GhOst RAT 원격제어 악성코드 유포

2014. 5

KISA 한국인터넷진흥원 Korea Internet & Security Agency

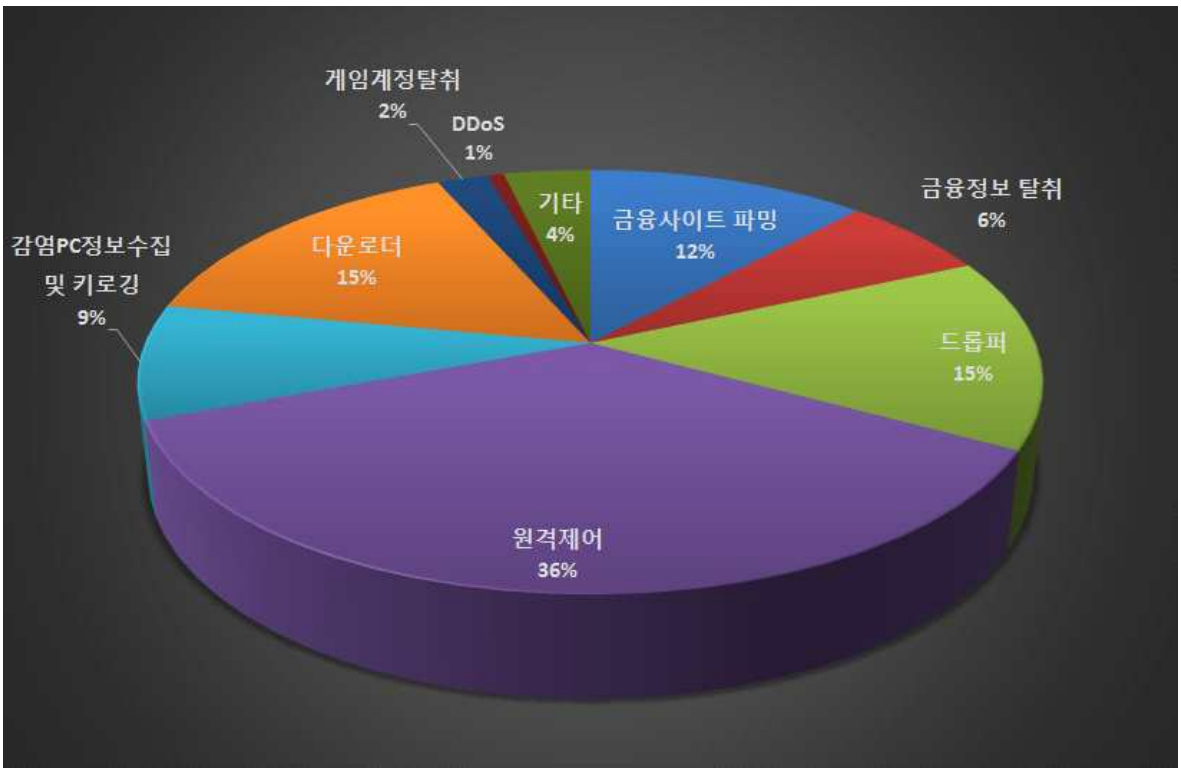
KrCERT/CC 인터넷 침해 대응 센터

[목 차]

1. Gh0st RAT 악성코드 유포

□ 악성코드 유포 현황

'13년 2월부터 '14년 2월까지 악성코드 은닉사이트에서 유포된 악성코드 현황은 총 731건으로 집계되었으며, 수집된 악성코드 종류로는 원격제어, 드롭퍼, 다운로더, 파밍, 감염PC정보수집, 금융정보 탈취 순으로 확인되었다. 그 중에서 가장 많이 수집된 악성코드는 원격제어 악성코드인데, 전체 731개중 265개(약36%)로 집계되었다.

