FireEye
Next Generation Threat Protection

FireEye Analysis Report

(6. 25 Cyber Attack)

Table of Contents

1 Summary

1) 개요

- 2013 년 6 월 25 일, 웹하드 파일을 변조하는 방법을 통해서, 악성코드를 다량으로 유포함.
- 유포된 악성코드를 통해서, 좀비 PC 를 생성하고, 대규모 Botnet 을 구성.
- 지정된 시간에 DDoS 공격을 수행하도록 동작함.

2) 특징

- VM 회피, Anti 디버깅등의 기능이 들어 있는, themida 패킹 프로그램을 사용해서, 분석 및 탐지를 어렵게 함.
- 동작에 관련된 대부분 파일에 대해서, themida 패킹프로그램을 적용.
- 사후 추적을 회피하기 위해서, 오픈소스 기반의 Tor 프로그램을 사용.
- TOR 를 이용해서, Proxy 와 같은 경유지 서버를 사용.

3) 위험도

- Anti-VM, Anti-Debugging 기능을 갖추고 있는, themida 패킹 프로그램을 사용하기 때문에, 현재 **APT 솔루션이라고 분류되는 대다수의 장비에서도 탐지가 불가능할것으로 추정됨**.
- Unknown 악성코드의 형태를 띄고 있으므로, **기존 백신으로는 탐지 불가**.

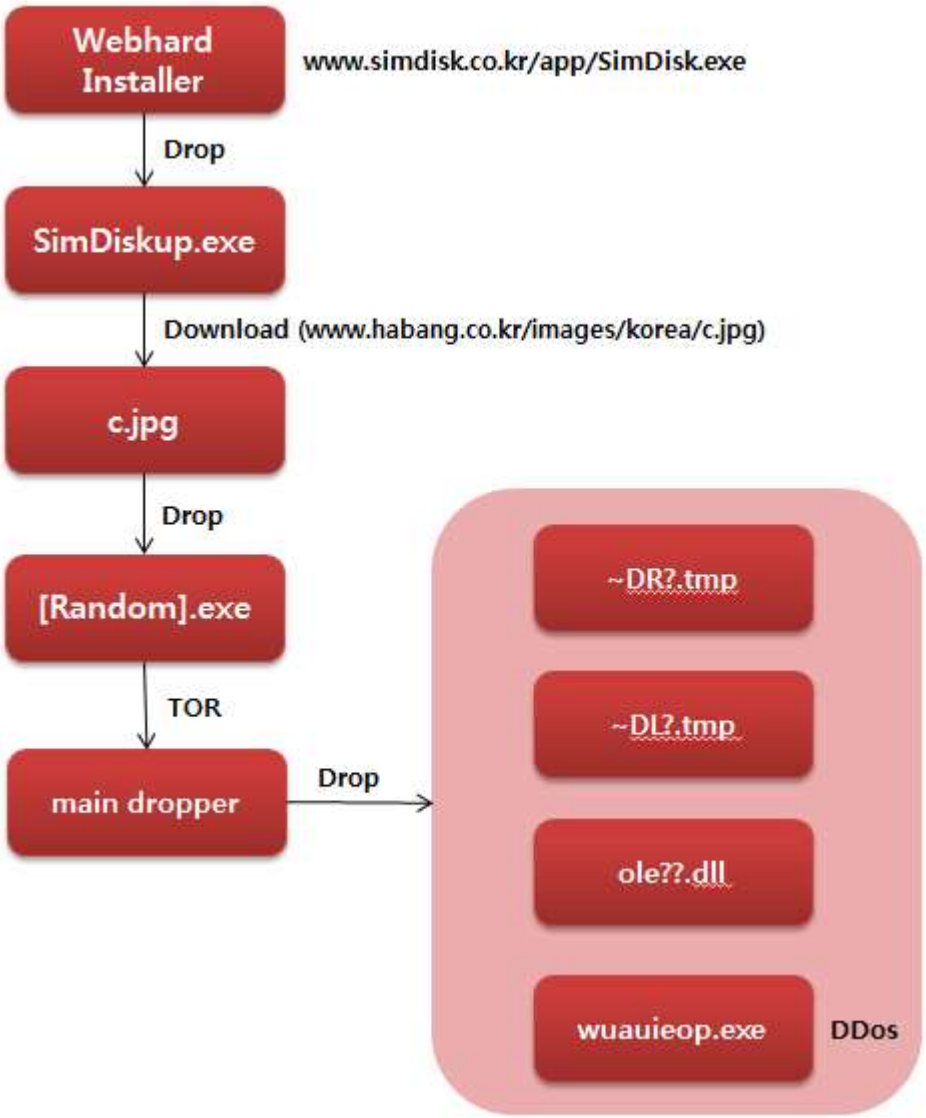
Scan Details	Vendor	
2013-06-25 02:21:32 UTC	Agnitum	Suspicious!SA
	AntiVir	TR/Dropper.Gen
	CAT-QuickHeal	(Suspicious) - DNAScan
	ESET-NOD32	a variant of Win32/Packed.Themida
	F-Secure	Gen:Trojan.Heur2.GZ.6yWabWwJ19f
	Panda	Suspicious file
	VIPRE	Backdoor.Win32.Ircbot.gen (v)

