Tác Giả: K□ s□ Nguy□n Ng□c B□o
Chúa Nhật, 08 Tháng 1 Năm 2012 08:33

... vi□c t□n công b□ng malware đ□ chi□m các máy vi tính, l□y c□p các máy vi tính đ□ khai thác d□ ki□n, s□ d□ng các máy b□ chi□m đ□ t□n công các máy khác, tr□ thành r□t thông d□ng.

An Ninh Máy Vi Tính và Nh□ng Cách S□ D□ng An Toàn (Best Practices)

BBT No Firewall xin g□i đ□n các b□n trình bày c□a k□ s□ Nguy□n Ng□c B□o trong bu□i h□□ng d□n v□ an ninh đi□n t□, đ□□c t□ ch□c trên Paltalk ngày 29/12 v□a qua.□ K□ s□ Nguy□n Ng□c B□o trách nhi□m v□ an ninh thông tin t□i m□t công ty chuyên v□ qu□c phòng t□i Pháp. Ông th□□ng xuyên c□ v□n cho blog No Firewall.

M□t vài con s□ liên quan đ□n máy vi tính

Máy vi tính hi□n nay tr□ thành r□t thông d□ng trong h□n 1/3 s□ gia đình trên kh□p th□ gi□i và tr□ thành d□ng c□ ph□ thông r□t h□u ích cho vi□c trao đ□i thông tin qua đi□n th□ (email), t□i xu□ng các tài li□u, thu th□p thông tin v□ chính tr□, kinh t□, xã h□i, mua bán, làm vi□c v□i nhau qua vi□c truy c□p vào m□ng toàn c□u Internet. Vi□c trao đ□i d□ ki□n, thông tin, còn tr□ thành m□t nhu c□u quan tr□ng h□n trong m□t xã h□i đ□c tài trong đó m□i lu□ng thông tin đ□c l□p d□u ph□i ch□u m□t s□ ki□m duy□t g□t gao.

Hi□n nay có kho□ng t□ 1,8 t□ đ□n 2 t□ máy vi tính trên kh□p th□ gi□i, so v□i h□n 2 t□ ng□□i x□ d□ng m□ng Internet. Năm 2010, s□ bán máy vi tính là 350 tri□u, tăng 3,8% so v□i 2009, con s□ bán □□c l□□ng cho 2012 là 400 tri□u máy. N□u tính đ□ đ□ng, c□ 3 năm m□i thay m□t máy vi tính, thì s□ máy vi tính t□i thi□u hi□n nay là 1,4 t□ máy. Kho□ng 1.000.000 máy đi□n toán b□ m□t c□p m□i năm. S□ l□□ng máy vi tính cá nhân b□ t□n công và tr□ thành m□t ph□n t□ c□a m□t m□ng botnet lên đ□n c□ trăm tri□u máy. H□u nh□ 100% các d□ ki□n cá nhân, s□ ID, m□t kh□u, tr□□ng m□c ngân hàng, đ□u đ□□c ch□a trong các máy vi tính dù t□i n□i làm vi□c hay t□i nhà riêng.

Do đó, vi□c t□n công b□ng malware đ□ chi□m các máy vi tính, l□y c□p các máy vi tính đ□ khai thác d□ ki□n, s□ d□ng các máy b□ chi□m đ□ t□n công các máy khác, tr□ thành r□t thông d□ng.

Tác Giả: K□ s□ Nguy□n Ng□c B□o
Chúa Nhật, 08 Tháng 1 Năm 2012 08:33

Trong Ph□n 2 v□ An Ninh máy Vi Tính và Nh□ng Cách S□ D□ng An Toàn (Best Practices)

Chúng ta s□ c□n nh□n di□n ra:

Nh□ng r□i ro l□n nh□t khi s□ d□ng máy vi tính đ□ bi□t cách phòng ch□ng, k□ ti□p là
Nh□ng cách s□ d□ng (behavior) an toàn thông d□ng trong nhi□u tình hu□ng s□ d□ng máy khác nhau, và sau cùng là
M□t s□ h□□ng d□n v□ nh□ng bi□n pháp an ninh đi□n toán k□ thu□t c□n thi□t qua nhi□u t□ng an ninh t□ th□p đ□n cao và b□ túc cho nhau.

