng chỉ ứng dụng công nghệ thông tin tại Thông tư liên tịch số 17/2016/TTLT-BGDĐT-BTTT ngày 21 tháng 6 năm 2016 giữa Bộ Giáo dục và Đào tạo và Bộ Thông tin và Truyền thông;

Kỳ thi Đợt 1 năm 2017, có 44 thí sinh đăng ký dự thi và có 41 đã hoàn thành tốt 2 phần thi của mình là phần thi trắc nghiệm lý thuyết trực tuyến trên phần mềm và phần thi thực hành kỹ năng trên máy tính; toàn bộ hồ sơ về kỳ thi đã được gửi Sở Giáo dục và đào tạo tỉnh để tiến hành cấp chứng chỉ, phối chứng chỉ được Bộ Giáo dục và đào tạo cấp theo số lượng thí sinh thi đậu, được Sở GDĐT Thanh Hóa phê duyệt.

Theo kế hoạch công tác của Trung tâm CNTT&TT Thanh Hóa, Trung tâm liên tục thu hồ sơ đăng ký bồi dưỡng, ôn thi và được tổ chức thi 01 lần vào các tháng trong năm

Mọi thông tin về đăng ký bồi dưỡng, ôn thi và đăng ký thi xin liên hệ về Phòng Đào tạo và Dịch vụ - Trung tâm CNTT&TT Thanh Hóa, số 73 Hàng Than, phường Lam Sơn, TP Thanh Hóa.

Số điện thoại: 02373. 718.698 hoặc thông qua website: http://ict.thanhhoa.gov.vn

CHÚC ANH HÒA