6월 25일 오전 10\ DDoS(Distributed Denial of Service) 공격 \_인랩 분석

.

**[업데이트 히스토리]**

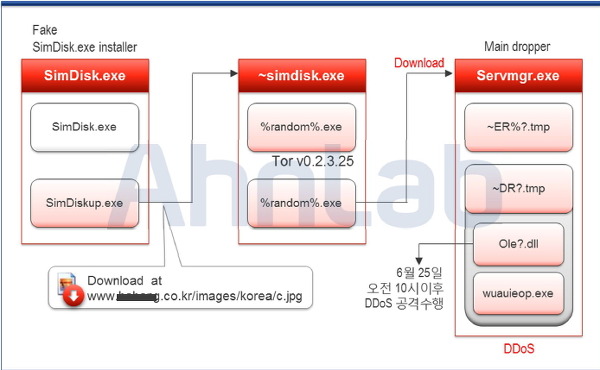
1) **2013.06.25** - 6.25 DDoS 공격에 사용된 악성코드 상세 분석 내용 최초 작성

2) **2013.06.26** - 6.25 DDoS 공격에 사용된 악성 스크립트 상세 분석 내용 추가

**1. 공격 시나리오**

특정 웹하드 업체(www.simdisk.co.kr)의 설치 파일(RARSFX)을 변조하여 압축 해제 후 SimDiskup.exe 가 실행 되도록 해두었다.

아래 이미지는 이 번에 유포된 악성코드들의 전체적인 상관 관계를 도식화한 이미지이다.



**2. 주요 파일 분석 정보**

**1) servmgr.exe (4,383,232 바이트)**

해당 파일은 전체적인 구조에서 드롭퍼(Dropper) 역할을 수행하도록 제작된 악성코드이다. 해당 파일의 리소스(Resource) 영역에는 다른 PE 파일 4개를 포함하고 있으나, 실제로는 동일한 기능을 수행하는 32비트(Bit)와 64비트(Bit) 악성코드로 나누어져 있다.

아래 이미지는 해당 파일에 대한 구조를 도식화 한 것 이다.



해당 악성코드가 실행이 되면 우선 감염된 시스템의 운영체제 버전 정보를 체크한 후, OpenFileMappingA 함수를 호출하여 동일한 악성코드에 이미 감염되어 있는지를 확인하게 된다.

MappingName = "Global\MicrosoftUpgradeObject9.6.4"

그리고 감염된 시스템의 윈도우가 32비트인지 64비트 운영체제인지를 확인하여, 해당 윈도우 운영체제  환경에 맞는 파일들을 생성하게 된다. 그리고 GetVersionExA 함수를 이용하여 윈도우 운영체제의 버전 정보가 6.0 (Vista) 이상일 경우에는 UAC(User Access Control)를 무력화 한 후 다른 파일들을 추가로 생성하게 된다.

우선 32비트 윈도우 운영체제에서는 %Temp% 폴더에 **~DR(임의의 숫자).tmp** (1,995,776 바이트) 파일을 생성 한 후에 별도의 인자값 없이 LoadLibaray 함수를 호출하여 자신을 로드 하게 된다.

이후 다시 **Ole(윈도우 정상 서비스명).dll** (936,448 바이트) 파일을 생성하고 윈도우 서비스로 등록 한다. **~DR(임의의 숫자).tmp**가 생성한 파일은  "Ole" 문자열과 감염된 시스템의 윈도우 서비스명을 조회하여 이를 조합하여 파일명을 생성하게 된다.

해당 **Ole(윈도우 정상 서비스명).dll** 파일은 특정 파일을 다운로드 한 이 후, 다운로드 한 파일에서 특정 조건이 확인 되면 DoS(Denial of Service) 공격을 수행하는 파일을 생성하고 실행하게 된다.

그리고 64비트 윈도우 운영체제에서는 다음 2개 파일 생성 한 이후에 CreateProcessA 함수를 이용하여 실행하게 된다.

\* 사용자 계정의 임시 폴더(Temp)에 **~ER6.tmp** (215,048 바이트)

64비트 윈도우 운영체제에서 UAC 무력화 기능을 수행하는 파일이다.

