

ELK, Suricata, Slack 기능으로 NAS 보안 관제 장비 구현

정보보안SW융합전공

91812139 김성준

Index

/

1. 주제선정 이유
2. 프로젝트 목표
3. 기술 소개
 - 기술 스택
 - Suricata
 - ELK
 - Alert to Slack
4. 시나리오

주제선정 이유 NAS의 취약점

[보안] NAS 장비 관련 랜섬웨어 감염 확산에 따른 보안점검 권고

관리자 0 2,964 글주소

지난 주 발견된 더티파이프 취약점, 큐냅 NAS 장비들에서도 추가로 발견돼

안녕하세요? 정보넷 서버팀입니다.

좋아요 11개 | 입력 : 2022-03-16 15:24



최근 NAS* 대상 랜섬웨어 감염 사고가 지속적으로 발생하고 있음
* NAS(Network-Attached Storage) : 네트워크에 연결된 파일 저장
각 기관에서는 피해가 발생하지 않도록 보안 점검 및 대비를 철저
또한, 침해사고 등 이상징후 포착 시 정보통신망법에 의거하여 한

개인정보보호법과
가이드라인에 최적화된
비식별화 솔루션



#정보보호 #정보보안 #IT보안 #사이버보안

□ 주요 사고 사례

- o 보안 설정이 미흡하여 랜섬웨어 감염
- [사례] 접근제어 없이 공장 출하 시 설정된 기본 관리자 패스워드 시
- [사례] 기업명 등이 포함된 취약한 관리자 패스워드 사용
- [사례] 보안 업데이트 미적용으로 취약점 존재

리눅스 커널 여러 버전에서 더티파이프라는 취약점이 지난 주 처음 발견됐었다. 그리고 오늘 큐냅사의
장비들에서도 같은 취약점이 나왔다. 이 취약점의 파급력이 생각보다 클 수 있다는 경고 메시지가 같이
나왔다.

□ 보안 권고 사항

- 최초 설치 시 기본 관리자 패스워드는 반드시 변경 후 사용
- 알파벳 대문자와 소문자, 특수문자, 숫자를 조합한 복잡한 패스워드
- 자동 업데이트를 활성화하여 최신 펌웨어 유지
- 인터넷을 통한 직접 접속은 차단하고, 사내망에서 운영 권고
- ※ 불가피한 경우, 장비의 비밀번호 관리 및 백업, 보안 업데이트, 방화벽 등 철저한 관리 필요
- 네트워크와 분리된 별도의 장비에 정기적인 백업 권고

[보안뉴스 문가용 기자] 대만의 NAS 제조사인 큐냅(QNAP)이 자사 제품 일부에서 심각한 리눅스 관련
취약점을 발견했다고 발표했다. 이 취약점은 더티파이프(Dirty Pipe)라고 불리며, 지난 주에 처음으로
발견됐다. 더티파이프 취약점의 영향력 혹은 파급력이 매우 넓을 수 있음을 시사하는 발표 내용이다.



제16회 국제 시큐리티 콘퍼런스
ISEC 2022 2022년 10월 18(화)
서울 코엑스 3층 Hall

제22회 세계 보안 엑스포
SECON 2023 2023년 3월 29(수)
제2기든 WAVE 홀

주제선정 이유

NAS의 취약점을 통한 피해

사회

[단독] 대학·기업 원격저장장치(NAS)도 해킹 피해... "연구·특허 자료 유출 우려"

2021년 12월 07일 04시 48분 댓글 1개



사생활 영상 유출로 논란이 된 아파트 월패드뿐 아니라 IP 카메라나 공유기 같은 일상 속 네트워크 제품들도 쉽게 해킹 피해에 노출된다는 소식 전해드렸는데요.

최근 대학이나 기업에서 많이 사용하고 있는 원격저장장치도 사이버 공격 대상이 됐던 것으로 YTN 취재 결과 확인됐습니다.

국정원과 제조 업체가 발 빠르게 나서 추가 피해를 막긴 했지만, 언제라도 비슷한 공격이 있을 수 있어 주의가 필요합니다.

김철희 기자가 단독 보도합니다.