Nh□n di□n nh□ng r□i ro (risks) khi s□ d□ng máy vi tính

R□i ro là m□t t□ng h□p nhân c□a các thành t□ (component) sau đây:

Risks = Threats X Vulnerabilities X Impact X Frequency
Threats = Đe D□a
Vulnerabilities = Y□u Kém
Impact = H□u qu□
Frequency = Nh□p Đ□

Thí d□ qua 4 tr□□ng h□p khác nhau:

• N□u threats cao, nh□ng vulnerabilities r□t th□p, thì dù impact cao và nh□p đ□ x□y ra th□□ng xuyên, Risks cũng ch□ □ m□c trung bình
• N□u threats trung bình, vulnerabilities trung bình, nh□ng impact cao và nh□p đ□ trung bình thì risks cũng □ m□c đ□ cao
• N□u threats cao, vulnerabilities cũng cao, nh□ng n□u impact r□t th□p, thì dù frequency có cao, thì risks cũng ch□ □ trung bình
• N□u threats cao, vulnerabilities trung bình, impact trung bình, nh□ng frequency r□t th□p, thì risks cũng ch□ m□c trung bình

Sau đây là nh□ng r□i ro chính liên quan đ□n vi□c s□ d□ng máy vi tính, d□a trên tiêu chu□n AICP (Availability, Integrity, Confidentiality, Proof):

M□t máy, máy b□ ăn c□p

H□u qu□: d□ li□u riêng t□ cá nhân b□ l□y c□p, s□ d□ng cho các ho□t đ□ng phi pháp. Đ□i v□i các thành ph□n ho□t đ□ng dân ch□, ho□t đ□ng c□a chính mình b□ b□i l□ và □nh h□□ng đ□n an ninh cá nhân c□a nh□ng ng□□i cùng ho□t đ□ng và có liên l□c v□i mình.

Máy b□ t□n công và b□ gài spyware

H□u qu□: d□ li□u l□u tr□ trong máy b□ spyware thu th□p và g□i ra bên ngoài, liên quan đ□n các tài li□u cá nhân riêng t□ (tr□□ng m□c ngân hàng, m□t kh□u, gi□y t□ cá nhân b□ l□y c□p), các d□ ki□n v□ ho□t đ□ng liên quan đ□n các thành ph□n dân ch□ khác, nh□ng ng□□i quen bi□t. Thí d□ nh□ các d□ ki□n truy c□p vào các tr□□ng m□c, n□m trong máy b□ l□y tr□m nh□m xâm nh□p vào các webmail đ□ l□y các tài li□u riêng t□, truy tìm ra nh□ng ng□□i liên l□c v□i ng□□i ch□ c□a máy.

Máy b□ t□n công, xâm chi□m và bi□n thành m□t ph□n t□ c□a m□t m□ng l□□i botnet đ□ t□n công t□ ch□i d□ch v□ (DOS) hay g□i th□ rác spam.

H□u qu□: cùng h□u qu□ nh□ trên, ngoài ra đ□a ch□ IP c□a máy b□ li□t kê vào lo□i máy x□u và có th□ b□ ngăn ch□n (block)

Do đó, các cách s□ d□ng an toàn và bi□n pháp an ninh đi□n toán thi□t trí trên máy nh□m
• đ□ làm gi□m thi□u r□i ro d□ ki□n riêng t□ b□ l□ ra bên ngoài do b□ malware xâm nh□p hay máy b□ m□t,
• đ□ tránh gây h□i đ□n chính ng□□i s□ d□ng và nh□ng ng□□i quen bi□t, cùng ho□t đ□ng.