\* 사용자 계정의 임시 폴더(Temp)에 **~DR7.tmp** (146,170 바이트)

32비트 윈도우 운영체제에서 로드 한 파일과 동일한 기능을 수행하는 파일로 Ole(정상윈도우서비스명).dll 파일을 윈도우 서비스로 등록하게 된다.

그리고 해당 파일들을 실행하기 위한 인자값으로 다음을 사용한다.

"C:\DOCUME~1\(사용자 계정)\LOCALS~1\Temp\~ER6.tmp"

"C:\DOCUME~1\(사용자 계정)\LOCALS~1\Temp\~DR7.tmp"

해당 파일들이 정상적으로 실행이 되면 이 후 다음 배치(Batch) 파일을 생성하여, 자기 자신을 삭제하게 된다.

C:\DOCUME~1\(사용자 계정)\LOCALS~1\Temp\ud.bat

**2) Ole(윈도우 정상 서비스명).dll (936,448 바이트)**

해당 악성코드는 윈도우 시스템 폴더(system32)에 ole(윈도우 정상 서비스명).dll 라는 파일 형태로 생성하여 실행 된다.

그러나 드로퍼에 의해 감염 될 때 마다 임의의 문자열을 사용하여 파일명이 달라지게 된다. 파일의 첫 문자열인 Ole는 접두어로 항상 일정하게 생성되나, 나머지 문자열은 감염된 시스템에 존재하는 정상 윈도우 시스템 파일들 중 하나의 DLL 파일명을 조합하여 사용하는 것으로  추정 된다.

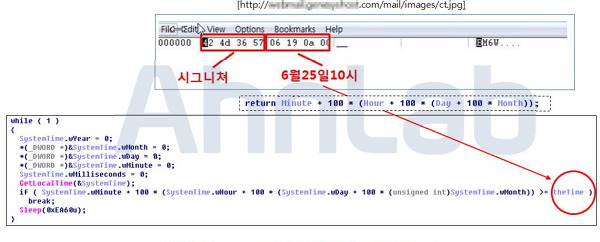
그리고 해당 파일은 윈도우 서비스로 동작 하며, 다음의 URL로 접속을 시도하여 성공하게 될 경 다른 파일을 다운로드 하게 된다.

webmail.genesyshost.com/mail/images/ct.jpg

www.hostmypic.net/pictures/e02947e8573918c1d887e04e2e0b1570.jpg

파일 다운로드가 성공하게 될 경우에는 사용자 계정의 임시 폴더(Temp)에 **~MR(임의의 숫자 2자리).tmp** 파일을 생성하게 된다.

해당 파일은 시그니쳐('BM6W')와 시간 정보(6월 25일10:00)를 포함하고 있는 데이터 파일로서, 감염된 시스템의 시간 정보를 비교하여 동일 할 경우에는 윈도우 시스템 폴더(system32)에 **wsauieop.exe**(847,872 바이트) 파일을 생성하고 실행하게 된다.



**3) wuauieop.exe (847,872 바이트)**

윈도우 시스템 폴더(system32)에 생성된 **wuauieop.exe** (847,872 바이트) 파일은 DDoS 기능을 수행한다.

해당 파일 내부에는 DDoS 공격의 대상이 되는 시스템의 IP 2개가 하드코딩되어 있으며, 각각 쓰레드로 무한루프를 돌면서 DDoS 공격이 이루어 지게 된다.

**// 무한루프를 돌 때 보통 for 문을 많이 씁니다. While 문을 써도 되고 말씀하신 반복문을 사용합니다.**

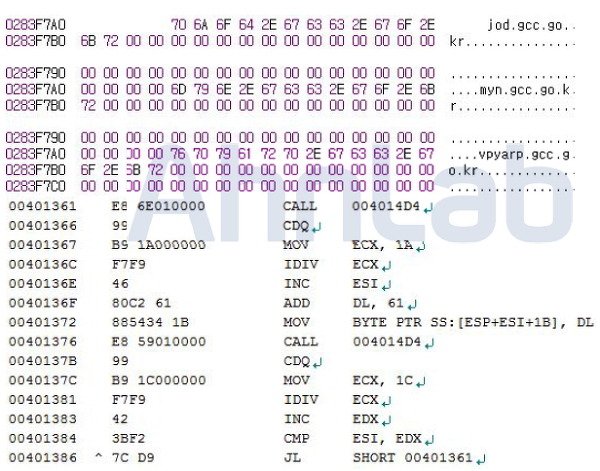
\* Thread Function(1) (=401110) 공격 대상 IP: "152.99.1.10:53"