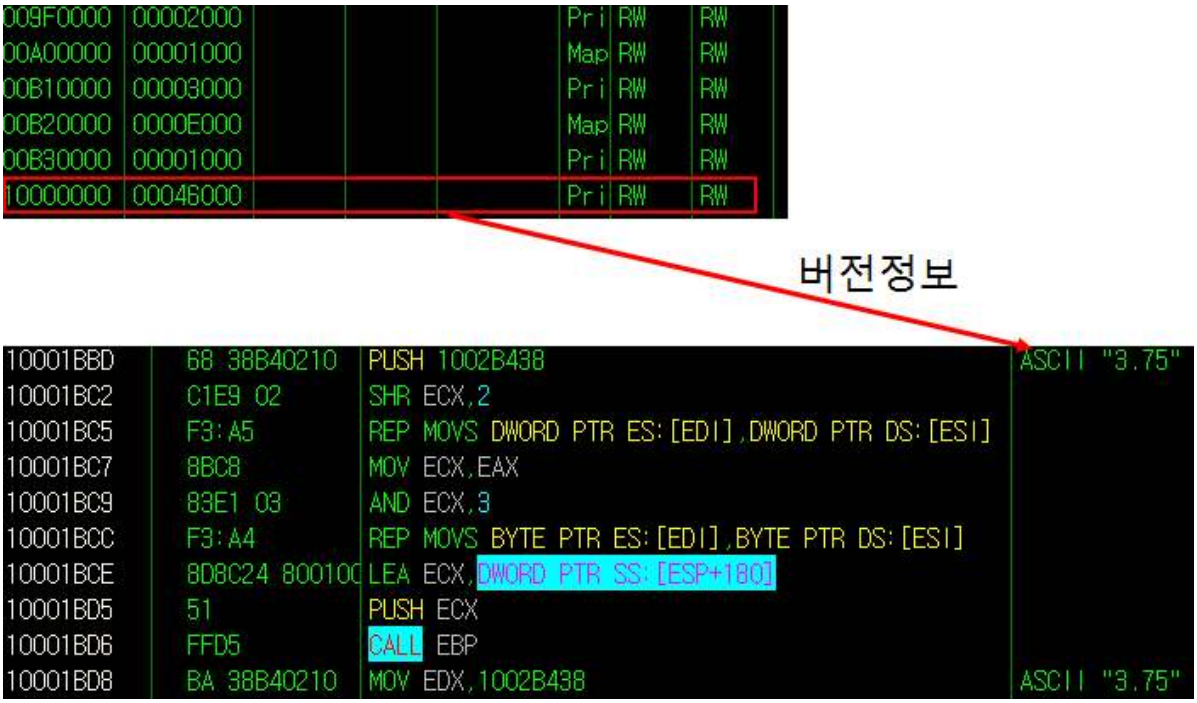


[그림 1] 1년간 악성코드 은닉사이트에서 유포된 악성코드 분포

전체 원격제어 악성코드를 주요 기능 및 파일 유사성 등을 기준으로 분석한 결과 URL을 제외하고 파일의 구조 및 기능이 모두 동일한 악성코드가 265개중 195개(74%)로 확인되었다. 이들 악성코드의 특징으로 악성코드가 실행될 경우 0x10000000 메모리 영역에 악성행위에 필요한 기능모듈을 로드한 뒤 공격자

의 명령에 따라 행위를 수행할 수 있도록 설계되어 있다.

또한 ASCII값으로 된 '3.75'라는 숫자가 악성코드에 삽입되어 있는데 이는 해당 프로그램의 버전을 명시하는 부분으로 파악되며, 구성 및 기능들을 종합해볼 때 195개의 악성코드들은 2013년에 유행한 'Gh0st RAT(Remote Access Trojan)'이라는 해킹도구에 의해 생성된 원격제어 악성코드로 추정된다.