이렇게 해킹당한 장비는 암호 화폐 채굴이나 악성 코드 유포에 악용되기도 합니다.

무엇보다 민감한 정보가 외부로 빠져나갈 수 있다는 것이 문제입니다.

- 주요 대상이었던 기업에서 바뀐 공격대상
- 이제 학교와 같은 관공서도 공격대상
- NAS에 대한 공격만이 아닌 내부 행동에 대한 감시도 필요

주제 선정 이유

NAS의 보안 이슈에 따른 보안

로그 수집 기술

로그 수집 기술이란 무엇일까?
나는 회사에서 일을 하기 전까지는 로그 수집에 대한 지
이전까지는 로그 기록에 대한 필요성도 느끼지 못했고,
(어차피 개발하는 과정에서는 애려가 기본이기 때문이
하지만 완성된 시스템을 안정적으로 운영하는 업무를 수
필수적인게 없다는 생각이 든다.

만약 운영하고 있는 시스템에 장애가 발생한다면, 로그가
있기 때문이다.

개발기야 프로젝트에 관계된 소수의 개발자들끼리 지지
운영기는 실제로 사용되는 서비스이기 때문에 짧은 몇분
내가 운영 업무를 진행하는 시스템에서도 이를 위해 로
사용하고 있다.


시스템이야 널리고 널렸고 회사마다 사용하는 것의 차이
어쨌든 IT 업계에서 개발 직군으로 일하게 된다면 반드시
로그 관련 기술이다.

