

# Internet Storm Center API

---

임현수  
3/7/2011



## 변경 이력

변경번호	변경일자	변경(작성)자	내용
01	2011/03/04	임현수	최초 작성
02	2011/03/07	임현수	통합검색 추가, rss.entries 호출 변경 (query)
			-이하 여백-



## 목 차

<b>1. NCHOVY Internet Storm Center</b> .....	<b>5</b>
1.1 개요 .....	5
1.2 API .....	5
<b>2. 경보단계</b> .....	<b>7</b>
2.1 threatcon.get .....	7
<b>3. SANS Internet Storm Center</b> .....	<b>9</b>
3.1 sans.getTopSourceSnapshots.....	9
3.2 sans.getRisingPortSnapshots.....	10
3.3 sans.getPortReportSnapshots .....	11
3.4 sans.getTopSources.....	12
3.5 sans.getRisingPorts.....	13
3.6 sans.getPortReports.....	14
<b>4. KrCERT 인터넷현황</b> .....	<b>15</b>
4.1 krcert.getHackingPatternSnapshots.....	15
4.2 krcert.getHackingPatterns .....	16
<b>5. 포트 정보</b> .....	<b>17</b>
5.1 serviceport.get.....	17
<b>6. CVE</b> .....	<b>18</b>
6.1 cve.get.....	18
6.2 cve.getList .....	19



<b>7. 홈페이지 변조현황</b> .....	<b>21</b>
7.1 deface.get.....	21
<b>8. 보안정보</b> .....	<b>23</b>
8.1 rss.entries.....	23
<b>9. 통합검색</b> .....	<b>25</b>
9.1 isc.search .....	25



# 1. NCHOVY Internet Storm Center

## 1.1 개요

---

엔초비 인터넷 스톰센터(<http://nchovy.kr>)에서는 각종 보안에 관련된 정보들을 한 눈에 볼 수 있게 정리해놓았고, 이를 편리하게 사용할 수 있도록 API를 제공하고 있다.

## 1.2 API

---

엔초비 인터넷 스톰센터의 정보들은 XML-RPC를 통해 제공된다. 아래 서버로 접속을 하면 된다.

- 주소: <http://nchovy.kr/xmlrpc>

API의 호출/반환에는 integer, double, string, boolean, date, map, list의 데이터 타입이 사용된다. 아래에는 많은 API에서 사용되는 호출/반환 항목들에 대한 설명을 적어놓았다.

### 1.2.1 호출

---

함수를 호출할 때 항목 요소가 써있는 순서대로 값을 입력해준다.

- api\_key (string)  
: 엔초비 인터넷 스톰센터로부터 발급받은 API KEY를 입력한다. 등록되지 않은 키값의 경우에는 값이 반환되지 않는다.
- page (integer)  
: 반환받을 정보들의 페이지
- page\_size (integer)  
: 한 페이지에 표시될 정보의 개수

### 1.2.2 반환

---

모든 함수들은 map 타입으로 반환된다. 항목 요소로 적혀있는 것이 key값이고, 괄호 안에 써있는 타입으로 value값이 반환된다.

date 타입의 경우 XML-RPC 스펙에서 지원하는 날짜 타입에서는 타임존을 지원하지 않기때문



에 모두 yyyy-MM-dd HH:mm:ssZ 포맷의 **스트링**으로 반환된다.

- total\_counts (integer)

: 여러 정보들을 반환받을 경우 반환받지 않은 정보들을 포함한 총 개수



## 2. 경보단계

국내경보단계와 국제경보단계 정보를 제공. 국내경보단계는 인터넷침해사고대응지원센터(<http://www.krcert.or.kr/>)의 정보를, 국제경보단계는 SANS Internet Storm Center (<http://isc.sans.edu/>)의 정보를 사용한다.

