월간 악성코드 분석 보고서 (2018-09)

“갠드크랩 5.0”

수산INT 기술 연구소 (CERT)

2018. 10. 01

본 문서는 국내를 대상으로 노리는 유포되는 랜섬웨어 갠드크랩 5.0을 분석한 보고서 입니다.
본 문서는 수산아이앤티 CERT에서 작성되었으며 연구 목적의 활용은 가능하나, 그 외 활용으로 인해 발생하는 문제에 대한 법적 책임은 당사자에 있음을 알려드립니다.

문의처: 기술 연구소 CERT 파트 (KimNamGuy@soosan.co.kr) (aallss123@soosan.co.kr)

SOOSAN INT

목 차

1. 동적 분석 (갠드크랩 5.0)

수산INT CERT에서는 갠드크랩 5.0을 실제로 분석해 보았습니다. 분석 내용은 다음과 같습니다.

1.1 분석 파일 정보

분석 파일명은 "**[임의로 지정 된 파일명].exe**" 입니다.

해당 파일 해시 정보는 아래와 같습니다.

- MD5: 07FADB006486953439CE0092651FD7A6
- SHA-1: E42431D37561CC695DE03B85E8E99C9E31321742
- SHA-256: d77378dcc42b912e514d3bd4466cdda050dda9b57799a6c97f70e8489dd8c8d0

