#HNS-WI-13-028

북한 의심 APT 공격에 대한 Kaspersky 의 분석 정리

2013-09-12

내용 요약

이 보고서는 Kaspersky의 Dmitry Tarakanov가 작성하여 우리나라 시간으로 9월 12일 발표한 "The 'Kimsuky' Operation: A North Korean APT?"를 정리 및 분석한 것으로, Kaspersky는 지난 몇 달 동안 한국의 세종연구소, KIDA(한국국방연구원), 통일부, 현대해상, '통일을 생각하는 사람들의 모임' 등에 대한 사이버 첩보 작전을 모니터링해왔음

'Kimsuky' Operation이라고 이름을 붙인 것은 수집된 정보가 전송되는 메일 계정이 '김숙향'이라는 이름으로 등록되어 있기 때문임

Kaspersky가 이 작전을 북한의 행위로 추정하는 근거는 다음과 같음

1. 악성코드 컴파일 경로에 '공격'이라는 문자열이 발견됨
2. 북한과 연결지을 수 있는 정부기관, 연구소, 기업 등이 그 대상이 됨
3. 한국에서 주로 사용되는 안랩의 방화벽이 공격 대상이 되고 있음
4. hwp 파일을 수집함
5. 수집된 정보가 전송되는 이메일 계정 등록자가 북한식 이름 '김숙향'으로 되어 있음
6. 공격자의 IP가 북한 근처 지역인 중국 지린성, 랴오닝성 지역의 ISP에서 제공하는 IP임

1. 개요

이 보고서는 Kaspersky의 Dmitry Tarakanov가 작성하여 우리나라 시간으로 9월 12일 발표한 "The 'Kimsuky' Operation: A North Korean APT?"[1]를 정리 및 분석한 것으로, Kaspersky는 지난 몇 달 동안 한국의 세종연구소, KIDA(한국국방연구원), 통일부, 현대해상, '통일을 생각하는 사람들의 모임' 등에 대한 사이버 첩보 작전을 모니터링해왔음

전체 공격 대상의 리스트는 알려지지 않았으며, Kaspersky가 발견했다고 하는 국내 타깃 11개 중 일부 조직의 이름만 공개한 것은 영업 전략과 관련되어 있는 것으로 판단되며, 모니터링 방법은 공개하지 않았음

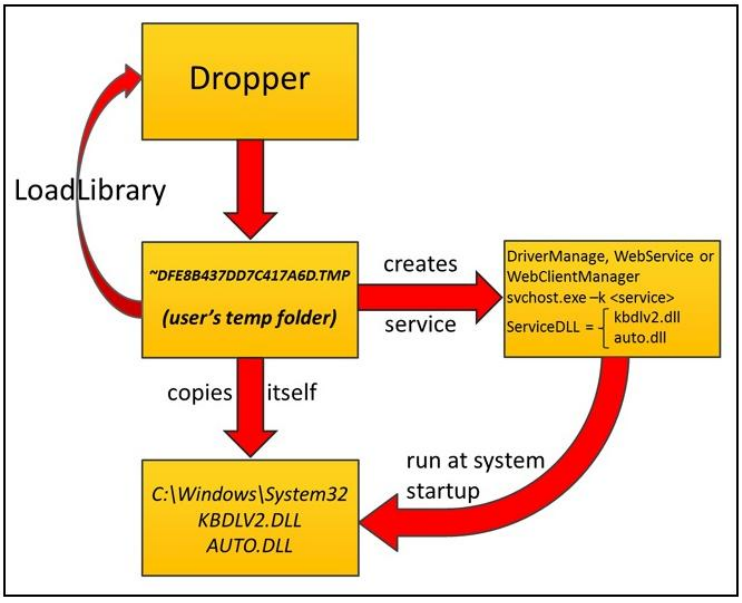
Kaspersky는 이 공격에 사용된 악성코드가 어떻게 유포되었는지 확인하지 못했으며, 분석에 사용된 악성코드의 샘플은 스피어 피싱 이메일을 통해 전달된 초기 단계의 악성코드임