[그림 2] 0x10000000 메모리 영역 Gh0st RAT 버전정보

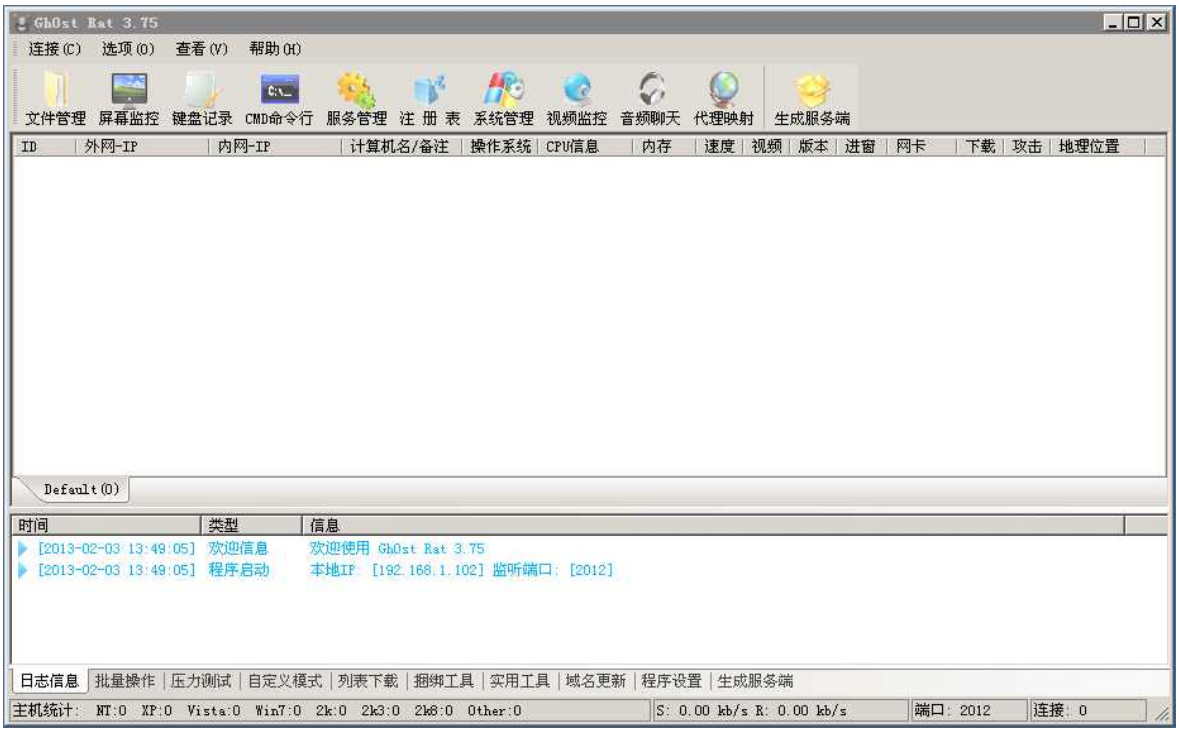
2. 'Gh0st RAT(Remote Access Trojan)'이란?

□ 원격제어 프로그램 'Gh0st RAT'

'Gh0st RAT(Remote Access Trojan)'은 감염에 필요한 악성코드를 생성하고 좀비화된 감염PC들의 관리와 공격명령을 통한 악성행위를 수행할 수 있는 해킹도구이다. 이 프로그램을 이용하여 해커는 자신의 서버로 접속한 좀비PC들에게 간단한 조작으로 DDoS공격, 화면제어, 키로깅, 도청 등 여러형태의 악성행위를

손쉽게 수행할 있다.

원격제어 프로그램 'Gh0st RAT'은 소스코드가 인터넷상에 공개[1]되어 있어 꾸준하게 버전업이 진행되고 있으며, 조작법 또한 간단하여 저수준의 해커들도 쉽게 사용할 수 있는 장점도 있다.



[그림 3] Gh0st RAT의 좀비PC 관리 화면

3. Gh0st RAT 원격제어 악성코드 주요기능 소개

'Gh0st RAT' 해킹도구를 통해 생성된 악성코드의 주요기능은 다음과 같다.

	기능	설명
1	스케줄러 및 레지스트리 등록	파일이 실행이 되면 'C:₩WINDOWS₩[임의8자리]' 경로에 'svchsot.exe'를 생성하고(자기복제), 'C:₩WINDOWS₩Tasks'경로에 At1~24까지 24개의 스케줄러 파일을 생성, 'svchsot.exe'를 1시간 간격으로 매일 자동실행 하도록 설정됨

1) 2013년에 2.x 버전의 소스코드가 공개되었음.