Tác Giả:: K□ s□ Nguy□n Ng□c B□o
Chúa Nhật, 08 Tháng 1 Năm 2012 08:33

Nh□ng cách th□c s□ d□ng an toàn (Best Practices)

Nh□ trình bày trong Ph□n 1 Malware R□i Ro, Nh□n Di□n và Cách Phòng Ch□ng, cách th□c s□ d□ng (behavior) an toàn đóng góp 10% vào ph□n b□o đ□m m□c an ninh nói chung.

Sau đây là m□t s□ tình hu□ng đi□n hình mà chúng ta c□n quan tâm đ□n s□ an toàn c□a máy vi tính.

T□i nh□ng n□i công c□ng, t□i cyber café, t□i nhà ga, trên xe l□a, phi tr□□ng, trên phi c□, khách s□n, t□i n□i làm vi□c.

Không n□i vào các n□i làm vi□c, ho□t đ□ng v□i các d□ ki□n h□ tr□ng, n□u đ□□ng liên l□c không đ□□c mã hóa (b□ng VPN Virtual Priate Network hay b□ng SSL v□i giao th□c HPPS)
Khi c□n truy c□p vào m□ng Internet, c□n tránh truy c□p vào các web site "l□" t□i các n□i trên.
Khi n□i b□ng Wifi, m□c đ□ mã hoá ph□i t□i thi□u WPA hay t□t h□n là WPA2 (128 bits) nh□m phòng ch□ng l□i k□ □ gi□a nghe lén (Man In The Middle)
Không m□ các h□ s□ quan tr□ng trong máy □ n□i công c□ng có nhi□u ng□□i có th□ nhìn th□y đ□□c. C□n tìm m□t n□i khu□t, l□ng ph□i t□a vào t□□ng, đ□ tránh có k□ nhìn tr□m đ□ng sau l□ng.
Luôn luôn mang máy vi tính trong hành lý mang tay và đem lên phi c□, không bao gi□ g□i hành lý có máy vi tính, không r□i xa hành lý có máy vi tính, luôn mang theo n□u d□i xa ch□ ng□i trên phi c□, trên xe l□a hay trong khách s□n.
Không bao gi□ cho ng□□i khác m□□n máy vi tính, khi không s□ d□ng n□a nên t□t h□n máy
Nên mang theo m□t th□ nh□ USB có mã hóa ch□a các h□ s□ quan tr□ng, các h□ s□ này không sao chép trong máy vi tính đ□ phòng h□ tr□□ng h□p máy b□ quan thu□ t□ch thu.

Khi nh□n hay chuy□n hay l□u tr□ tài li□u, d□ ki□n v□i th□ nh□ USB

C□n khoá (block kh□ năng autorun t□ th□ nh□ USB) trên máy vi tính
Nên dùng th□ nh□ c□a chính mình đ□ chuy□n hay nh□n h□ s□ cho an toàn h□n. C□n gi□i mã tr□□c t□p hay directory đã đ□□c mã hoá đ□ tránh t□o s□ tò mò
Khi nh□n h□ s□ nên quét th□ nh□ USB ngay, tr□□c khi chép vào đĩa c□ng trong máy vi tính
Các nhu li□u mã hoá mi□n phí có th□ dùng : TrueCrypt (đĩa c□ng), FlexCrypt (www.flexcrypt.com) , Zed (www.primx.eu

) , PGP (
http://www.pgpi.org/products/pgp/versions/freeware/winxp/8.0
) , GnuPG (
http://gpg4win.org/
)

Khi đ□a máy đi s□a hay thay máy

Nên nh□ m□t ng□□i quen thân tín, đi mua dùm máy, h□n là t□ mình đi mua, n□u không mu□n b□ nh□n di□n

Tr□□c khi mang máy đi s□a, nên c□ g□ng nh□ nh□ng ng□□i quen bi□t v□ đi□n toán xem dùm máy. Nên chép h□t các h□ s□ quan tr□ng ra th□ nh□ bên ngoài và mã hoá. Secured deletion các h□ s□ quan tr□ng trong máy (CCleaner), đ□ tránh không còn d□u v□t các h□ s□ đã xóa

Sau khi nh□ ng□□i quen mang máy s□a xong v□, ki□m l□i t□t c□ các functions xem có gì thay đ□i hay không. Quét (scan ngay) v□i anti virus c□p nh□t. T□i xu□ng m□t anti virus th□ nhì đ□ quét xem có gì thay đ□i kh□ nghi hay không?