Kaspersky 측에서 관심을 가진 부분은 불가리아의 웹 메일 서비스(mail.bg)와 파일 컴파일 경로(***D:\rsh\공격\UAC_dll(완성)\Release\test.pdb***)에 '공격'과 '완성'과 같은 한글 문자들이 사용되었다는 것임

2. 세부내용

시스템 감염

- 악성코드의 시스템 감염 과정은 다음과 같음



① dropper는 또 다른 하나의 암호화된 라이브러리를 로딩
(dropper에 의해 로딩된 이 라이브러리가 실제 모든 첩보 기능을 하는 수행함)

[1] http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT

② 로딩된 라이브러리는 Metasploit Framework의 Win7Elevate를 사용해 악성코드를 explorer.exe에 인젝트하고, 인젝트된 악성코드는 또 다른 감시용 라이브러리를 *~DFE8B437DD7C417A6D.TMP*와 같은 형식으로 사용자의 임시 폴더에 저장함

③ 인젝트된 악성코드는 System32 폴더에 KBDLV2.DLL 또는 AUTO.DLL이라는 이름으로 자신을 복사하고, DriverManage, WebService, WebClientManager와 같은 이름의 서비스를 실행시키는데, 이것들은 시스템이 다시 부팅된 후에도 악성코드가 작동할 수 있도록 하는 역할을 함(이 단계에서 악성코드는 감염된 시스템의 정보를 수집하여 oledvbs.inc라는 파일에 저장하고, 이 파일은 하드코딩된 `C:\Program Files\Common Files\System\Ole DB\oledvbs.inc`에 저장됨)

 # 감시 모듈

- 이 첩보전에 동원되는 악성 프로그램들이 많지만 각각은 단일 기능만 하는 경우가 대부분으로, 다음과 같은 기능을 함

* 키로깅
* 디렉토리 목록 수집
* hwp 문서 수집
* 원격 다운로드 및 실행
* 원격 통제

 # 방화벽 통제

- 감염된 시스템이 부팅되면 악성코드는 레지스터리의 다음 값을 0으로 만들어 Windows 시스템의 방화벽과 안랩의 방화벽을 비활성화시킴

```
SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile
   EnableFirewall = 0

SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\PublicProfile
   EnableFirewall = 0

HKLM\SOFTWARE\AhnLab\V3IS2007\InternetSec
   FWRunMode = 0

HKLM\SOFTWARE\Ahnlab\V3IS80\is
   fwmode = 0
```

- 시스템의 방화벽이 비활성화되었다는 사실을 감추기 위해 Windows Security Center 서비스를 역시 꺼버림

- 악성코드가 안랩의 방화벽을 비활성화시키면 C:\WINDOWS\ 폴더에 taskmgr.exe가 존재하는지 확인하고, 존재하면 그 파일을 실행시키고, 매 30분마다 지시자에게 보고를 함

- Kaspersky의 분석가는 이 문서에서 한국의 관련 기관이 피해기관들 중 하나를 조사하면서 외국 보안 제품을 사용한 것을 비난했다는 내용과 실제로는 한국 기관들이 대부분 안랩 제품을 사용하고 있음을 언급하면서 책임을 안랩에 지우려는 뉘앙스를 풍기고 있는데, 이는 Kaspersky의 영업 전략인 것으로 판단됨

- 안랩의 해명에 따르면 해당 악성 코드에 대해서 이미 대응을 했다고 하며, 안랩 방화벽을 무력화하는 기능이 있는 것이지 무력화에 성공했다는 것을 반드시 의미하지 않는다고 함 (https://www.facebook.com/AhnLabOfficial?fref=ts 참고)