		또한 'HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RUN' 경로에 'svchsot.exe'파일이 부팅시 자동실행 될 수 있도록 레지스트리를 추가함
2	Anti-Virus 종료	Taskkill명령이나 TerminateProcess()를 이용하여 Anti-Virus프로그램들을 종료함
3	Guest계정 활성화 및 관리자 그룹 등록	CMD 명령을 이용하여 윈도우 운영체제에 기본적으로 접근하는 Guest계정을 관리자 그룹으로 추가 및 활성화를 통해 감염PC로 접근하기가 쉽도록 설정함
4	화면 및 키보드&마우스를 제어	감염된 PC를 공격자가 원격으로 화면 및 키보드&마우스를 원격지에서 조정함
5	음성정보를 녹음	감염된 PC에 설치된 마이크를 통해 음성정보를 기록하여 공격자에게 전달함
6	키로그 저장기능	감염된 PC에 조작되는 키보드 이벤트를 기록하여 [임의8자리].key로 저장한 후 공격자에게 전달함
7	DDoS공격 기능	공격자가 지정한 URL로 TCP,UDP, ICMP, SYN등의 DDoS 공격을 수행함
8	추가 다운로드기능	공격자는 추가로 악성행위에 필요한 악성코드를 다운로드 시킬수 있음
9	모뎀정보 확인	감염PC에 모뎀이 설정된 경우 운영체제에 저장된 전화모뎀 설정파일에 접근하여 전화번호 등의 사용자 정보를 획득함
10	웹캠 작동	감염PC에 장착된 웹캠이 있을 경우 사용자 동의 없이 웹캠을 작동하여 카메라 화면을 캡쳐함

4. 대응방안

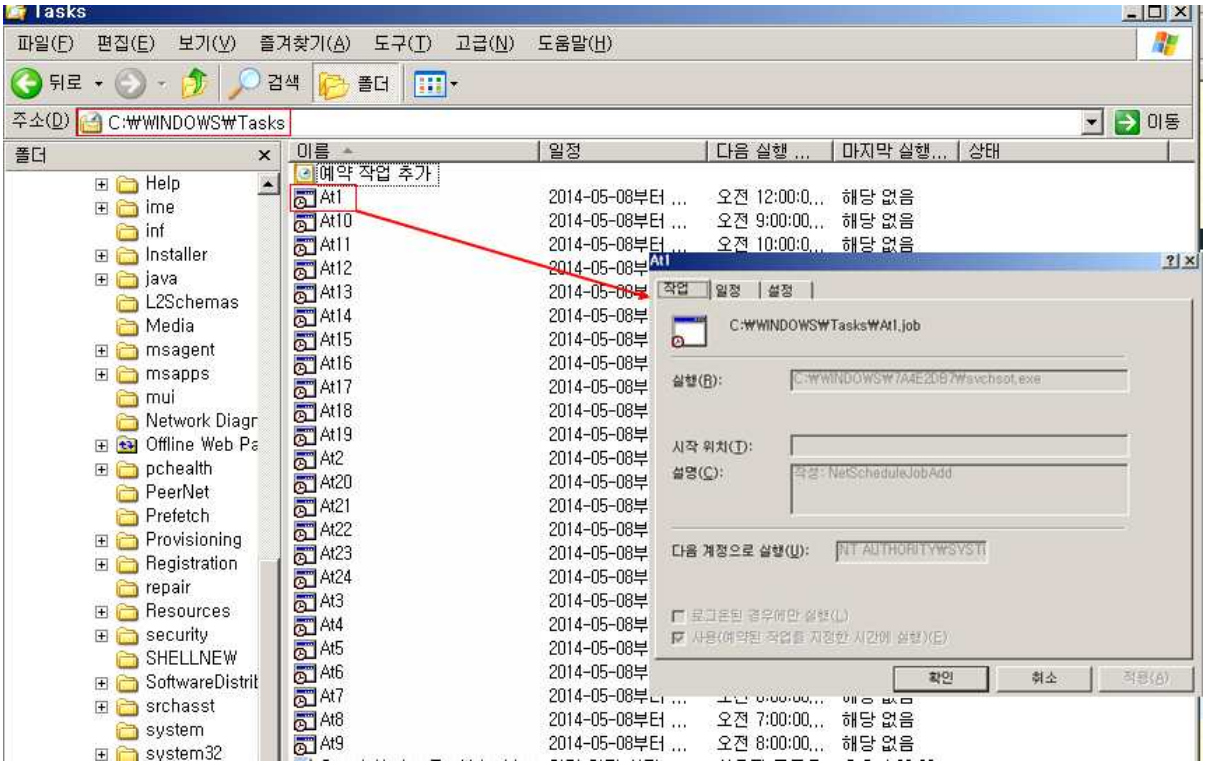
최근 'Gh0st RAT' 악성코드는 감염PC의 웹캠을 원격으로 제어하여 사생활을 침해하고, 키로깅 기능을 이용해 계정정보를 획득하거나 공인인증서와 같은 인터넷뱅킹 정보를 노리는 공격에 활용되고 있으며, 대규모로 구성된 좀비PC를