<VirusTotal 탐지결과 히스토리 조회 결과>

- VirusTotal 의 결과 값을 보면, 사고 발생 후, 한국시간 11:21:00 경에 어떤 국내 백신에서도 해당 파일을 탐지하지 못하는 것을 확인 가능.

2 Infection Diagram

최초 특정 웹하드 설치 파일이 사용자 PC 로 다운로드 및 실행되어 감염되게 되며 최종적으로 DDoS 트래픽을 유발하는 악성코드에 감염되게 된다.



3 Malware Information

➢ SimDiskup.exe

변조된 웹하드 설치 프로그램에 의해 생성되는 악의적인 목적의 파일

- 파일 생성일 : 2013 년 6 월 24 일 20:04:46

Machine	IMAGE_FILE_MACHINE_I386
Number of Sections	
Time Date Stamp	2013/06/24 11:04:46 UTC
Pointer to Symbol Table	

- Infection Procedure
  - 특정 서버에 접속하여 추가 악성코드 다운로드 시도

Network	Dns Query	*Protocol Type:* udp *Qtype:* Host Address *Hostname:* www.habang.co.kr *Imagepath:* C:\SimDiskup.exe
API Call		*API Name:* WaitForMultipleObjectsEx *Address:* 0x77df9b26 *Params:* [2, 0x2c9ff6c, 0, 300000, 1] *Imagepath:* C:\SimDiskup.exe *DLL Name:* kernel32.dll
Network	Dns Query Answer	*IP Address:* 199.16.199.2 *Hostname:* www.habang.co.kr *Imagepath:* C:\SimDiskup.exe
Network	Connect	*Protocol Type:* tcp *Destination Port:* 80 *IP Address:* 199.16.199.2 *Imagepath:* C:\SimDiskup.exe
Malicious Alert	Misc Anomaly	*Message:* Network outbound communication attempted *Detail:* Process attempting connections via standard ports

<파이어아이 MPS 장비 실제 탐지 내역>

➢ c.jpg

다운로드된 c.jpg 파일은 시스템 파일명으로 위장한 추가적인 파일을 생성하며 가상 터널 네트워크를 구성하는 Tor 를 이용하여 추가 접속을 시도

- 파일 생성일 : 2013 년 6 월 24 일 20:33:44

Machine	IMAGE_FILE_MACHINE_I386
Number of Sections	
Time Date Stamp	2013/06/24 11:33:44 UTC
Pointer to Symbol Table	

- Infection Procedure
  - 악성코드 생성을 위한 폴더 생성

Folder	Created	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}
Folder	Hide	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}
Malicious Alert	Misc Anomaly	*Message:* File/folder hiding *Detail:* Process hiding file/folder

<파이어아이 MPS 장비 실제 탐지 내역>

  - 추가 파일 생성(svchost.exe)

File	Created	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\svchost.exe
Malicious Alert	Misc Anomaly	*Message:* Well-known EXE/DLL created/modified in non-protected location *Detail:* Process creating/modifying well-known EXE/DLL in non-protected location

<파이어아이 MPS 장비 실제 탐지 내역>

- 추가 파일 생성(thttp.exe) 후 파일 생성 시간 및 파일명 변경(explorer.exe)

File	Created	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\t http.exe
File	Date Change	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\t http.exe
API Call		*API Name:* Sleep *Address:* 0x00658eff *Params:* [100] *Imagepath:* C:\exec\c.exe *DLL Name:* kernel32.dll
API Call		*API Name:* Process32First *Address:* 0x00657a87 *Params:* [0x140, 0x12f2a8] *Imagepath:* C:\exec\c.exe *DLL Name:* kernel32.dll
API Call		*API Name:* Sleep *Address:* 0x0040144f *Params:* [349] *Imagepath:* C:\exec\c.exe *DLL Name:* kernel32.dll
API Call		*API Name:* Process32First *Address:* 0x00657d54 *Params:* [0x140, 0x12f2a8] *Imagepath:* C:\exec\c.exe *DLL Name:* kernel32.dll
File	Rename	*Old Name:* C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\t http.exe *New Name:* C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\e xplorer.exe *Imagepath:* C:\exec\c.exe