### 2.1 threatcon.get

---

현재 경보단계의 정보를 제공

#### 2.1.1 호출

---

- api\_key (string)

#### 2.1.2 반환

---

- alertcon (map)
  - id (integer)
  - status (integer)
    - : 1~5의 값을 가지며, 숫자가 작을수록 경보단계가 낮다. 순서대로 Green, Blue, Yellow, Orange, Red의 색을 의미
  - started\_at (date)
    - : 현재 경보 단계가 시작된 시간
  - checked\_at (date)
    - : 경보 단계를 확인한 시간
- infocon (map)
  - id (integer)
  - status (integer)
    - : 1~4의 값을 가지며, 숫자가 작을수록 경보단계가 낮다. 순서대로 Green, Yellow, Orange, Red의 색을 의미
  - reason (string)
    - : 경보를 발령한 이유
  - link (string)
  - started\_at (date)



- : 현재 경보 단계가 시작된 시간
- checked\_at (date)
  - : 경보 단계를 확인한 시간



## 3. SANS Internet Storm Center

포트 사용 통계, 공격자 IP 정보, 활동 증가 포트의 정보를 제공한다. 이 정보들은 SANS Internet Storm Center (<http://isc.sans.edu/>)에서 제공하는 정보들을 사용한다.

### 3.1 sans.getTopSourceSnapshots

---

공격자 IP 정보들을 수집했던 시간들을 최근순으로 반환.

#### 3.1.1 호출

---

- api\_key (string)
- page (integer)
- page\_size (integer)

#### 3.1.2 반환

---

- snapshots (date list)  
: 정보를 수집한 시간들 (최신순)
- total\_counts (integer)



## 3.2 sans.getRisingPortSnapshots

---

활동 증가 포트 정보들을 수집했던 시간들을 반환.

### 3.2.1 호출

---

- api\_key (string)
- page (integer)
- page\_size (integer)

### 3.2.2 반환

---

- snapshots (date list)  
: 정보를 수집한 시간들 (최신순)
- total\_counts (integer)



### 3.3 sans.getPortReportSnapshots

---

포트 사용내역 정보들을 수집했던 시간들을 반환.

#### 3.3.1 호출

---

- api\_key (string)
- page (integer)
- page\_size (integer)

#### 3.3.2 반환

---

- snapshots (date list)  
: 정보를 수집한 시간들 (최신순)
- total\_counts (integer)



## 3.4 sans.getTopSources

---

수집한 공격자 IP 정보들을 반환한다.

### 3.4.1 호출

---

- api\_key (string)
- date (string)
  - : yyyyMMddHHmmss 포맷으로 요청해야한다. 지정한 시간 이전의 정보들 중 가장 최근의 정보를 반환받게 된다. 일부만 입력(yyyyMMdd 또는 yyyy 등)해도 무방
- page (integer)
- page\_size (integer)
- order (string)
  - : 정보를 정렬할 방법을 지정. 유효값은 "attacks", "reports", "first\_seen", "last\_seen"

### 3.4.2 반환

---

- items (map list)
  - ip (string)
  - attacks (integer)
    - : 해당 IP로부터 발생한 공격 횟수
  - reports (integer)
    - : 보고서 수
  - first\_seen (date)
    - : hour 이하의 정보는 무효하며, day 단위 정보까지만 유효하다.
  - last\_seen (date)
    - : hour 이하의 정보는 무효하며, day 단위 정보까지만 유효하다.
- total\_counts (integer)
- created\_at (date)



## 3.5 sans.getRisingPorts

---

수집한 활동증가 포트 정보들을 반환한다.

### 3.5.1 호출

---

- api\_key (string)
- date (string)
  - : yyyyMMddHHmmss 포맷으로 요청해야한다. 지정한 시간 이전의 정보들 중 가장 최근의 정보를 반환받게 된다. 일부만 입력(yyyyMMdd 또는 yyyy 등)해도 무방
- page (integer)
- page\_size (integer)

### 3.5.2 반환

---

- max\_trend (map)
  - : 정보들 중 증가율이 가장 높은 포트
    - port (integer)
    - trend (double)
- items (map list)
  - port (integer)
  - trend (double)
    - : 해당 포트의 활동 증가율 (상대값)
- total\_counts (integer)
- created\_at (date)



## 3.6 sans.getPortReports

---

수집한 포트 사용내역 정보들을 반환한다.