\* Thread Function(2) (=4012A0) 공격 대상 IP: "152.99.200.6:53"

이 외에 추가로 2개의 쓰레드 루틴을 더 생성하여 임의의 도메인명을 생성하게 된다. 이는 임의의 도메인명들을 생성하여 DDoS 공격효과를 증대 시킨 것으로 추정 된다.

생성하는 임의의 도메인명들은 "**[임의의 문자열].gcc.go.kr**" 을 가지고 있으며, 사용하는 임의의 문자열은  a~z 까지의 ASCII로 무작위로 채워진다.



그리고, 도메인명에 사용하는 임의의 문자열은 최대 길이는 28자를 넘을 수가 없도록 제작 되었다.



**4) ~SimDisk.exe (3,405,824 바이트)**

해당 파일은 인터넷에 공개되어 있는 [**토르(Tor) 프로그램**](https://www.torproject.org/)의 소스코드를 사용하여 제작된 파일로 네트워크 접속 정보의 감시, 추적 및 분석을 어렵게 하기 위한 목적으로 제작 된 것으로 추정된다.

다음 경로에 다수의 파일들을 생성하며 생성한 파일들의 파일명은 윈도우 시스템 폴더(System32)를 조회하여 사용하는 것으로 추정된다.

C:\Documents and Settings\(사용자 계정명)\Application Data\Identities\{e38632c0-f9a0-11de-b643-806d6172696f}

cmd.exe (Npkcmsvc.exe) - conime.exe (tor.exe) 를 구동하는 런처 프로그램

config.ini - cmd.exe 가 참조하는 구성 설정 파일

conime.exe - 토르(Tor) 프로그램의 소스코드를 사용하여 제작한 파일

**3. DNS(Domain Name Service) DDoS 트래픽 분석**

**1) DNS DDoS**

DNS DDoS는 DNS 서버에 과도한 양의 네트워크 트래픽(Network Traffic)을 전송하여, 정상적인 DNS 조회가 성공하지 못하도록 서비스 거부를 유발하게 된다.

발생하는 트래픽은 2 개의 DNS 서버를 목표로 공격하였으며, 공격 대상이 되는 해당 네임 서버는 주요 정부 기관에서 사용하는 것으로 이로 인해 이번 공격의 대상이 된 것으로 추정된다.

ns.gcc.go.kr (152.99.1.10)

ns2.gcc.go.kr (152.99.200.6)

해당 악성코드에 의해 발생한 DDoS 공격 트래픽의 특징을 정리하면 다음과 같다.

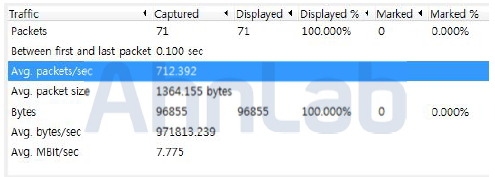
일반적인 경우 A Query인데 반해, 모두 ANY Query를 전송

질의는 하나의 NS에 전송하는 데 반해, 152.99.1.10, 152.99.200.6 을 동시에 요청

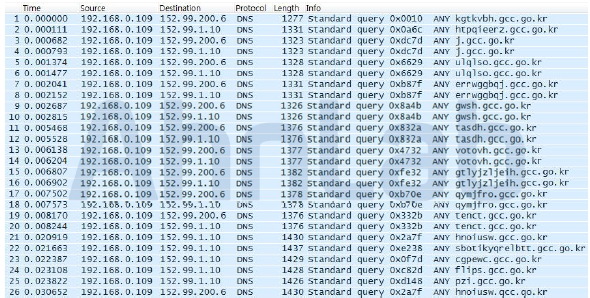
일반적인 DNS Query는 소량의 트래픽이지만, DNS 서버 부하를 위해 데이터 크기를 1300~1400 Byte로 조정

ANY 레코드가 사용 된 점은 "gcc.go.kr" 의 주 네임 서버를 효과적으로 공격하기 위한 것이며, [임의의 문자열].gcc.go.kr 를 쿼리(Query)에 사용한 점은 랜덤 호스트명을 사용하여 캐쉬(Cached) 된 정보 재사용으로 인해 공격 효과가 떨어지는 것을 막기 위해서 이다. 그리고 약 1400 bytes 의 데이터를 사용한 것은 공격 네임 서버로의 밴드위쓰(Bandwidth)  소모하기 위해서이다.