<파이어아이 MPS 장비 실제 탐지 내역>

- 설정 파일(config.ini) 생성

File	Created	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\c onfig.ini
File	Open	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\c onfig.ini

<파이어아이 MPS 장비 실제 탐지 내역>

- 추가 생성한 파일(svchost.exe) 실행

Process	Started	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\s vchost.exe *Parentname:* C:\exec\c.exe *Command Line:* "C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\svchost.exe" MD5: d39201291338215f7405e9a719e431ad SHA1: 800996908c06236e583948aabde9f4655bd77777

<파이어아이 MPS 장비 실제 탐지 내역>

- 자기 자신 삭제를 위한 배치 파일 생성 및 실행

File	Created	C:\Documents and Settings\admin\Local Settings\Temp\~E8536.bat
File	Close	C:\Documents and Settings\admin\Local Settings\Temp\~E8536.bat MD5: ef32314fc012e4516c489f5a9682698a SHA1: 0e02bae3c41d8926c77c1b4b2a8bbcff165927be
Process	Started	C:\WINDOWS\system32\cmd.exe *Parentname:* C:\exec\c.exe *Command Line:* cmd /c C:\DOCUME~1\admin\LOCALS~1\Temp\~E8536.bat MD5: eeb024f2c81f0d55936fb825d21a91d6 SHA1: dd47ff16176412ec2e170cda441b4a220ff52f46
Malicious Alert	Misc Anomaly	*Message:* New command prompt started *Detail:* Process starting command prompt

<파이어아이 MPS 장비 실제 탐지 내역>

- 자동 실행을 위한 레지스트리 등록

Regkey	Setval	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"svchost" = "C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\svchost.exe"
Malicious Alert	Misc Anomaly	*Message*: Startup services added *Detail*: Process adding itself (non-DLL) to windows startup areas

<파이어아이 MPS 장비 실제 탐지 내역>

- 추가 생성된 파일(explorer.exe)을 실행하며 옵션으로 통신을 위한 포트 지정(-SOCKSPort 17027)

Process	Started	C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\explorer.exe *Parentname*: C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\svchost.exe *Command Line*: "C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\\explorer.exe" -SOCKSPort 17027 MD5: 506b0b49821637 1d64abb69145b70e4c SHA1: 71da7037f29bf8afe78d2a504350cdaf7cc6c9da

<파이어아이 MPS 장비 실제 탐지 내역>

- 특정 포트 오픈 후 수신 대기

Network	Listen	*Protocol Type*: tcp *Listen Port*: 1039 *IP Address*: 127.0.0.1 *Imagepath*: C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\explorer.exe
Malicious Alert	Misc Anomaly	*Message*: Network port opened to allow loopback connections *Detail*: Listening on a localhost port
Network	Connected	*Protocol Type*: tcp *Destination Port*: 1039 *IP Address*: 127.0.0.1 *Imagepath*: C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\explorer.exe
Malicious Alert	Misc Anomaly	*Message*: Loopback communication attempted *Detail*: Process attempting connections to loopback interface
Network	Listen	*Protocol Type*: tcp *Listen Port*: 17027 *IP Address*: *Imagepath*: C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\explorer.exe

<파이어아이 MPS 장비 실제 탐지 내역>

- Tor 통신을 위한 설정 파일 생성

Folder	Created	C:\Documents and Settings\admin\Application Data\tor
File	Created	C:\Documents and Settings\admin\Application Data\tor\lock
File	Created	C:\Documents and Settings\admin\Application Data\tor\state.tmp
File	Close	C:\Documents and Settings\admin\Application Data\tor\state.tmp MD5: ad8a55f62fec3a18d73c67523c00aa78 SHA1: 3683b83cea995714839444 1ae055d36229e01ff8

<파이어아이 MPS 장비 실제 탐지 내역>

- 네트워크 통신 수행

Network	Connect	*Protocol Type*: tcp *Destination Port*: 9090 *IP Address*: 76.73.17.194 *Imagepath*: C:\Documents and Settings\admin\Application Data\Identities\{8d70b240-31aa-11e1-9034-806d6172696f}\explorer.exe
Malicious Alert	Misc Anomaly	*Message*: Network outbound communication attempted *Detail*: Process attempting connections via odd ports