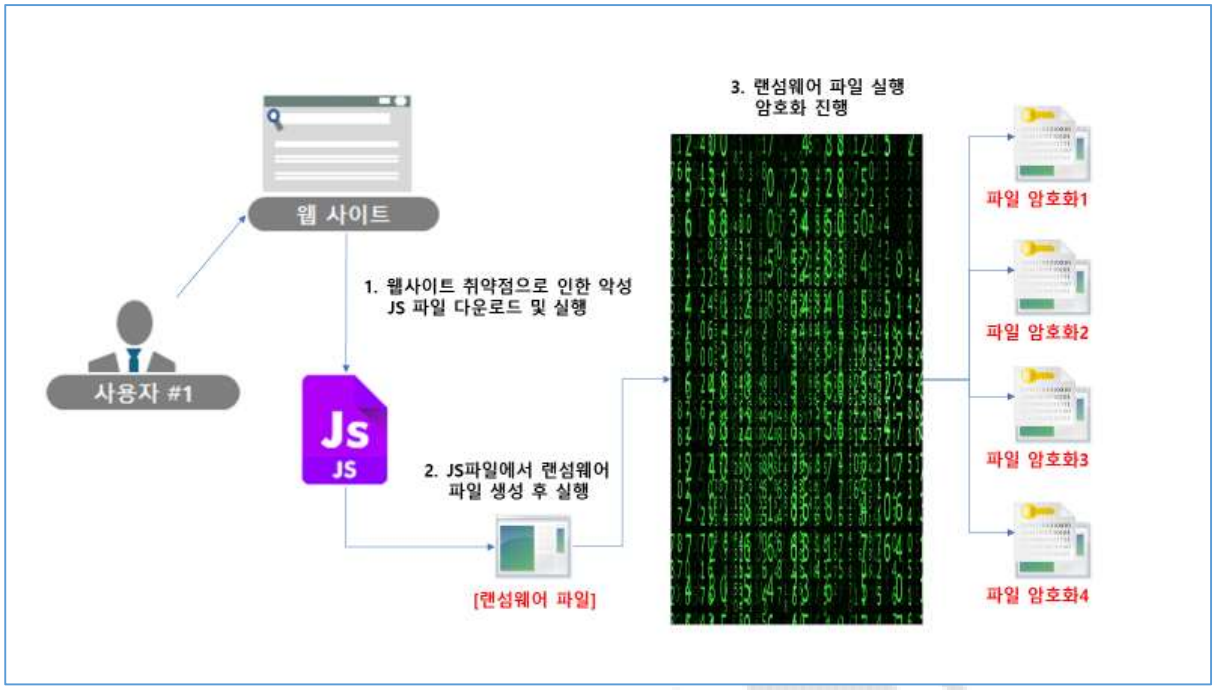
해당 악성 파일은 밑의 표와 같이 프로세스 및 파일 관련 정보

실행 차단 대상 프로세스
msftesql.exe sqlagent.exe sqlbrowser.exe sqlwriter.exe oracle.exe ocssd.exe dbsnmp.exe synctime.exe agntsvc.exe isqlplussvc.exe xfssvccon.exe sqlservr.exe mydesktopservice.exe ocautoupds.exe agntsvc.exe agntsvc.exe agntsvc.exe encsvc.exe firefoxconfig.exe tbirdconfig.exe mydesktopqos.exe ocomm.exe mysqld.exe mysqld-nt.exe mysqld-opt.exe dbeng50.exe sqbcoreservice.exe excel.exe infopath.exe msaccess.exe mspub.exe onenote.exe outlook.exe powerpnt.exe steam.exe thebat.exe thebat64.exe thunderbird.exe visio.exe winword.exe wordpad.exe
암호화 확장자
.1st .602 .docb .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .xps .xls .xlt ._doc .dotm ._docx .abw .act .adoc .aim .ans .apkg .apt .asc .asc .ascii .ase .aty .awp .awt .aww .bad .bbs .bdp .bdr .bean .bib .bib .bibtex .bml .bna .boc .brx .btd .bzabw .calca .charset .chart .chord .cnm .cod .crwl .cws .cyi .dca .dfti .dgs .diz .dne .dot .doc .docm .dotx .docx .docxml .docz .dox .dropbox .dsc .dvi .dwd .dx .dxb .dxp .eio .eit .emf .eml .emlx .emulecollection .epp .err .err .etf .etx .euc .fadein .template .faq .fbl .fcf .fdf .fdr .fds .fdt .fdx .fdxt .fft .fgs .flr .fodt .fountain .fpt .frt .fwd .fwdn .gmd .gpd .gpn .gsd .gthr .gv .hbk .hht .hs .hwp .hwp .hz .idx .iil .ipf .ipspot .jarvis .jis .jnp .joe .jp1 .jrtf .jtd .kes .klg .klg .knt .kon .k

wd .latex .lbt .lis .lnt .log .lp2 .lst .lst .ltr .ltx .lue .luf .lwp .lxfml .lyt .lyx .man .mbox .mcw .md5 .me .mell .mellel .min .mnt .msg .mw .mwd .mwp .nb .ndoc .nfo .ngloss .njx .note .notes .now .nwctxt .nwm .nwp .ocr .odif .odm .odo .odt .ofl .opeico .openbsd .ort .ott .p7s .pages .pages-tef .pdpcmd .pfx .pjt .plain .plantuml .pmo .prt .prt .psw .pu .pvj .pvm .pwd .pwdp .pwdpl .pwi .pwr .qdl .qpf .rad .readme .rft .ris .rpt .rst .rtd .rtf .rtfd .rtx .run .rvf .rzk .rzn .saf .safetext .sam .sam .save .scc .scm .scriv .scrivx .sct .scw .sdm .sdoc .sdw .se .session .sgm .sig .skcard .sla .sla .gz .smf .sms .ssa .story .strings .stw .sty .sublime-project .sublime-workspace .sxg .sxw .tab .tab .tdf .tdf .template .tex .text .textclipping .thp .tlb .tm .tmd .tmdx .tmv .tmvx .tpc .trelby .tvj .txt .u3i .unauth .unx .uof .uot .upd .utf8 .utxt .vct .vnt .vw .wbk .webdoc .wn .wp .wp4 .wp5 .wp6 .wp7 .wpa .wpd .wpd .wpd .wpl .wps .wps .wpt .wpt .wpw .wri .wsd .wtt .wtx .xbdoc .xbplate .xdl .xdl .xwp .xwp .xwp .xy .xy3 .xyp .xyw .zabw .zrtf .zw
암호화 확장자 제외
rar .zip .cab .arj .lzh .tar .7z .gzip .iso .z .7-zip .lzma .vmx .vmdk .vmem .vdi .vbox .ani .cab .cpl .cur .diagcab .diagpkg .dll .drv .lock .hlp .ldf .icl .icns .ico .ics .lnk .key .idx .mod .mpa .msc .msp .msstyles .msu .nomedia .ocx .prf .rom .rtp .scr .shs .spl .sys .theme .themepack .exe .bat .cmd .gandcrab .KRAB .CRAB .zerophage_i_like_your_pictures