악성코드에 의해 생성된 패킷(Packet)에서는 초당 약 712회의 DNS Query를 전송하는 것으로 확인 되었다.



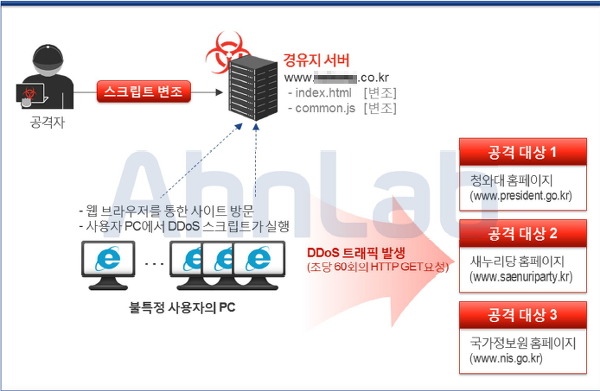
DNS Query의 형식은 아래 이미지와 같이 [임의의 문자열의 호스트 이름].gcc.go.kr로 되어 있다.



**4. DDoS 공격 악성 스크립트 분석**

**1) 스크립트 기반의 DDoS 공격 시나리오**

이번 6.25 DDoS 공격에는 기존의 좀비 PC를 이용한 공격 외에 악성 스크립트를 이용한 공격 방식이 이용됐다. 이 경우, 일반 사용자가 웹 브라우저를 통해 변조된 서버를 방문하는 것만으로 악성 트래픽을 발생하게 된다.



위 이미지는 스크립트(Script) 기반의 DDoS 공격의 시나리오를 재구성한 것으로, 주요 공격 진행 과정은 다음과 같다.

\* 공격자는 사전에 다수의 불특정 사용자들이 방문하는 경유지 서버를 해킹

\* 경유지 서버에서 사용하는 정상적인 페이지에 DDoS 공격 스크립트 삽입

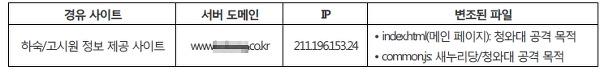
\* 불특정 다수 사용자들이 웹 브라우저로 경유지 서버 방문시, 사용자 PC 상에서 DDoS 공격 스크립트 실행

\* 스크립트에 설정된 공격 대상 서버에 다량의 HTTP GET을 요청해 악성 트래픽 유발

**2) 경유지/공격대상 서버 정보**

**\* 경유지 서버**

경유지로 이용된 서버는 외국인들이 주로 이용하는 하숙/고시원 정보 제공 사이트로, 공격 목적에 따라 다음과 같이 일부 파일이 변조되었으나 현재 정상화되었다.



\* 공격 대상 서버

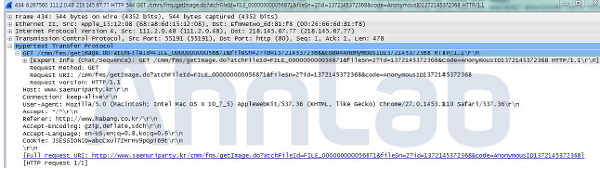
공격 대상인 3개 사이트의 총 60개 하위 URL을 대상으로 DDoS HTTP GET 공격이 이루어졌다.

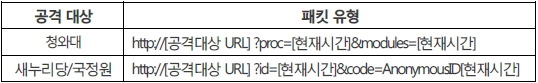


**3) 공격 트래픽 분석**

**\* HTTP GET 패킷 정보**

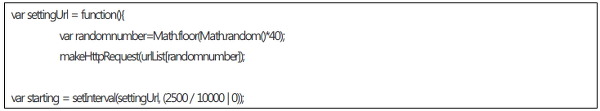
아래 이미지는 HTTP GET 요청 패킷 정보로, 아래 표의 HTTP GET 요청의 특징적인 부분을 확인할 수 있다.