이번 글에서는 그런 기술 중에서도 꽤나 트렌디하고 핫


2. ELK Stack의 장점

정말 간단하게 썼지만, ELK가 뭔지에 대해
매년 쏟아져 나오는 IT 기술, 그리고 그걸
보통 그 다음으로 궁금해하는건.. "그래서

가격



ELK는 Elastic이라는 회사에서 제공하
별도로 AWS EC2 등의 인스턴스에 시
ELK 자체로만은 무료이기 때문에 다

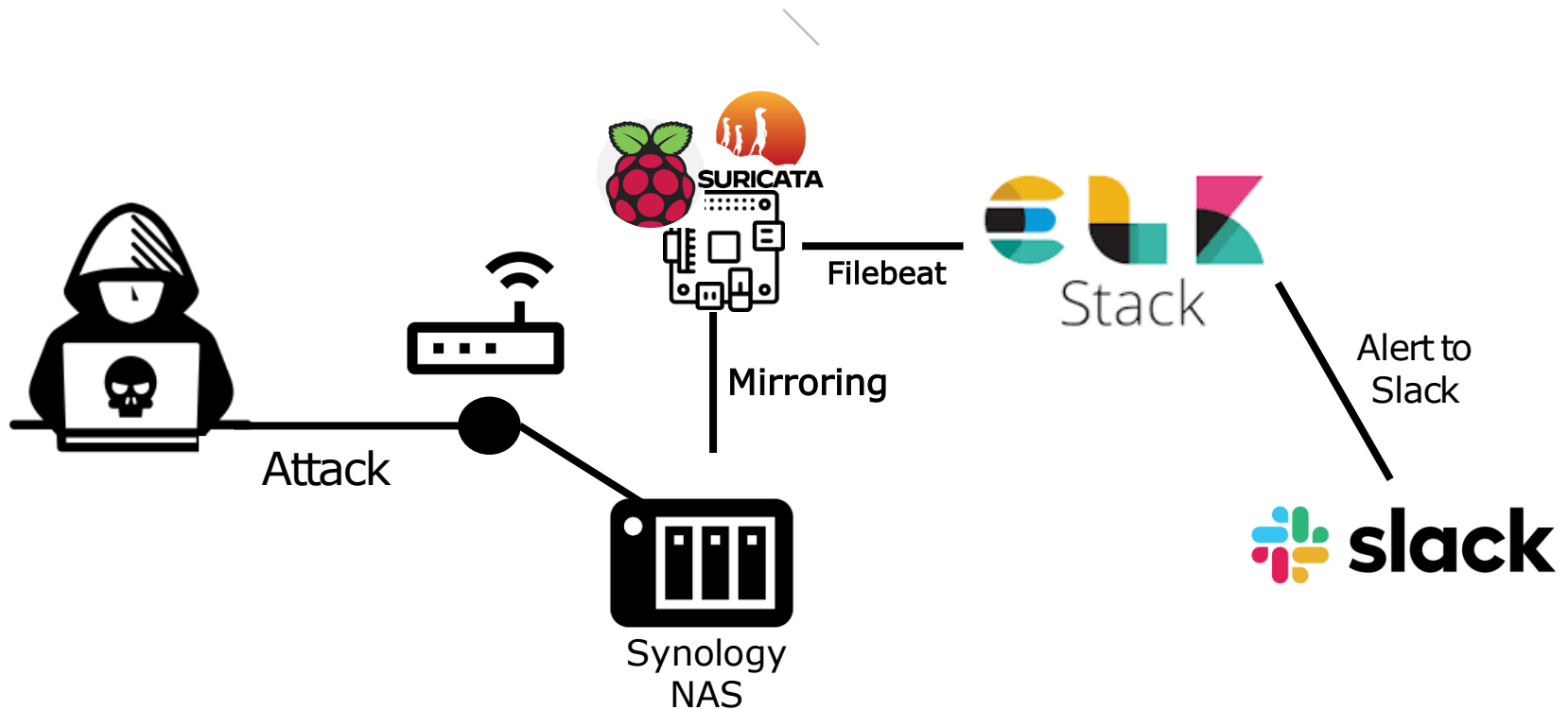


Collect & Transform → Search & Analyze → Visualize & Manage

logstash → elasticsearch → kibana

- 1. Data Processing (Logstash)**
 - 서버 내의 로그, 웹, 메트릭 등 다양한 소스에서 데이터를 수집하여 입력
 - 데이터 변환 및 구조 구축
 - 데이터 출력 및 송신
- 2. Storage (Elasticsearch)**
 - 데이터 저장
 - 데이터 분석
 - 데이터 관리
- 3. Visualize (Kibana)**
 - Dashboard를 통한 데이터 탐색
 - 팀원들과 공유 및 협업하는데 사용 가능
 - 액세스 제어 (Access Control) 사용 가능