[표-1] 악성파일 정보

1.2 실행 과정



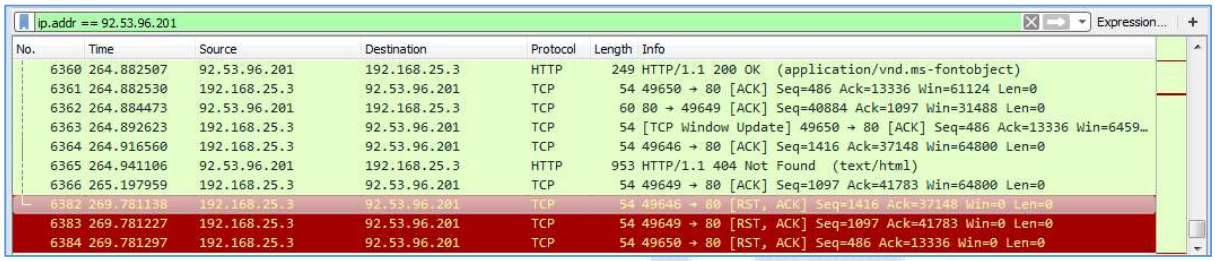
[그림-1] 실행 과정

1. 취약한 웹사이트 접속 시 사용자 컴퓨터에 악성 스크립트(Java Script)파일 다운 및 실행
2. 악성 스크립트(Java Script) 실행하여 C&C 통신 또는 악성 스크립트 안에 숨겨둔 실행 파일을 따로 생성하여 실행한다. 이러한 행위는 1차적으로 악성 파일을 탐지하는 안티바이러스들을 우회하기 위하여 많이 사용
3. 최종적으로 실행 된 "갠드크랩 5.0"은 암호화를 진행

- 해당 "갠드크랩 5.0"은 "갠드크랩 4.0" 기반의 소스에서 버전 수정 및 확장자 수정만 하였으며, 기존의 C&C 주소 또 한 기존 "갠드크랩 4.0"에서 변경되지 않고 "갠드크랩 5.0"으로 유포 되었음, 네트워크 트래픽 탐지 수리카타에서 C&C 탐지를 하게 되고, 레지스트리 정보 읽기는 하나 수정을 하여 부팅 시 자동 실행 행위는 하지 않는걸로 보임.

