Vi□t Nam tr□□c hi□m h□a t□n công APT

Tr□□c các cu□c t□n công ngày càng tinh vi và có ch□ đích, nhi□u t□ ch□c, doanh nghi□p b□ xâm nh□p và gánh ch□u thi□t h□i tàn kh□c là khó tránh kh□i.

Ông Tất Thành Cang – Phó Bí th□, Phó Ch□ t□ch UBND TP.HCM cho bi□t, Thành ph□ tr□□c đây đã phê duy□t ch□□ng trình xây d□ng và tri□n khai an ninh thông tin trong c□ quan qu□n lý nhà n□□c giai đo□n 2012-2015. □nh: Cao Minh

Đó là l□i c□nh báo c□a các chuyên gia đ□n t□ nhi□u công ty ho□t đ□ng trong lĩnh v□c an ninh thông tin, CNTT có uy tín trên th□ gi□i t□i Ngày ATTT Vi□t Nam 2015 t□i TP.HCM hôm 19/11. Theo các chuyên gia, s□ b□o v□ ngày nay là không đ□ đ□ đ□i phó v□i t□n công m□ng hi□n đ□i vì

các gi□i pháp tri□n khai khác nhau th□□ng đ□c l□p v□i nhau. Đ□ đ□t m□c tiêu gi□m thi□u nguy c□ b□ t□n công có ch□ đích thì các gi□i pháp an ninh m□ng ph□i đ□□c k□t h□p ch□t ch□ d□□i cái nhìn b□c tranh toàn c□nh, phát hi□n s□m, ph□n □ng nhanh.

H□ th□ng nào cũng có th□ b□ t□n công APT xuyên th□ng

T□n công có ch□ đích, hay t□n công APT g□n đây đ□□c nh□c t□i liên t□c, đ□c bi□t trong Ngày ATTT năm nay. V□y t□n công APT là gì và nguy hi□m ra sao?

APT là vi□t t□t c□a c□m t□ "Advanced Persistent Threat" – nh□ng m□i nguy hi□m cao th□□ng tr□c. T□n công APT là hình th□c mà hacker, hay m□t nhóm hacker có t□ ch□c, t□n công b□n b□ có ch□ đích nh□m vào t□ ch□c, doanh nghi□p (TC/DN) c□ th□ nh□m đ□t cho đ□□c m□c tiêu, ch□ng h□n nh□ đánh c□p d□ li□u quan tr□ng b□ng m□i cách.

T□i ph□m m□ng đang tr□ thành m□t ngành công nghi□p có l□i nhu□n l□n, giá tr□ hàng t□ đô la M□. Các cu□c t□n công c□a hacker chuyên nghi□p, có t□ ch□c, ph□n l□n là có ch□ đích nh□m ki□m ti□n ho□c phá ho□i theo đ□n đ□t hàng. Theo các chuyên gia thuy□t trình t□i Ngày ATTT 2015, t□i ph□m m□ng đang có nh□ng b□□c phát tri□n r□t nhanh, s□ d□ng nhi□u k□ thu□t tiên ti□n, khai thác các l□ h□ng zero-day, t□n công b□ng nhi□u ph□□ng th□c tinh vi đ□ xuyên th□ng các h□ th□ng phòng v□.

Đi□u đ□c bi□t nguy hi□m c□a t□n công APT là hacker có th□ t□o ra malware riêng cho t□ng m□c tiêu c□ th□, □ b□nh r□t lâu, th□m chí theo chia s□ c□a các chuyên gia b□o m□t thì có nh□ng lo□i malware có hành vi th□ hi□n r□t ít nên c□c k□ khó phát hi□n, k□ c□ khi ch□y ki□m th□ trong môi tr□□ng gi□ l□p Sandbox. V□i nh□ng lo□i malware này, gi□i pháp truy□n th□ng d□a trên phân tích ch□ ký (signature) tr□ nên b□t l□c trong vi□c phát hi□n và ngăn ch□n.

Chiêu th□c đánh l□a ki□u phi k□ thu□t (social engineering) thông qua nh□ng email hay website có ch□a mã đ□c v□n đ□□c hacker dùng nhi□u và r□t hi□u qu□. Xu h□□ng BYOD và ng□□i dùng truy c□p làm vi□c t□ xa cũng t□o đi□u ki□n h□n cho hacker xâm nh□p m□ng TC/DN. Vi□c truy tìm hacker không h□ d□, ch□a k□ là t□i ph□m t□n công m□ng và n□n nhân th□□ng không cùng m□t qu□c gia nên càng gây khó cho các c□ quan th□c thi pháp lu□t.