- 악성코드가 Windows 방화벽과 안랩의 방화벽을 비활성화시키는 것을 Kaspersky 연구원이 언급하였는데, 악성코드에 감염됨 취약한 시스템은 Kaspersky의 제품을 포함해 어떤 방화벽과 보안 솔루션도 무력화될 수 있으므로, Windows 자체 방화벽과 안랩 제품만을 비활성화시킨다면 뛰어난 공격툴로 간주할 수 없는 셈이며, 이 케이스의 경우 사실 악성코드에 대한 진단 가능성 여부를 두고 보안 제품의 질을 판단해야 하는 것이므로 Kaspersky 연구원의 언급은 영업 전략에서 나온 것으로 판단할 수 있음

- Kaspersky가 안랩의 방화벽에 대한 공격을 강조한 것은 영업 전략에서 나온 측면도 있지만 한국에서 주로 사용하고 있다는 점에서 북한이 개입되어 있을 수 있다는 것을 표현하기 방편으로 간주할 수 있을 것임

 # bot과 작전 수행자 사이의 통신

- bot과 작전 수행자 사이의 통신은 불가리아의 웹 기반의 무료 이메일 서버(mail.bg)를 이용하고, 봇이 이용하는 이메일 게정은 하드코딩되어 있음

- 봇이 하드코딩된 이메일 계정에 인증을 통해 접근하면 다시 지정된 다른 이메일 주소로 메일을 보내며, 첨부파일을 통해 감염된 시스템의 정보를 전송함

- 봇이 1차로 접근하는 메일 계정 목록은 다음과 같음(kaspersky가 찾아낸 계정임)
  beautifl@mail.bg
  ennemyman@mail.bg
  fasionman@mail.bg
  happylove@mail.bg
  lovest000@mail.bg
  monneyman@mail.bg
  sportsman@mail.bg
  veryhappy@mail.bg

- 봇이 두 번째로 접근하는 'master' 이메일 계정 목록
  iop110112@hotmail.com
  rsh1213@hotmail.com

 # 정보 보고

- 수집된 정보를 작전 수행자에게 보내는 과정

① systeminfo 명령의 결과물인 `oledvbs.inc` 파일 확인

② 사용자 관련 정보 파일인 sqlxmlx,inc 파일을 읽어려고 시도
(이 파일은 생성되지 않으며, 개발자의 실수로 추측하고 있음)

③ 키로깅 파일 확인

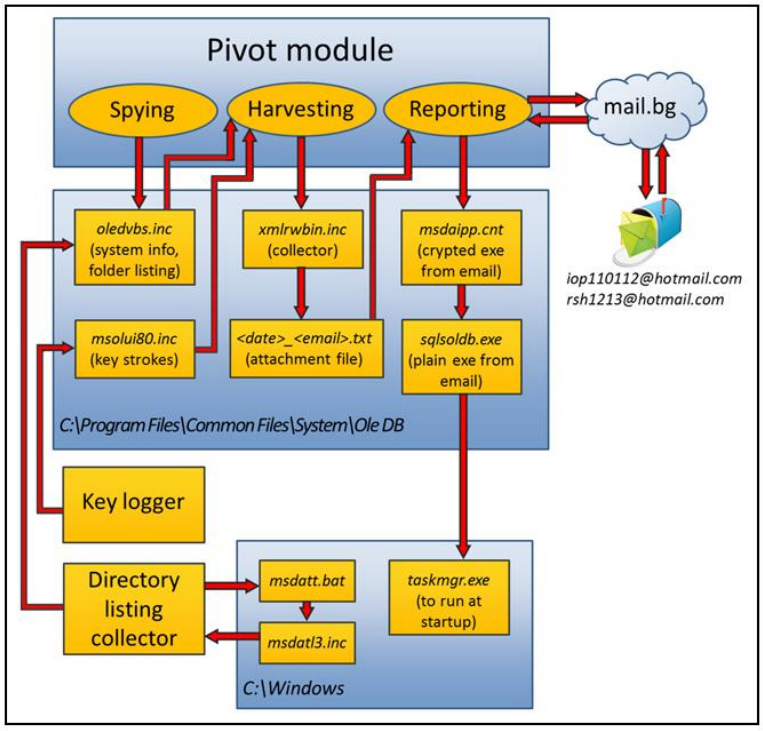
④ 위의 데이터를 통합하여 xmlrwbin.inc 파일로 만들며, 이것은 RC4로 암호화되고, 다시 RSA로 암호화되어 마스터에게 전송되며, 전송이 완료되면 이 파일은 즉시 삭제됨