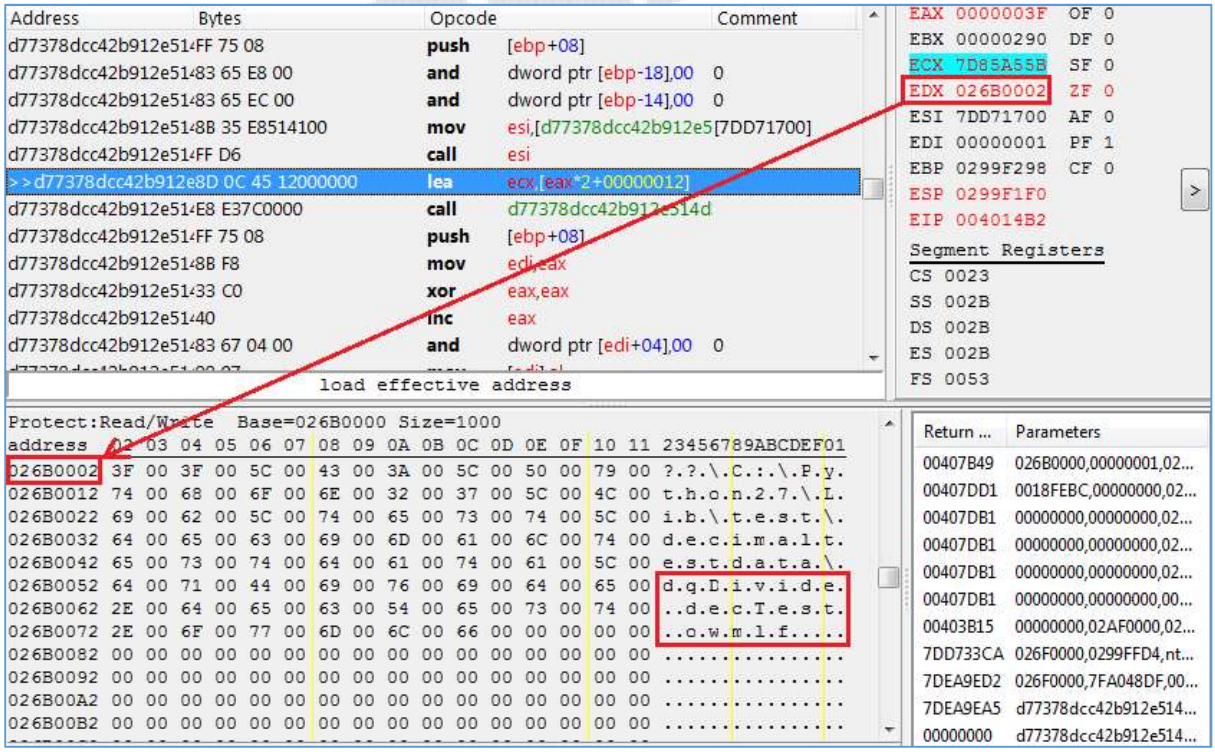
[그림-2] 수리카타 탐지

- 92.53.96.201 C&C 주소와 통신



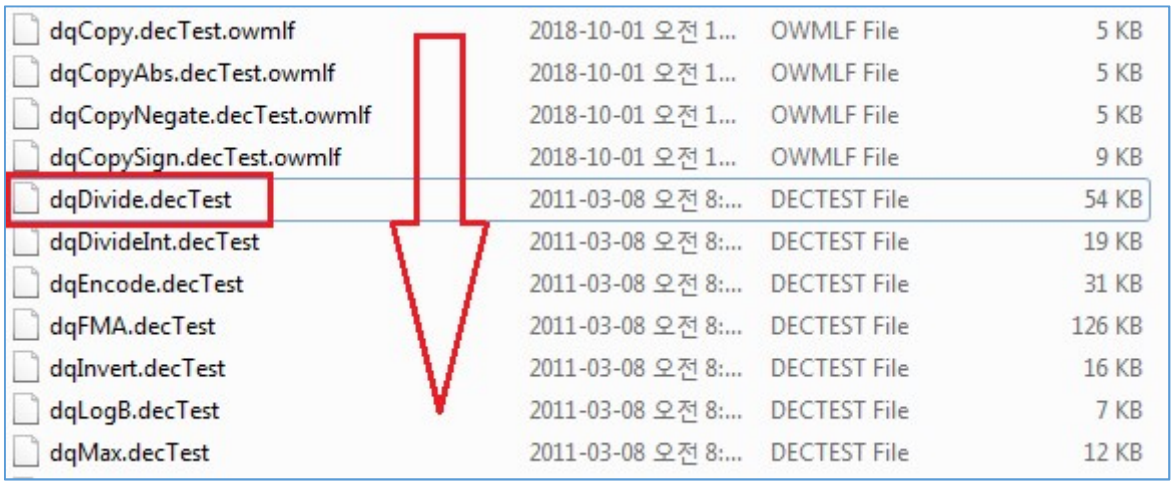
[그림-3] C&C 통신

- [그림-3]은 C:₩ 부터 해서 들어가 파일을 하나씩 암호화 시키는 과정



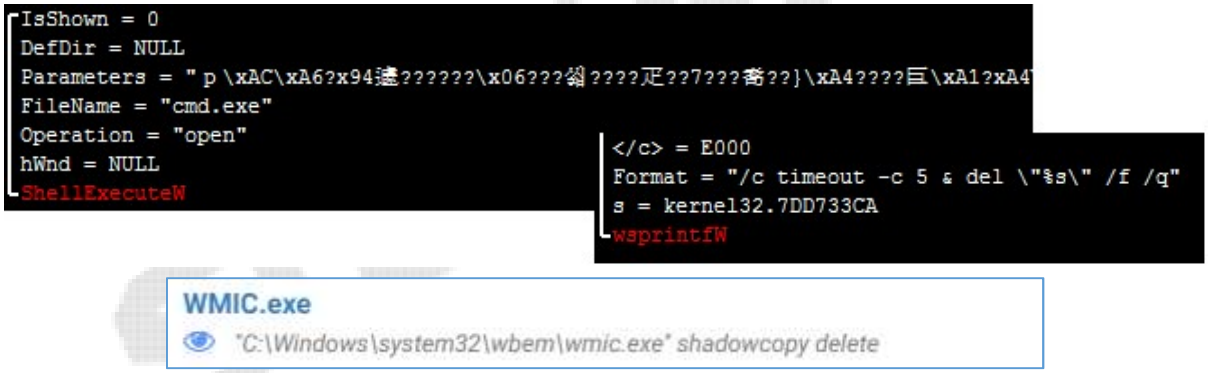
[그림-4] 암호화 진행

- 폴더에 접근하여 하위 파일들을 변경 하는 과정



[그림-5] 확장자 변경 진행

- WMIC를 이용하여 shadowcopy delete CMD 명령어를 실행 하여, 백업 파일들을 복구시키지 못하도록 함.



[그림-6] WMIC 명령어

- [그림-7]은 암호화 진행하는데 윈도우 시스템 중요 파일 및 랜섬웨어 암호화 된 파일은 중복 암호화를 하지 않기 위해서 제외리스트가 존재

```
004075A PUSH d77378dc.0041A084          UNICODE "desktop.ini"
004075B PUSH d77378dc.0041A09C          UNICODE "autorun.inf"
004075C PUSH d77378dc.0041A0B4          UNICODE "ntuser.dat"
004075C PUSH d77378dc.0041A0CC          UNICODE "iconcache.db"
004075D PUSH d77378dc.0041A0E8          UNICODE "bootsect.bak"
004075E PUSH d77378dc.0041A104          UNICODE "boot.ini"
004075F PUSH d77378dc.0041A118          UNICODE "ntuser.dat.log"