이용해 DDoS 및 APT공격으로 악용할 우려가 있기 때문에 피해를 방지하기 위해서는 감염여부를 확인하여 악성코드를 삭제하는 조치가 필요하다.

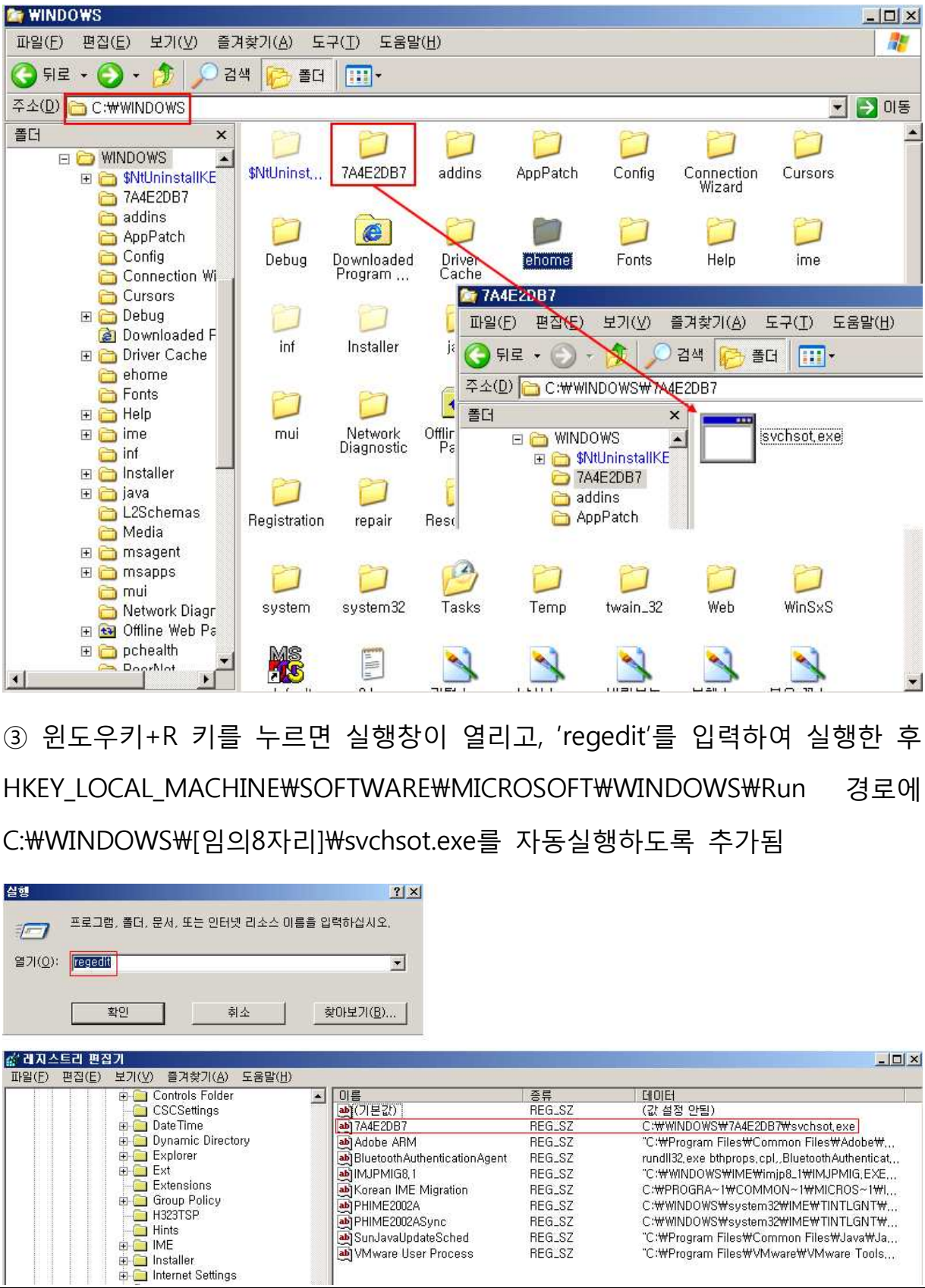
1차적으로 백신프로그램의 패턴을 최신으로 업그레이드한 후 파일검사를 통해 악성코드 감염 확인 및 치료 조치하고, 백신에서 탐지되지 않은 변종 악성코드의 경우 아래와 같이 확인할 수 있다.