<파이어아이 MPS 장비 실제 탐지 내역>

➢ **Main Dropper**

실제로 PC 를 DDoS Bot 으로 만들기 위해 감염을 수행하는 Main Dropper

- 파일 생성일 : 2013 년 6 월 25 일 06:36:31

Machine	IMAGE_FILE_MACHINE_I386
Number of Sections	
Time Date Stamp	2013/06/24 21:36:31 UTC
Pointer to Symbol Table	

- Infection Procedure

- 추가 악성코드(~DR4.tmp) 생성 및 로드

File	Created	C:\Documents and Settings\admin\Local Settings\Temp\~DR4.tmp
Uac	Audit policy change	
File	Overwritten	C:\Documents and Settings\admin\Local Settings\Temp\~DR4.tmp
Uac	Service	Telephony
File	Close	C:\Documents and Settings\admin\Local Settings\Temp\~DR4.tmp MD5: 0ff67e022fa9ce7056316ceff82a80a8 SHA1: cd55c86f0c9ca8d5af84256a2e5911a54c8afb8b
DLL Loaded		*Imagepath*: C:\d97aef01ac94d2c7654033caa707a59f.exe *DLL Path*: C:\Documents and Settings\admin\Local Settings\Temp\~DR4.tmp MD5: 0ff67e022fa9ce7056316ceff82a80a8 SHA1: cd55c86f0c9ca8d5af84256a2e5911a54c8afb8b
Malicious Alert	Misc Anomaly	*Message*: Suspicious DLL loaded via newly created file *Detail*: Process loading suspicious DLL via newly created file

<파이어아이 MPS 장비 실제 탐지 내역>

- 로드된 악성코드(~DR4.tmp)에 의해서 추가 악성코드(~DL5.tmp) 생성

File	Created	C:\Documents and Settings\admin\Local Settings\Temp\~DL5.tmp
File	Overwritten	C:\Documents and Settings\admin\Local Settings\Temp\~DL5.tmp

<파이어아이 MPS 장비 실제 탐지 내역>

- 시스템 폴더에 추가 악성코드(ole[서비스명].dll) 생성

File	Created	C:\WINDOWS\system32\olerasauto.dll
Malicious Alert	Misc Anomaly	*Message*: System services modified *Detail*: EXE/DLL/SYS/OCX/VXD files created/renamed under WINDOWS or SYSTEM32 directories
API Call		*API Name*: GetSystemDirectoryA *Address*: 0x10001d5e *Params*: [0x12e718, 259] *Imagepath*: C:\d97aef01ac94d2c7654033caa707a59f.exe *DLL Name*: kernel32.dll
File	Date Change	C:\WINDOWS\system32\olerasauto.dll
File	Open	C:\WINDOWS\system32\olerasauto.dll

<파이어아이 MPS 장비 실제 탐지 내역>

- 추가 생성된 악성코드 자동 실행을 위해 윈도우 정상 서비스의 파라미터 교체

Regkey	Setval	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\RasAutoSvc\"Type" = 0x00000020
Malicious Alert	Misc Anomaly	*Message*: System services tampered *Detail*: Process modifying system services
Regkey	Added	\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\RasAutoSvc\Parameters
API Call		*API Name*: Sleep *Address*: 0x10001ff7 *Params*: [1000] *Imagepath*: C:\d97aef01ac94d2c7654033caa707a59f.exe *DLL Name*: kernel32.dll
Regkey	Added	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\RasAutoSvc\Parameters
Regkey	Setval	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\RasAutoSvc\Parameters\"ServiceDll" = %SystemRoot%\System32\olerasauto.dll

<파이어아이 MPS 장비 실제 탐지 내역>

- 정상 윈도우 서비스로 악성코드 실행

DLL Loaded		*Imagepath*: C:\WINDOWS\system32\svchost.exe *DLL Path*: C:\WINDOWS\system32\olerasauto.dll MD5: 13b4617013f22f9eba25be0b6ab2a7a8 SHA1: 0fd75f6863b4cf4f4d15c96b9ae4b2f2e533c3c1