004075F PUSH d77378dc.0041A138          UNICODE "thumbs.db"
0040767 PUSH d77378dc.0041A14C          UNICODE "%s-DECRYPT.html"
004076A PUSH d77378dc.0041A16C          UNICODE "%s-DECRYPT.txt"
0040770 MOV EBX,d77378dc.0041A18C       UNICODE "KRAB-DECRYPT.html"
0040772 PUSH d77378dc.0041A1B0          UNICODE "KRAB-DECRYPT.txt"
0040773 PUSH d77378dc.0041A1D4          UNICODE "CRAB-DECRYPT.txt"
0040774 PUSH d77378dc.0041A1F8          UNICODE "ntldr"
0040775 PUSH d77378dc.0041A204          UNICODE "NTDETECT.COM"
0040776 PUSH d77378dc.0041A220          UNICODE "Bootfont.bin"
004077E PUSH d77378dc.0041A23C          UNICODE "%s "
004078C PUSH d77378dc.0041A23C          UNICODE "%s "
0040793 PUSH d77378dc.0041A244          UNICODE "%s\\%s-DECRYPT.html"
0040795 PUSH d77378dc.0041A26C          UNICODE "%s\\KRAB-DECRYPT.html"
00407A3 PUSH d77378dc.0041A298          UNICODE "%s.KRAB"
00407A3 PUSH d77378dc.0041A2A8          UNICODE "\\??\\%s.KRAB"
```