### 3.6.1 호출

---

- api\_key (string)
- date (string)  
: yyyyMMddHHmmss 포맷으로 요청해야한다. 지정한 시간 이전의 정보들 중 가장 최근의 정보를 반환받게 된다. 일부만 입력(yyyyMMdd 또는 yyyy 등)해도 무방
- page (integer)
- page\_size (integer)
- order (string)  
: 정보를 정렬할 방법을 지정. 유효값은 "port", "records", "sources", "targets"

### 3.6.2 반환

---

- items (map list)
  - port (integer)
  - sources (integer)  
: 출발지로 사용된 횟수
  - targets (integer)  
: 목적지로 사용된 횟수
  - reports (integer)  
: 보고서 수
- total\_counts (integer)
- created\_at (date)



## 4. KrCERT 인터넷현황

국내 해킹 유형의 통계를 제공한다. 해킹 유형과 점유율의 정보는 인터넷침해사고대응지원센터 (<http://www.krcert.or.kr/>)에서 제공하는 정보를 사용한다.

### 4.1 krcert.getHackingPatternSnapshots

---

해킹 유형 정보를 수집한 시간들을 반환

#### 4.1.1 호출

---

- api\_key (string)
- page (integer)
- page\_size (integer)

#### 4.1.2 반환

---

- snapshots (date list)  
: 정보를 수집한 시간들 (최신순)
- total\_counts (integer)



## 4.2 krcert.getHackingPatterns

---

해킹 유형 정보를 반환

### 4.2.1 호출

---

- api\_key (string)
- date (string)  
: yyyyMMddHHmmss 포맷으로 요청해야한다. 지정한 시간 이전의 정보들 중 가장 최근의 정보를 반환받게 된다. 일부만 입력(yyyyMMdd 또는 yyyy 등)해도 무방
- page (integer)
- page\_size (integer)
- order (string)  
: 반환되는 정보들의 정렬 방법을 지정. 유효값은 "name", "share"

### 4.2.2 반환

---

- items (map list)
  - name (string)  
: 해킹 유형의 이름
  - share (double)  
: 해당 해킹 유형의 점유율 (%)
  - rank (integer)
  - term (integer)  
: 엔초비 스톱센터의 용어사전에 등록된 유형일 경우, 글 번호가 반환된다. 해당 글은 엔초비 스톱센터 포럼 용어사전 (<http://nchovy.kr/forum/5/article/{글번호}>)를 통해 접속할 수 있다.
- total\_counts (integer)



## 5. 포트 정보

포트별로 자주 사용되는 서비스들의 정보를 제공한다.

### 5.1 serviceport.get

---

포트별 서비스 정보들을 반환

#### 5.1.1 호출

---

- api\_key (string)
- page (integer)
- page\_size (integer)
- query (string)  
: 검색 키워드
- order (string)  
: 반환되는 정보들의 정렬 방법을 지정. 유효값은 “port”, “protocol”, “name”, “description”

#### 5.1.2 반환

---

- items (map list)
  - id (integer)
  - port (integer)
  - protocol (string)  
: 서비스가 사용하는 프로토콜. “tcp”, “udp”가 반환된다
  - name (string)
  - description (string)
- total\_counts (integer)



## 6. CVE

NIST NVD (<http://nvd.nist.gov/>)에서 배포되는 CVE 정보들을 정리하여 제공한다.

### 6.1 cve.get

---

CVE의 자세한 정보를 반환

#### 6.1.1 호출

---

- api\_key (string)
- name (string)
  - : “CVE-2011-0001”의 형태로 요청

#### 6.1.2 반환

---

- name (string)
  - : CVE의 이름. “CVE-2011-0001”의 형태로 반환된다.
- modified (date)
- published (date)
- discovered (string)
- descriptions (string list)
- cvss (map)
  - : CVSS 평가정보
    - base\_score (double)
      - : 해당 CVE의 위험도 지수
    - metrics (map list)
      - metric (string)
        - : 평가 기준. “access-vector”, “access-complexity”, “authentication”, “confidentiality-impact”, “integrity-impact”, “availability-impact”, “source”, “generated-on-datettime” 등이 있다.
      - value (string)
        - : metric이 “generated-on-datettime”인 경우 date 형태로 리턴된다
- vulnerable\_versions (map list)