프로젝트 목표
NAS의 공격 시나리오

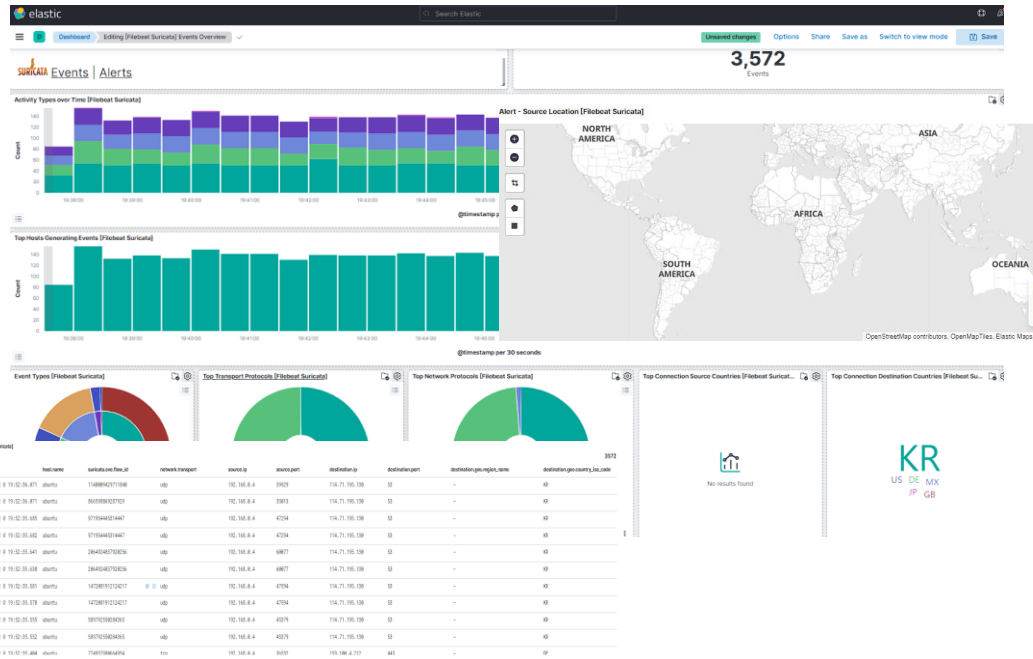


프로젝트 목표
NAS의 보안 구축

ELK 대쉬보드에 공격 정보를 출력하여 보안 모니터링 중 발생한 이벤트에 대하여 slack 연동하여 실시간 알람 기능 제공

<ELK Dashboard>

Slack



```
# post_malware
[{"pkts_to_server":1,"pkts_to_client":0,"bytes_to":1074,"bytes_to_client":0,"start":"2022-07-25T20:37:19.720019+0000","end":"2022-07-25T20:37:19.720019+0000","age":0,"state":"new","reason":{"timeout":"alerted":false},"community_id":"1/J3wcDdtNz+NloBhp7Y7eZMRPs="}
num_hits: 3
num_matches: 1
간략히 보기

ICMP try to connect
ICMP try to connect

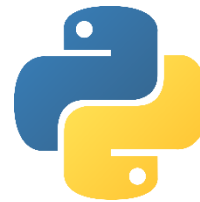
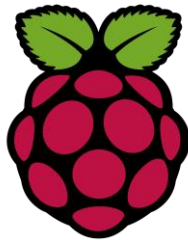
@timestamp: 2022-07-25T20:44:57.856Z
_id: B0kbN4IBR1dLHB8EG1pX
_index: filebeat-7.17.5-2022.07.25-000001
_type: _doc
agent: {
  "ephemeral_id": "240ad64b-f1c7-4e15-8a95-7554a858f106",
  "hostname": "ubuntu",
  "id": "375301c3-f9a1-4552-a104-32eb7c8a388d",
  "name": "ubuntu",
  "type": "filebeat",
  "version": "7.17.5"
}
destination: {
  "address": "192.168.0.4",
  "bytes": 0,
  "ip": "192.168.0.4",
  "packets": 0,
  "port": 0
}
ecs: {
  "version": "1.12.0"
}
```

기술 소개
보안 관제 기술 스택

Device

Software

Synology®



ubuntu



SURICATA

기술 소개 Suricata 흐름도

공격자는 Synology NAS에 공격을 시도합니다. 공격 패킷들은 NAS를 미리링 하는 Razpi (IPS)장비에 로그가 쌓이게 됩니다.



Hacker

```
# Store the message 'ts' and 'channel', so we can request the message
# permalink later when the user clicks the link button
TASK_IDS[task_id] = {
    'channel': res['channel'],
    'ts': res['message']['ts']
}

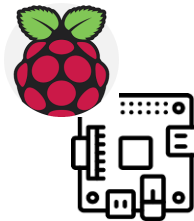
# This is where our link button will link to, showing the user a
# task to complete before redirecting them to the '/complete' page
@app.route("/workflow/<task_id>", methods=['GET'])
def test(task_id):

    task_form = """<form method="POST" action="/complete/{}">
        <input type="submit" value="Do The Thing" />
    </form>""".format(task_id)

    return make_response(task_form, 200)

@app.route("/complete/<task_id>", methods=['POST'])
```