- 악성코드는 메일 서버로부터 특정 제목 태그를 가진 계정을 확인하기도 함

- 키로깅된 정보는 `C:\Program Files\Common Files\System\Ole DB\msolui80.inc`에 저장됨

- 디렉토리 목록을 확인하기 위해 악성코드는 ***dir <drive letter>: /a /s /t /-c*** 명령을 내림

- 다음은 위의 과정을 정리한 것임



 # hwp 파일 수집 및 전송

- hwp 문서 파일을 수집하는 'stealer'가 있음

- 이 stealer는 감염된 시스템에서 모든 hwp 파일을 수집하는 것이 아니라 사용자가 오픈한 파일들에만 반응하고, 그 파일들을 확보함

- 이 stealer는 스스로를 HNC 디렉토리에 HncReporter.exe로 복사하고, 디렉토리의 내용을 다음과 같이 수정함

```
HKEY_CLASSES_ROOT\Hwp.Document.7\shell\open\command
또는
HKEY_CLASSES_ROOT\Hwp.Document.8\shell\open\command
```

- 기본 레지스트리 세팅은 "<Hangul full path>\Hwp.exe" "%1"와 같이 되어 있으나 이 세팅을 "<Hangul full path>\HncReporter.exe" "%1"로 변경하며, 따라서 사용자가 hwp 파일을 오픈하면 이 파일을 'Hwp'라는 제목으로 공격자에게 이메일의 첨부파일로 전송하게 되는 것임

- hwp 파일을 공격자에게 전송하는 것은 다음 루틴에 의존함

```
C:\Program Files\Common Files\System\Ole DB folder: xmlrwbin.inc, msdaipp.cnt, msdapml.cnt, msdaerr.cnt, msdmeng.cnt, oledjvs.inc
```

원격 통제

- 공격자는 원격 통제를 위해 TeamViewer 클라이언트(버전 5.0.9104)를 사용했으며, dropper는 C:\Windows\System32에 다음 세가지 파일은 생성함

  netsvcs.exe – 수정된 Team Viewer 클라이언트
  netsvcs_ko.dll – Team Viewer 클라이언트 리소스 라이브러리
  vcmon.exe – installer/starter;

- 또한 dropper는 원격 접근 서비스를 만들기 위해 시스템이 시작할 때마다 C:\Windows\System32\vcmon.exe를 실행하게 하는데, vcmon.exe가 실행되면 앞에서 언급한 것처럼 레지스터리를 조작해 안랩의 방화벽이 비활성됨

- 방화벽이 비활성되면 Team Viewer의 레지스트리 값을 다음과 같이 수정함

```
HKLM\Software\Goldstager\Version5 -> HKLM\Software\Coinstager\Version5
```

* 이를 통해 원격 공격자는 사전에 설정된 값(패스워드 등)을 이용해 Team Viewer 클라이언트에 접근함

 # master 이메일 계정 등록자 정보

- 두 master 이메일 계정 iop110112@hotmail.com와 rsh1213@hotmail.com의 등록자는 각각 'kimsukyang'과 'Kim asdfa'으로 되어 있으며, 'kimsukyang'에서 'kimsuky'만 사용하여 글의 제목으로 삼고 있으며, Kaspersky의 악성코드 진단명에도 **Trojan.Win32.Kimsuky**로 사용하고 있음

- 이 두 이름 중 첫번 째 이름 '김숙향'은 북한식 이름으로 Kaspersky 분석자는 판단하고 있으며, 이것은 Kaspersky 연구자가 이 악성코드를 이용한 정보수집 활동이 북한에 의해 이루어졌다고 판단하는 중요한 근거가 되고 있으나 분석가 역시 공격자에 대한 정확한 정보임을 확신하지는 못하고 있음