C□n tránh cho ng□□i khác, dù là quen bi□t s□ d□ng máy

N□u không tránh đ□□c, nêu t□o ra m□t account khách m□i (invite)

Yêu c□u không đ□□c t□i xu□ng b□t c□ ch□□ng trình software nào. T□t nh□t là nêu activate account control (c□n đánh vào m□t kh□u administrator n□u mu□n thi□t trí m□t nhu li□u m□i)

Khi b□t bu□c ph□i cho s□ d□ng máy c□a mình, nên có m□t t□i ch□, đ□ng đ□ng sau l□ng đ□ xem xét

Sau khi cho s□ d□ng xong, nên cho quét máy ngay (scan anti virus, anti spyware)

Chu□n b□ cho tình hu□ng máy b□ t□ch thu

C□n quét th□□ng xuyên (scan v□i Ccleaner) đ□ xoá an toàn các h□ s□ không s□ d□ng n□a trong máy, ngay sau khi m□i khi m□, làm vi□c trên các h□ s□ quan tr□ng.

C□n sao chép các h□ s□ quan tr□ng ra bên ngoài và l□u gi□ trên m□t th□ nh□ USB hay removable disk có mã hoá, đ□ tránh tr□□ng h□p m□t h□t h□ s□ khi máy b□ t□ch thu.

Không gi□ m□t kh□u trong máy tr□ khi mã hóa h□ s□ này. Luôn luôn xoá (clear) cache PGP hay c□a m□t ch□□ng trình mã hóa khác, đ□ tránh pass phrase (m□t kh□u) dùng cho mã hóa b□

l□

C□□ng quy□t t□ ch□i không cung c□p m□t kh□u mã hóa.

Khi không s□ d□ng ho□c đi v□ng kh□i nhà không lâu

Máy nên t□t và nên l□y đĩa c□ng ra bên ngoài. C□t d□u □ n□i kín đáo. N□u v□ng nhà lâu nên mang theo máy vi tính.

Trong tr□□ng h□p có h□ s□ quan tr□ng, nên sao chép vào trong m□t th□ nh□ USB có mã hoá (PGP, TrueCrypt) và xoá an toàn (secured deletion) trong máy v□i CCleaner.

Máy c□n có khoá t□ đ□ng (lock). N□u không có m□t tr□□c máy, nên t□t đ□□ng liên l□c (wifi hay rút dây network RJ45 ra kh□i máy)

Nh□ng Bi□n Pháp An Ninh Đi□n Toán K□ Thu□t

Đ□i v□i nh□ng r□i ro gây ra b□i malware, m□i r□i ro đ□u c□n có bi□n pháp phòng ch□ng nhi□u t□ng (multi layer defense)

Các m□c đ□ an ninh c□a máy vi tính đ□□c chia thành 4 m□c đ□ t□ th□p đ□n cao nh□ sau :

M□c đ□ 1: M□c an ninh đ□t 80% (70% k□ thu□t + 10% cách s□ d□ng) liên h□ đ□n 99% ng□□i s□ d□ng Internet (□□c l□□ng 1.980.000.000)

M□c đ□ 2: M□c an ninh đ□t 95% (85% k□ thu□t + 10% cách s□ d□ng) liên h□ đ□n 0,95% ng□□i s□ d□ng Internet (□□c l□□ng kho□ng 19.000.000)

M□c đ□ 3: M□c an ninh đ□t 99%, (89% k□ thu□t + 10% cách s□ d□ng) liên h□ đ□n 0,049% ng□□i s□ d□ng Internet (□□c l□□ng kho□ng 1.980.000)