[그림-7] 암호화 제외 리스트

- 특정 안티바이러스 제품을 언급 하는 문자열도 보임

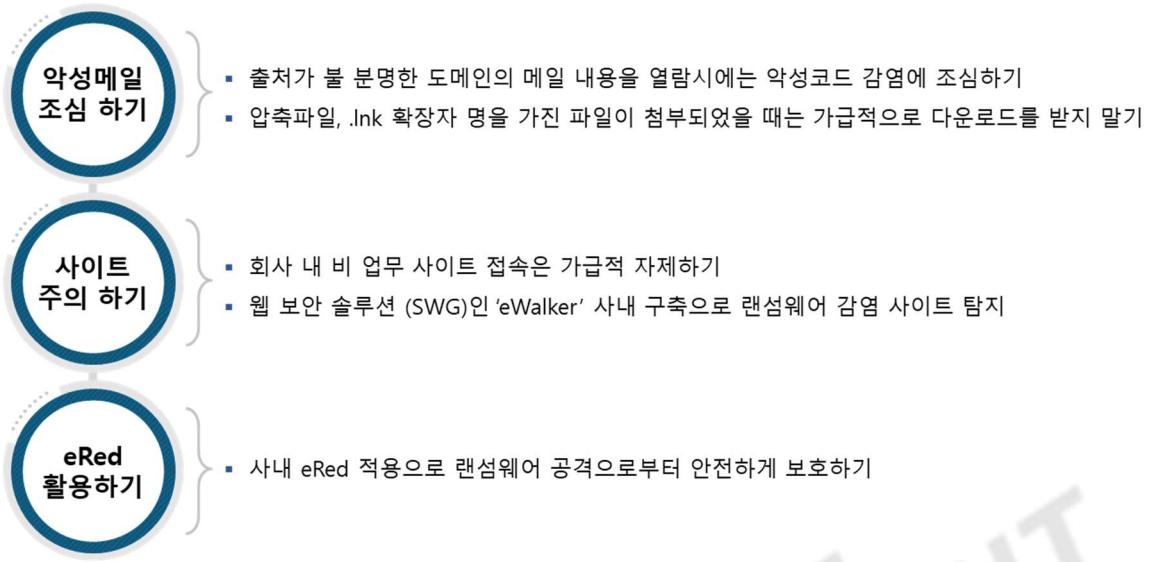
```
ASCII "hey ahnlab, score - 1:1. 0day exploit for Ahnlab V3 Lite Denial of service. Possibly can trigger

full write-what-where condition with privelege escalation, pass GandCrab http://filestorage.biz/download.php?file=e
```

[그림-8] 문자열

C&C (IP)	92.53.96.201

[표-2] 악성 파일 C&C IP

2. 대응방안



[그림 4-1] 갠드크랩 2.1 대응 방안

1. **악성메일 조심하기**

   출처가 불 분명한 메일은 가급적 열람하지 않는 것이 좋습니다. 그리고 압축파일 혹은 확장자가 .lnk인 경우에는 악성 파일로 의심해볼 필요가 있습니다.

2. **사이트 방문 주의 하기**

   웹 사이트 경로로 사용자를 감염 시키기도 합니다. 따라서 의심스러운 사이트 방문에 주의할 필요가 있습니다. 그러나 일반 사용자가 이를 판별하기란 쉽지 않습니다. 이러한 한계점을 eWalker 제품 구매로 극복할 수 있습니다. eWalker는 매일 **3만 개가 넘는 악성 사이트를 신규로 업데이트 하고 있어서**, 사용자가 악성 사이트에 접속하는 것을 원천적으로 차단합니다. 따라서 **eWalker 제품으로 갠드크랩 5.0 감염을 예방할 수 있습니다**.

3. **eRed 활용하기**

   eRed는 화이트 리스트 기반으로 허용되지 않은 프로세스 실행을 원천적으로 차단하는 보안 기술입니다. 그러므로 eRed는 랜섬웨어와 같은 악성 공격 프로세스를 원천적으로 차단합니다. 더욱이 eRed의 동작은 게스트 OS 하부의 하이퍼바이저 OS에 동작하기 때문에 차단 행위를 노리는 악성 공격에도 대응이 가능합니다. **실제로 갠드크랩 5.0을 eRed에 적용해 보았는데, 원천적으로 차단하는 것을 확인했습니다**.

2018 년 수산 INT 보안 연구 보고서 발간 내역

월간 악성코드 분석 보고서

2018-01 호: 가상화폐 채굴 악성코드 분석 (2018 년 01 월)
2018-02 호: UBoat Rat 분석 보고서 (2018 년 02 월)
2018-03 호: 평창올림픽 파괴 악성코드 분석 보고서 (2018 년 03 월)
2018-04 호: 웹으로 감염시키는 악성코드 '헤르메스' 분석 (2018 년 04 월)
2018-05 호: 국내 맞춤형 랜섬웨어 '갠드크랩' (2018 년 05 월)
2018-06 호: 서비스형 랜섬웨어 표본 '갠드크랩 3.0' (2018 년 06 월)
2018-07 호: 키보드 정보로 중요 정보 유출 시키는 '키로거' (2018 년 07 월)
2018-08 호: 정보 탈취 악성코드 "Orcus RAT" (2018 년 08 월)
2018-09 호: "갠드크랩 5.0" (2018 년 09 월)

감사합니다.

글로벌 네트워크 보안 솔루션 전문기업

SOOSAN INT

서울특별시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)

Tel 02.541.0073 | **Fax** 02.541.0204

E-mail QI@soosan.co.kr

HP http://www.soosanint.com