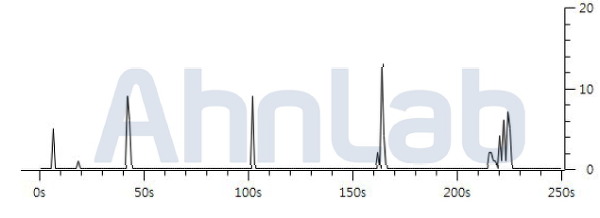


**\* DDoS 트래픽 통계 정보**

공격 스크립트는 아래 이미지와 같이 0.25 ms 단위로 공격 대상 URL을 랜덤으로 선택하여 HTTP GET 요청을 시도하도록 구현되어 있다.



분석 환경에서 재현한 결과, 아래 이미지과 같이 대략 초당 60회의 HTTP GET 요청을 시도하는 것으로 분석되었으나, 사용자 시스템에 따른 영향이 있을 수 있다.

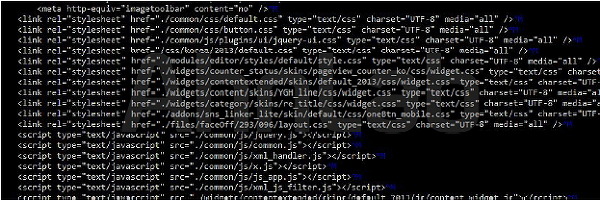


**4) 공격 스크립트 구성**

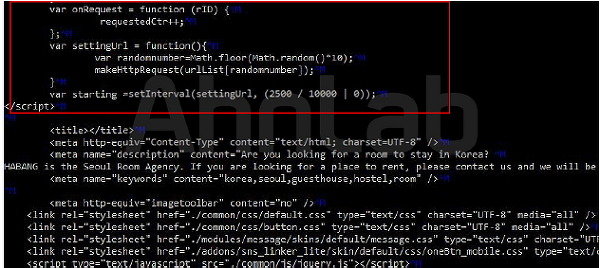
공격자는 다음과 같이 다수의 사용자가 방문하는 경유지 서버(www.\*\*\*\*\*\*\*\*.co.kr)를 해킹하여 DDoS 공격을 수행하는 스크립트를 삽입하였다.

[메인 페이지]

www..\*\*\*\*\*\*\*\*\*.co.kr/index.html - 청와대 공격용 스크립트 삽입

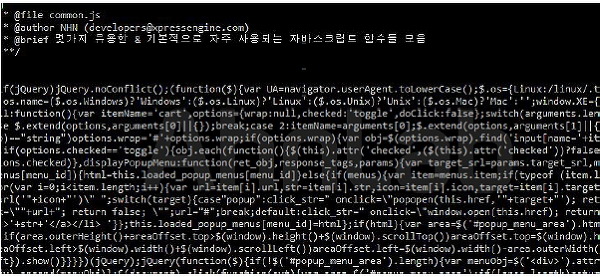


위 이미지는 경유지 서버의 메인 페이지가 변조 전의 코드들이며, 아래 이미지는 공격자에 의해 변조된 메일 페이지 모습을 나타낸다.

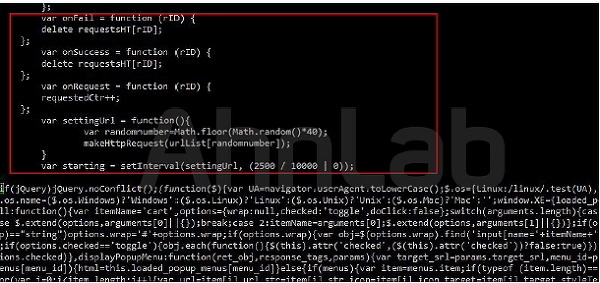


[공통 자바 스크립트 파일]

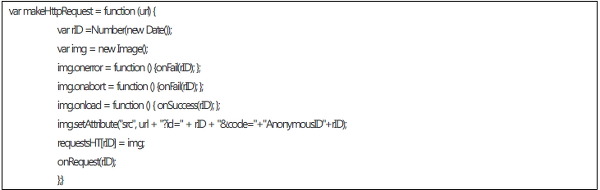
www..\*\*\*\*\*\*\*.co.kr/common/js/common.js - 새누리당/국정원 공격용 스크립트 삽입



위 이미지는 경유지 서버의 변조 전의 자바 스크립트(Java Script) 코드이며, 아래 이미지는 공격자에 의해 변조된 자바 스크립트 코드 모습을 나타낸다.