M□c đ□ 4: M□c an ninh đ□t 99%+ liên h□ đ□n 0,001% ---> 20.000

Tác Giả: K□ s□ Nguy□n Ng□c B□o
Chúa Nhật, 08 Tháng 1 Năm 2012 08:33

M□c đ□ 1

Các bi□n pháp k□ thu□t c□n thi□t cho m□c đ□ 1

Anti virus, c□p nh□t, quét th□□ng xuyên (đ□ khám phá và di□t tr□, cô l□p các malware)
Anti spyware, c□p nh□t, quét th□□ng xuyên
C□p nh□t th□□ng xuyên v□ an ninh đ□ vá các l□ h□ng an ninh (patch security update).

Đ□c đi□m:

□ m□c đ□ 1 v□ an ninh, khi áp d□ng tri□t đ□ các bi□n pháp phòng ch□ng, m□c đ□ an ninh t□ng quát đ□t kho□ng 80%
R□i ro cao nh□t v□n đ□n t□ vi□c b□ malware t□n công
Danh sách các URL các nhu li□u anti virus, anti spyware mi□n phí (nofirewall.blogspot.com)
Microsoft Security Essentials http://www.microsoft.com/security_essentials/
Comodo Security suite http://www.comodo.com/home/internet-security/free-internet-security.php
AVG http://free.avg.com/us-en/homepage
AVAST http://www.avast.com/index
Avira http://www.avira.com/en/for-home
B□n x□p h□ng các nhu li□u anti virus, anti spyware theo m□c hi□u qu□ c□a kh□ năng khám phá và tiêu di□t các malware.
http://us.generation-nt.com/review-free-antivirus-virus-antispyware-spyware-antirootkit-rootkit-avira-avast-review-2028861-1.html
Các security suite m□i đây đ□u có m□t s□ kh□ năng gi□i h□n ch□ng root kit và Firewall và t□□ng đ□i có hi□u qu□ khá đ□ng đ□u v□i nhau. N□u có kh□ năng nên mua phiên b□n th□□ng m□i ra, s□ có đ□□c nhi□u options h□n.

Nh□ng đi□m c□n quan tâm:

C□n li□t kê ra nh□ng nhu li□u đang s□ d□ng đ□ activate cách c□p nh□t các vá (Patch). Ngoài các vá c□a Mirosoft hay Mac, c□n t□i xu□ng các vá c□a Adobe Reader, Flash Player, Itunes

(Mac).

Cho h□ th□ng đi□u hành Windows và Mac, nên activate (b□t) kh□ năng c□p nh□t các vá (patch) m□t cách t□ đ□ng (ngay cho c□ các ch□□ng trình □ng d□ng nh□ Microsoft Office, Adobe Reader, …)

C□n l□y option c□p nh□t hàng ngày và quét th□□ng xuyên toàn b□ các đĩa c□ng vào ban đêm, ít nh□t 2 l□n m□t tu□n và tiêu di□t t□ đ□ng m□i malware khám phá ra đ□□c (lúc đó, t□t Wifi hay rút giây network ra kh□i máy)

C□n xem xét nhu li□u có ch□y th□□ng xuyên trên máy (check icône trên task bar và process trên b□ng CRTL+ALT+SUP)

C□n tham kh□o th□□ng xuyên k□t qu□ các đ□t quét xem có gì đáng quan tâm hay không.