<파이어아이 MPS 장비 실제 탐지 내역>

- C&C 서버 접속

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

www.hostmypic.net/pictures/e02947e8573918c1d887e04e2e0b1570.jpg

Network	Dns Query	*Protocol Type*: udp *Qtype*: Host Address *Hostname*: webmail.genesyshost.com *Imagepath*: C:\WINDOWS\system32\svchost.exe
Network	Dns Query Answer	*IP Address*: 199.16.199.3 *Hostname*: webmail.genesyshost.com *Imagepath*: C:\WINDOWS\system32\svchost.exe
Network	Connect	*Protocol Type*: tcp *Destination Port*: 80 *IP Address*: 199.16.199.3 *Imagepath*: C:\WINDOWS\system32\svchost.exe
Malicious Alert	Misc Anomaly	*Message*: Network outbound communication attempted *Detail*: Process attempting connections via standard ports

<파이어아이 MPS 장비 실제 탐지 내역>

➢ **DDos Bot(wuauieop.exe)**

C&C 서버의 명령에 따라 실제 DDoS 트래픽을 유발하는 악성코드

- 파일 생성 시간 : 2013 년 6 월 24 일 18:45:38 UTC

Machine	IMAGE_FILE_MACHINE_I386
Number of Sections	
Time Date Stamp	2013/06/24 09:45:38 UTC
Pointer to Symbol Table	

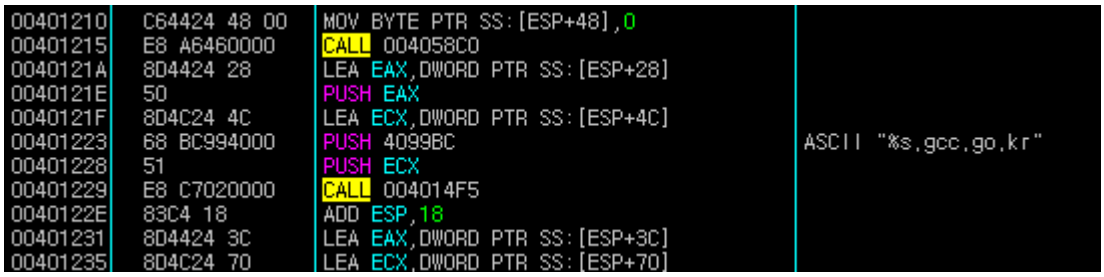
- 악성코드 기능

wuauieop.exe 악성코드의 경우 특정 조건 만족시 아래와 같이 [랜덤].gcc.go.kr 를 대상으로 대규모의 DNS Query 를 발생한다.

Source	Destination	Protocol	Info
192.168.126.128	152.99.200.6	DNS	Standard query ANY pwcqcomaj.gcc.go.kr
192.168.126.128	152.99.1.10	DNS	Standard query ANY hthr.gcc.go.kr
192.168.126.128	152.99.1.10	DNS	Standard query ANY egdxdwkj.gcc.go.kr
192.168.126.128	152.99.1.10	DNS	Standard query ANY ol.gcc.go.kr
192.168.126.128	152.99.1.10	DNS	Standard query ANY r.gcc.go.kr
192.168.126.128	152.99.1.10	DNS	Standard query ANY b.gcc.go.kr
192.168.126.128	152.99.200.6	DNS	Standard query ANY ubcmp.gcc.go.kr
192.168.126.128	152.99.200.6	DNS	Standard query ANY atyuqzh.gcc.go.kr
192.168.126.128	152.99.200.6	DNS	Standard query ANY dyzfe.gcc.go.kr
192.168.126.128	152.99.200.6	DNS	Standard query ANY nl.gcc.go.kr
192.168.126.128	152.99.200.6	DNS	Standard query ANY ue.gcc.go.kr
192.168.126.128	152.99.1.10	DNS	Standard query ANY nbtp.gcc.go.kr
192.168.126.128	152.99.1.10	DNS	Standard query ANY xgu.gcc.go.kr

<파이어아이 MPS 장비 실제 탐지 내역>

- DDoS 공격 관련 루틴


00401210 C64424 48 00 MOV BYTE PTR SS:[ESP+48],0
00401215 E8 A6460000 CALL 004058C0
0040121A 8D4424 28 LEA EAX,DWORD PTR SS:[ESP+28]
0040121E 50 PUSH EAX
0040121F 8D4C24 4C LEA ECX,DWORD PTR SS:[ESP+4C]
00401223 68 BC994000 PUSH 4099BC ASCII "%s,gcc,go,kr"
00401228 51 PUSH ECX
00401229 E8 C7020000 CALL 004014F5
0040122E 83C4 18 ADD ESP,18
00401231 8D4424 3C LEA EAX,DWORD PTR SS:[ESP+3C]
00401235 8D4C24 70 LEA ECX,DWORD PTR SS:[ESP+70]