아래 이미지와 같이 makeHTTPRequest 함수에서 실제 공격 URL을 구성해 HTTP GET 요청 트래픽을 발생시킨다.

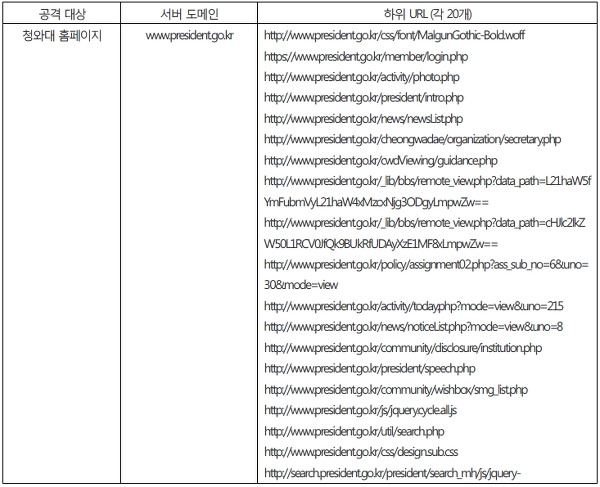


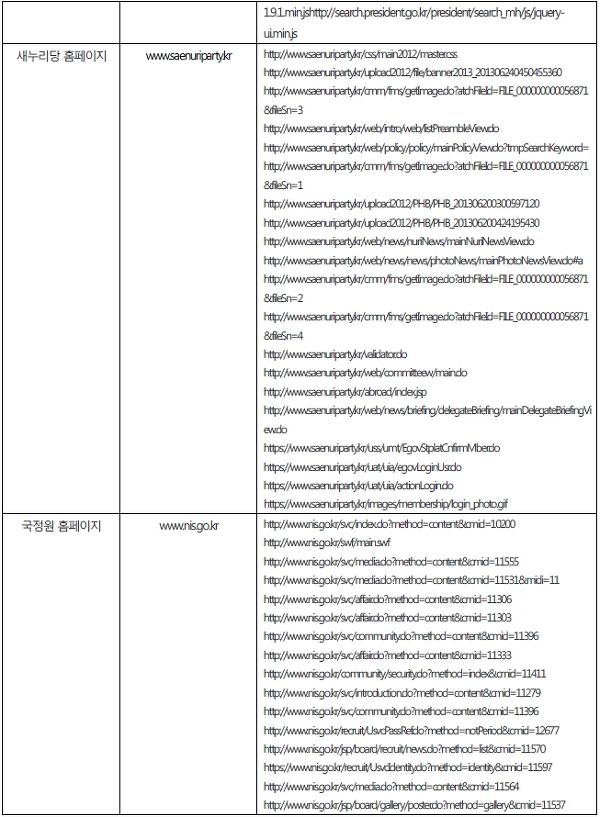
아래 이미지와 같이 setInterval 함수를 이용해 일정 시간 단위로 공격 URL을 요청하는 settingUrl 함수를 호출한다.



**5) 공격 대상 상세 정보**

아래 표와 같이 공격 대상인 3개 사이트의 하위 URL 총 60개를 대상으로 HTTP GET 요청을 반복적으로 수행한다.







6월 25일 오전 정부 기관 홈페이지를 대상으로 발생한 DDoS(Distributed Denial of Service) 공격을 수행하도록 제작된 악성코드들은 2013.06.25.04 버전 이후의 최신 엔진으로 업데이트 한 V3 제품군들에서는 모두 다음과 같이 진단한다.

**Trojan/Win32.Ddkr**

**Trojan/Win32.XwDoor**

앞서 언급한 바와 같이 ASEC에서는 상세한 분석을 진행 중에 있으며, 추가적으로 확인 된 정보들에 대해서는 본 블로그를 통해 지속적으로 업데이트 할 예정이다.