M□c đ□ 2

Các bi□n pháp an ninh c□a m□c đ□ 1

Anti rootkit, (nh□m phá v□ vi□c che d□u malware)
Firewall đ□ ngăn ch□n các liên l□c không đ□□c cho phép ra bên ngoài.
Mã hóa m□t ph□n (partition) đĩa c□ng, mã hoá các h□ s□ l□u tr□, g□i đi

Đ□c đi□m:

□ t□ng 2 v□ an ninh, khi áp d□ng tri□t đ□ các bi□n pháp phòng ch□ng, m□c đ□ an ninh t□ng quát đ□t kho□ng 95% (tr□ r□i ro đ□n t□ các malware lo□i “0 day “, có nghĩa là ch□a có □n d□u)

R□i ro cao nh□t v□n đ□n t□ malware qua đi□n th□ (email), t□i xu□ng h□ s□, truy c□p vào web site b□ nhi□m malware. □ t□ng này, vi□c mã hoá các h□ s□, quan tr□ng s□ giúp ch□ng l□i vi□c tài li□u b□ l□t ra ngoài, khi máy b□ m□t hay b□ ăn c□p hay b□ malware lo□i trojan.

Danh sách các nhu li□u anti rootkit, firewall cá nhân và mã hóa mi□n phí

Anti rootkit

Spybot Search and Destroy http://www.safer-networking.org/en/index.html

Sophos anti rootkit http://www.sophos.com/fr-fr/products/free-tools/sophos-anti-rootkit.aspx

Firewall

PC Tools Firewall Plus Free Firewall

Privatefirewall
Zone Alarm Free Firewall 2012

Mã hóa
PGP
TrueCrypt
FlexCrypt
Zed

Nên s□ d□ng 2 lo□i anti rootkit khác nhau đ□ đ□i chi□u các k□t qu□ tìm th□y

N□u l□u gi□ lo□i h□ s□ quan tr□ng, nên mã hóa □ m□c h□ s□ (PGP) và toàn b□ đĩa c□ng (TrueCrypt)

Đ□nh nghĩa rootkit : c□m t□ đ□n t□ h□ th□ng đi□u hành UNIX nay cũng hi□n h□u trong h□ th□ng đi□u hành Windows. M□t h□ th□ng bao g□m m□t s□ m□nh l□nh và function v□i m□c tiêu t□o ra m□t context qu□n tr□ viên (administrator) đ□ che d□u ho□t đ□ng c□a các malware.

Nh□ng đi□m c□n quan tâm:

C□n l□y option c□a Firewall : “t□t c□ nh□ng liên l□c ra bên ngoài, c□n ph□i đ□□c s□ ch□p thu□n (click vào OK)”, đ□ khám phá và ngăn ch□n nh□ng liên l□c bí m□t ra bên ngoài, ch□ d□u c□a máy b□ nhi□m malware lo□i trojan (có function key logger : thu l□i nh□ng ch□ đánh trên bàn phím nh□ m□t kh□u đ□ g□i lén ra ngoài)

Nên kh□i đ□ng (launch) nhu li□u anti rootkit chuyên bi□t, ph□ thêm vào nhu li□u anti virus, anti spyware đã có □ m□c đ□ 1, ít nh□t 1 tu□n 1 l□n. Nh□t là sau khi truy c□p vào các web site không quen thu□c. Hi□n nay, □□c l□□ng kho□ng vài tri□u web site (trên t□ng s□ h□n 500 tri□u) b□ nhi□m malware và tr□ thành máy ch□ (server) đ□ phân ph□i malware.

C□n th□n khi phân tích k□t qu□ tìm ki□m c□a nhu li□u anti rootkit (AVG, Sophos, …) vì có th□ li□t kê ra nh□ng lo□i h□ s□ không ph□i là root kit. C□n xác đ□nh b□ng cách chuy□n lên web site
www.virustotal.com
hay
www.threatexpert.com
đ□ ki□m ch□ng có đúng là malware lo□i rootkit không.

C□n s□ d□ng lo□i nhu li□u rà soát các process thông d□ng nh□ sysinternals (http://technet.microsoft.com/fr-fr/sysinternals
) đ□ ki□m soát xem có nh□ng process kh□ nghi (suspicious) nào đang ch□y trong máy hay không (process explorer V11.02).