- : 해당 CVE에 취약한 소프트웨어들
  - software\_vendor\_name (string)
  - software\_name (string)
  - version (string)
  - edition (string)
- references (map list)
  - : 참조 문서들
    - source (string)
      - : 참조 문서의 출처
    - url (string)
    - title (string)

## 6.2 cve.getList

---

여러 CVE의 간략한 정보를 반환

### 6.2.1 호출

---

- api\_key (string)
- page (integer)
- page\_size (integer)
- query (string)
  - : 검색 키워드

### 6.2.2 반환

---

- items (map list)
  - name (string)
  - seq (string)
  - modified (date)
  - published (date)
  - discovered (string)



- descriptions (string list)
- total\_counts (integer)



## 7. 홈페이지 변조현황

zone-h (<http://www.zone-h.org/>)에서 배포하는 홈페이지 변조현황 정보 중에서 피해 사이트가 한국 IP인 정보들을 제공한다.

### 7.1 deface.get

---

홈페이지 변조현황을 반환

#### 7.1.1 호출

---

- api\_key (string)
- page (integer)
- page\_size (integer)

#### 7.1.2 반환

---

- items (map list)
  - id (integer)
  - add\_date (date)
  - accept\_date (date)
  - attacker (string)
  - domain (string)
  - os (string)
  - image (string)
    - : 변조됐을 당시의 페이지를 보존한 주소. zone-h 페이지(<http://defaced.zone-h.net/>)를 통해 접속할 수 있다.
  - reason (string)
  - ip (string)
  - hackmode (string)
    - : “File Inclusion”, “SQL Injection”, “brute force attack” 등 어떤 방법을 사용하였는지 정보
  - webserver (string)
  - type (string)
    - : 대량으로 변조되었는지 여부에 따라 “mass”, “regular”의 값을 가진다.



- redefacement (boolean)
- is\_published (boolean)
- def\_grade (string)
  - : 변조 정도를 의미. 첫 화면 변조 여부에 따라 “homepage”, “secondary”의 값을 가진다.
- received (date)
- total\_counts (integer)



## 8. 보안정보

엔초비 스톰센터의 보안 정보들을 제공한다. 블로그스피어, 뉴스, 권고문, 익스플로잇, 바이러스의 정보들이 있다.

### 8.1 rss.entries

---

보안 정보들을 반환

#### 8.1.1 호출

---

- api\_key (string)
- type (string)
  - : 보안 정보의 타입을 지정. 유효값은 “blogosphere”, “news”, “advisory”, “exploit”, “malware”
- page (integer)
- page\_size (integer)
- query (string)
  - : 검색 키워드

#### 8.1.2 반환

---

- items (map list)
  - id (integer)
  - title (string)
  - author (string)
  - link (string)
    - : 원본 글의 주소
  - source (string)
    - : 원본 글이 있는 사이트의 이름
  - created\_at (date)
  - modified\_at (date)
  - read\_count (integer)
    - : 엔초비 스톰센터에서의 조회수
- total\_counts (integer)





## 9. 통합검색

엔초비 스톰센터의 모든 보안 정보들 중에서 원하는 키워드로 검색한 결과를 반환한다.

### 9.1 isc.search

---

보안 정보들을 반환

#### 9.1.1 호출

---

- api\_key (string)
- query (string)  
: 검색 키워드
- page (integer)
- page\_size (integer)

#### 9.1.2 반환

---

- cve (map list)
  - cve.getList의 반환형태와 동일. 단, modified, published의 정보 중 hour 이하 단위는 무효하다.
- blogosphere (map list)
  - content (string)  
: 해당 rss 내용의 앞부분 일부
  - rss.entries의 반환형태와 동일. 단, id, author, read\_count의 정보와 created\_at, modified\_at의 hour 이하 단위는 무효하다.
- news (map list)
  - blogosphere의 반환형태와 동일
- advisory (map list)
  - blogosphere의 반환형태와 동일
- exploit (map list)
  - blogosphere의 반환형태와 동일
- malware (map list)
  - blogosphere의 반환형태와 동일