- Kaspersky 연구자의 분석 과정에서 공격자의 IP 10개를 찾았으며, 이 IP들은 지린성, 랴오닝성 네트워크 소속의 것임을 확인하고, 북한과 가까운 지역에 위치하는 것을 통해 북한의 공격으로 추정하고 있으나 역시 확신은 하지 못하고 있음

3. 기타

- 악성코드가 사용한 파일들

```
%windir%\system32\kbdlv2.dll
%windir%\system32\auto.dll
%windir%\system32\netsvcs.exe
%windir%\system32\netsvcs_ko.dll
%windir%\system32\vcmon.exe
```

```
%windir%\system32\svcsmon.exe
%windir%\system32\svcsmon_ko.dll
%windir%\system32\wsmss.exe
%temp%\~DFE8B437DD7C417A6D.TMP
%temp%\~DFE8B43.TMP
%temp%\~tmp.dll
C:\Windows\taskmgr.exe
C:\Windows\setup.log
C:\Windows\winlog.txt
C:\Windows\update.log
C:\Windows\wmdns.log
C:\Windows\oledvbs.inc
C:\Windows\weoig.log
C:\Windows\data.dat
C:\Windows\sys.log
C:\Windows\PcMon.exe
C:\Windows\Google Update.exe
C:\Windows\ReadMe.log
C:\Windows\msdatt.bat
C:\Windows\msdatl3.inc
C:\Program Files\Common Files\System\Ole DB\msdmeng.cnt
C:\Program Files\Common Files\System\Ole DB\xmlrwbin.inc
C:\Program Files\Common Files\System\Ole DB\msdapml.cnt
C:\Program Files\Common Files\System\Ole DB\sqlsoldb.exe
C:\Program Files\Common Files\System\Ole DB\oledjvs.inc
C:\Program Files\Common Files\System\Ole DB\oledvbs.inc
C:\Program Files\Common Files\System\Ole DB\msolui80.inc
C:\Program Files\Common Files\System\Ole DB\msdaipp.cnt
C:\Program Files\Common Files\System\Ole DB\msdaerr.cnt
C:\Program Files\Common Files\System\Ole DB\sqlxmlx.inc
<Hangul full path>\HncReporter.exe
```

- 관련 MD5

3baaf1a873304d2d607dbedf47d3e2b4

3195202066f026de3abfe2f966c9b304

4839370628678f0afe3e6875af010839

173c1528dc6364c44e887a6c9bd3e07c

191d2da5da0e37a3bb3cbca830a405ff

5eef25dc875cfcb441b993f7de8c9805

b20c5db37bda0db8eb1af8fc6e51e703

face9e96058d8fe9750d26dd1dd35876

9f7faf77b1a2918ddf6b1ef344ae199d

d0af6b8bdc4766d1393722d2e67a657b

45448a53ec3db51818f57396be41f34f

80cba157c1cd8ea205007ce7b64e0c2a

f68fa3d8886ef77e623e5d94e7db7e6c

4a1ac739cd2ca21ad656eaade01a3182

4ea3958f941de606a1ffc527eec6963f

637e0c6d18b4238ca3f85bcaec191291

b3caca978b75badffd965a88e08246b0

dbedadc1663abff34ea4bdc3a4e03f70

3ae894917b1d8e4833688571a0573de4
8a85bd84c4d779bf62ff257d1d5ab88b
d94f7a8e6b5d7fc239690a7e65ec1778
f1389f2151dc35f05901aba4e5e473c7
96280f3f9fd8bdbe60a23fa621b85ab6
f25c6f40340fcde742018012ea9451e0
122c523a383034a5baef2362cad53d57
2173bbaea113e0c01722ff8bc2950b28
2a0b18fa0887bb014a344dc336ccdc8c
ffad0446f46d985660ce1337c9d5eaa2
81b484d3c5c347dc94e611bae3a636a3
ab73b1395938c48d62b7eeb5c9f3409d
69930320259ea525844d910a58285e15