M□c đ□ 3

Các bi□n pháp k□ thu□t c□n thi□t cho m□c đ□ 3

M□c đ□ 1 + 2
Th□m đ□nh rõ r□t m□c đ□ các r□i ro (Risks Analysis)
Quan tâm đ□n các c□nh báo (security alert) đ□ phòng ch□ng
Phòng ch□ng malware “0 day “, khi ch□a tìm ra đ□□c d□u □n c□a malware. Stormshield
Ki□m soát registry

Đ□c đi□m:

□ t□ng 3 v□ an ninh, khi áp d□ng tri□t đ□ các bi□n pháp phòng ch□ng, m□c đ□ an ninh t□ng quát đ□t kho□ng 99% (tr□ r□i ro đ□n t□ các malware lo□i “0 day “đ□c bi□t, có nghĩa là ch□a có d□u □n và nh□m vào m□t s□ m□c tiêu nh□t đ□nh). □ m□c này, v□i s□ hi□u bi□t các r□i ro trên m□ng và v□ an ninh máy vi tính, xác xu□t b□ xâm nh□p r□t th□p.

N□u máy đ□□c s□ d□ng vào m□t s□ l□u tr□ d□ ki□n quan tr□ng, đ□c bi□t, c□n ti□n hành m□t th□m đ□nh m□c đ□ r□i ro (risks analysis, method EBIOS, MEHARI, MARION, SANS (www.sans.org), Risk Management Guide c□a NIST http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf , đ□ l□□ng đ□nh nh□ng r□i ro cao nh□t c□n phòng ch□ng và m□c đ□ an ninh và các bi□n pháp k□ thu□t c□n thi□t.

C□n ghi danh và thu nh□n nh□ng c□nh báo đ□n t□ nh□ng c□ quan an ninh thông tin qu□c gia (National CERT Computer Emergency Response Team, CERT-US, ANSSI (Pháp), BSSI (Đ□c), ENISA (Liên Âu)), và t□ các phòng thí nghi□m v□ an ninh thông tin (security labs) c□a các công ty l□n v□ an ninh thông tin (McAfee, Sophos, Symantec, …). Nh□n nh□ng c□nh báo này giúp cho chúng ta bi□t tr□□c m□t s□ r□i ro (risks), đe d□a (threats) hay y□u kém (vulnerabilities) đang x□y ra trên m□ng và có m□t s□ bi□n pháp phòng ch□ng t□i thi□u c□n làm ngay.

Nh□ng đi□m c□n quan tâm:

C□n l□y algorithm mã hóa symetric m□t chìa khóa AES (Advanced Encryption Standard v□i đ□ dài (key length) 128 bits thay th□ DES hay 3DES), hay algorithm mã hóa asymetric RSA 2048 bits 2 chìa khóa đ□ có m□t m□c đ□ an ninh v□a ph□i ch□ng l□i kh□ năng gi□i mã (decryption) trong m□t t□□ng lai nhìn th□y đ□□c.http://www.cryptovision.com/fileadmin/media/documents/Whitepaper_Produkte/Modern_Cryptography.pdf

Khi nh□n đ□□c security alert, c□n xem xét ngay c□nh báo có liên quan tr□c ti□p đ□n vi□c s□ d□ng máy vi tính, đi□n th□, skype, nhu li□u mã hóa, Adobe Reader, Microsoft Office hay không.

N□u có c□n áp d□ng ngay nh□ng khuy□n cáo.

C□n t□i xu□ng và thi□t trí Stormshield Personal Edition (http://spe.skyrecon.com/update/setup.exe), nhu li□u mi□n phí cho máy vi tính, có kh□ năng ch□ng l□i các y□u kém vulnerabilities " 0 day ", và ch□ng l□i các key logger m□t cách t□ đ□ng. Stormshield không di□t malware, nh□ng có kh□ năng ngăn ch□n (block) ho□t đ□ng kh□ nghi (suspicious) c□a malware (thí d□ nh□ nâng c□p quy□n h□n thành administrator, m□ ra c□ng (port) m□i đ□ liên l□c ra bên ngoài, s□a đ□i registry đ□ bám vào máy, …)

S□ d□ng Ccleaner hay m□t nhu li□u khác chuyên duy□t xét registry nh□ PCTools Registry Mechanic đ□ xoá th□□ng xuyên và rà l□i registry.