'Gh0st RAT' 악성코드가 실행되면 다음과 같은 행위를 수행함

① C:₩WINDOWS₩Tasks 폴더에 At1~At24.job 스케줄러 파일을 생성함

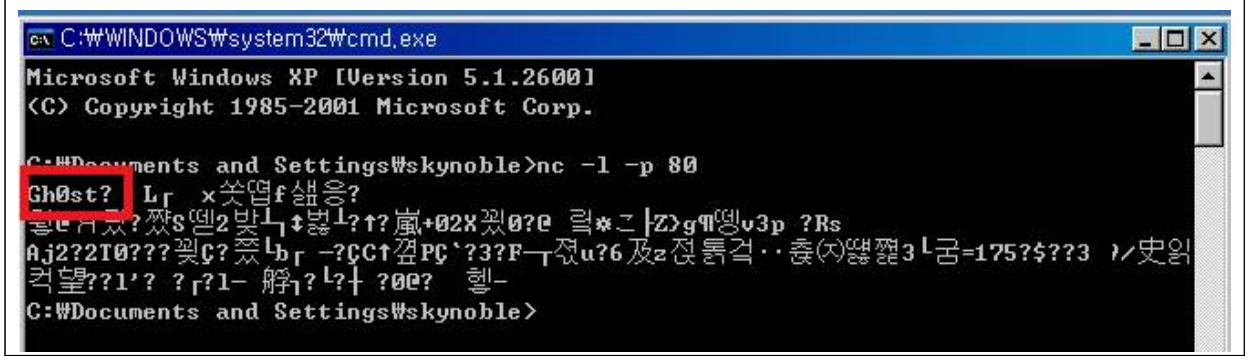


② C:₩WINDOWS₩[임의8자리] 폴더에 svchsot.exe(복사된 악성코드)파일이 저장됨



③ 윈도우키+R 키를 누르면 실행창이 열리고, 'regedit'를 입력하여 실행한 후 HKEY_LOCAL_MACHINE₩SOFTWARE₩MICROSOFT₩WINDOWS₩Run 경로에 C:₩WINDOWS₩[임의8자리]₩svchsot.exe를 자동실행하도록 추가됨

④ C&C에 접속하는 패킷의 내용 중 'Gh0st'라는 String값이 포함됨



< 'Gh0st RAT' 악성코드 설치 확인>

감염이 확인되면 해당 경로에 생성된 스케줄러 파일과 레지스트리를 삭제하여 자동실행이 되지 않도록 조치한 후 C:₩WINDOWS₩[임의8자리]폴더에 저장된 svchsot.exe파일을 삭제하면 악성코드 조치가 완료된다.