Minh ch□ng rõ nh□t là tr□□ng h□p nhóm APT30 su□t 10 năm qua đã t□n công nhi□u c□ quan chính ph□ và nhà báo t□i các n□□c Đông Nam Á, trong đó có Vi□t Nam, b□ng cùng m□t ph□□ng th□c mà g□n đây m□i b□ phát hi□n, theo công b□ c□a công ty b□o m□t FireEyE c□a M□ trong m□t cu□c h□p báo h□i tháng 5.

V□ hãng phim Sony Pictures b□ hacker t□n công vào cu□i năm 2014 gây thi□t h□i hàng t□ đô la M□, và nhi□u n□n nhân tr□□c đó nh□ Home Depot, eBay, JPMorgan báo hi□u các TC/DN đang đ□i m□t v□i nguy c□ thi□t h□i khó l□□ng n□u ph□□ng th□c b□o m□t không thay đ□i.

M□c đ□ nguy hi□m c□a t□n công APT đ□□c ông Nguy□n Thành Đ□ng – k□ s□ b□o m□t c□a công ty NPCore chia s□ t□i Ngày ATTT, qua s□ c□ nhi□u ngân hàng và đài truy□n hình Hàn Qu□c b□ tê li□t do hacker t□n công vào năm 2013, t□n th□t vô cùng to l□n. Đây đ□u là nh□ng đ□n v□ có h□ t□ng CNTT t□t v□i h□ th□ng an ninh thông tin đ□□c đ□u t□ bài b□n.

T□i Vi□t Nam, theo ông Võ Đ□ Th□ng – Giám đ□c Trung tâm Athena cho bi□t, d□ li□u n□i b□ TC/DN có giá tr□ đang là đích nh□m t□n công APT. Đ□i t□□ng b□ t□n công nhi□u t□p trung vào nhóm các DN t□ nhân, FDI có doanh thu l□n, nh□t là nh□ng đ□n v□ không có ng□□i chuyên trách CNTT. Nhi□u doanh nghi□p có s□n ph□m đ□c quy□n nh□ đi□n, n□□c, xăng, d□u, th□c ph□m, cùng các ngân hàng, c□ quan chính ph□ cũng là đ□i t□□ng c□a t□n công APT, nhi□u đ□n v□ b□ xâm nh□p sâu.

“Có doanh nghi□p FDI □ Bình D□□ng b□ cài mã đ□c trong h□ th□ng máy tính h□n m□t năm mà không bi□t, đã b□ m□t hàng gigabyte d□ li□u k□ toán, bí m□t kinh doanh, các b□n thi□t k□ s□n ph□m… Giá tr□ thi□t h□i s□ b□ lên đ□n hàng trăm ngàn đô la M□”, ông Th□ng cho bi□t.

T□n công phá ho□i đáng chú ý t□i Vi□t Nam là v□ VCCorp b□ t□n công làm ng□ng tr□ nhi□u ngày m□t lo□t trang web trong n□□c có l□□t truy c□p cao mà công ty ch□u trách nhi□m qu□n lý k□ thu□t, gây thi□t h□i cho VCCorp hàng ch□c t□ đ□ng.

Tình hình chung là s□ vi ph□m không còn là “n□u” mà là “khi nào”. Và TC/DN s□ ch□u thi□t h□i tàn kh□c do m□t quá nhi□u th□i gian đ□ phát hi□n malware. Theo th□ng kê, th□i gian trung bình đ□ phát hi□n xâm nh□p đã gi□m xu□ng còn 205 ngày – v□n là kho□ng th□i gian quá l□n.


[*] Trying ip 192.168.100.93
[*] Trying ip 192.168.100.92
[*] Trying ip 192.168.100.95
[*] Trying ip 192.168.100.85
[*] Trying ip 192.168.100.68
[*] Trying ip 192.168.100.97
[*] Trying ip 192.168.100.90
- Error connect
ip 192.168.100.63
ip 192.168.100.80
ip 192.168.100.99
- Error connect
- Error connect
execution compl