Quan tâm đ□n th□i h□n h□t chu k□ b□o trì các phiên b□n h□ th□ng đi□u hành, các ch□□ng trình □ng d□ng (application), đ□ chuy□n sang (migration) sang phiên b□n m□i h□n.

M□c đ□ 4

Các bi□n pháp k□ thu□t c□n thi□t cho m□c đ□ 4

M□c đ□ 1 + 2 +3

Xây d□ng kh□ năng đi□u tra, truy tìm malware (forensic)

Xây d□ng kh□ năng phân tích mã l□nh c□a malware đ□ tìm ra m□c tiêu, cách th□c ho□t đ□ng, ngu□n g□c c□a ng□□i ch□ t□o ra malware (reverse engineering)

Đ□c đi□m :

□ t□ng 4 v□ an ninh, khi áp d□ng tri□t đ□ các bi□n pháp phòng ch□ng, m□c đ□ an ninh t□ng quát đ□t kho□ng 99%+ (tr□ r□i ro đ□n t□ các malware lo□i "0 day "đ□c bi□t, có nghĩa là ch□a có d□u □n và nh□m vào m□t s□ m□c tiêu nh□t đ□nh). □ m□c này, v□i s□ hi□u bi□t các r□i ro trên m□ng và v□ an ninh máy vi tính, xác xu□t b□ xâm nh□p r□t th□p.

Đây là t□ng duy nh□t có đ□ c□p đ□n kh□ năng truy tìm ngu□n g□c, nh□ng đ□c đi□m c□a malware và n□u c□n ph□n công trên m□t pháp lý và k□ thu□t.

C□n xây d□ng kh□ năng đi□u tra và truy tìm malware (forensic) c□a các chuyên viên đi□n toán v□ an ninh đi□n t□ qua các khoá th□c t□p https://www.sans.org/security-training/advanced-computer-forensic-analysis-incident-response-98-mid , http://www.digitalintelligence.com/forensictraining.php
,
http://hsc-formation.fr/formations/forensic.html.fr

Nh□ng đi□m c□n quan tâm:

C□n quan tâm đ□n vi□c b□o qu□n t□t c□ nh□ng d□ li□u đ□□c s□ d□ng đ□ đi□u tra, không đ□□c thay đ□i (no write).

Tìm ra trong kh□i l□□ng d□ ki□n c□a image memory và image disk, đ□a ch□ IP, d□u □n (signature) c□a ng□□i ch□ t□o ra malware, qua vi□c phân tích mã l□nh (code analysis), tìm ra các cách th□c xâm nh□p, t□ t□n t□i trong máy, t□ che d□u, cách th□c thu th□p d□ ki□n, thay đ□i d□ ki□n và g□i v□ ng□□i ch□ malware.

Tìm ki□m d□u v□t xác đ□nh malware có thu□c m□t botnet nh□ Zeus, TLD4, Mariposa, … http ://www.damballa.com/downloads/r_pubs/WP_Malware_Samples_Botnet_Detection.pdf , đ□ block b□ng firewall.

L□p h□ s□ v□i đ□y đ□ d□ ki□n đ□ g□i cho ISP, c□ quan cung c□p d□ch v□ m□ng và c□ quan an ninh m□ng s□ t□i đ□ có m□t s□ bi□n pháp (active) c□n thi□t.

Reference:
ANSSI www.ssi.gouv.fr (Pháp)
ENISA www.enisa.europa.eu (Liên Âu) European Networks and Information Security Agency
SANS www.sans.org
NIST www.nist.org
CERT-US www.us-cert.gov
AUSCERT (Autralian Computer Emergency Response Team)
CERT-A www.certa.ssi.gouv.fr

Download tài li□u qua d□ng PDF.