Attack



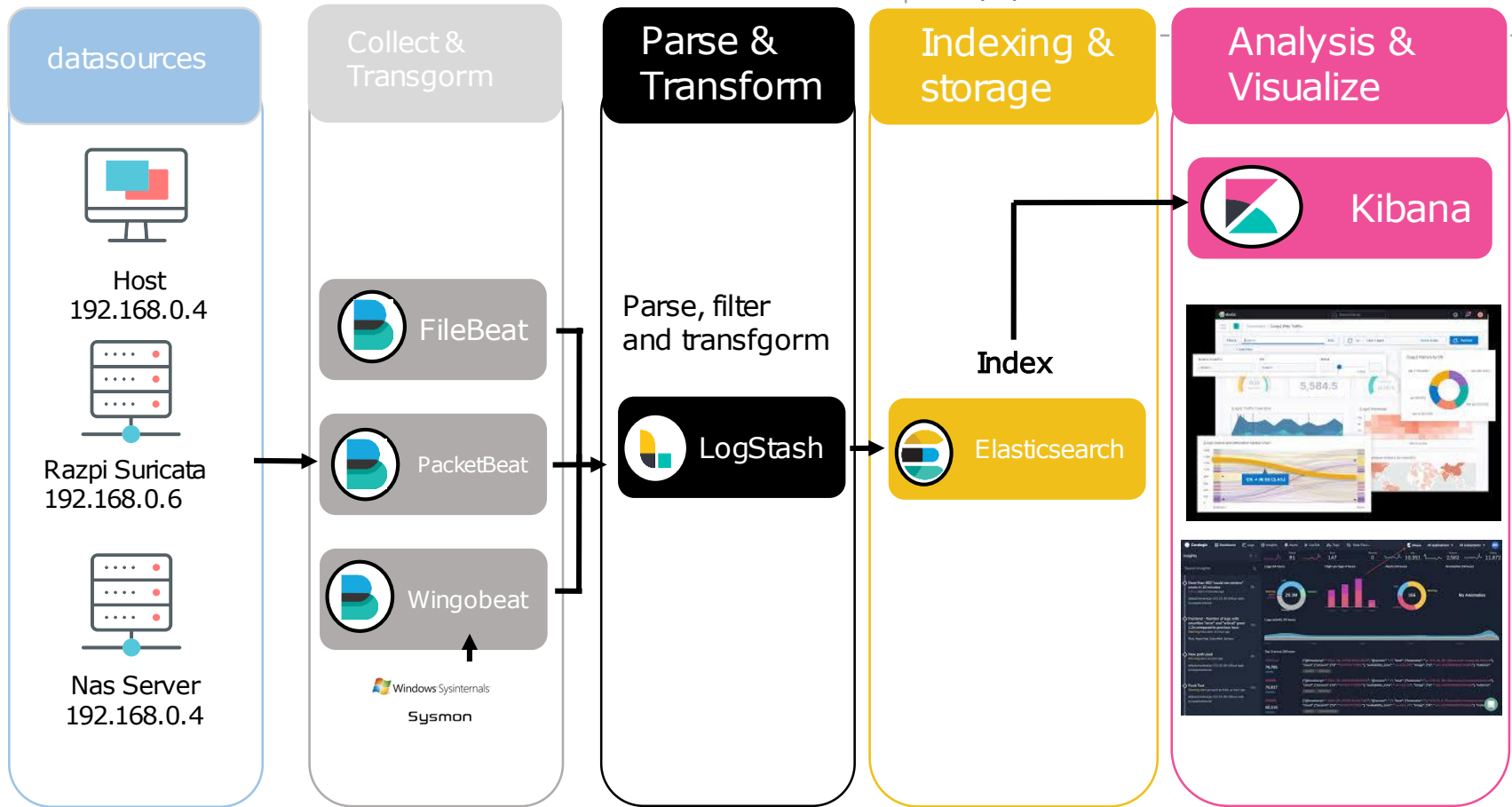
Razpi OS (IDS)

```
default-rule-path: /var/lib/suricata/rules
rule-files:
    #- suricata.rules
    - test.rules
```

```
alert icmp any any -> $HOME_NET any (msg:"UDP 연결 시도"; sid:1000002; rev:1;)
alert tcp any any -> any any (msg:"NAS 접속 시도"; content:"GET /"; content:"Host: https://quickconnect.to/bark0205"; sid:10001; rev:1;)
alert udp any any -> any any (msg:"NAS 접속 시도"; content:"GET /"; content:"Host: https://quickconnect.to/bark0205"; sid:10002; rev:1;)
alert tcp any any -> any any (msg:"Raz Pi 접속 시도"; content:"GET /"; content:"Host: 192.168.0.2"; sid:10011; rev:1;)
alert tcp any any -> any any (msg:"NAS IP 접속"; content:"GET /"; content:"Host: 192.168.0.4"; sid:10012; rev:1;)
alert udp any any -> any any (msg:"NAS IP 접속 UDP"; content:"GET /"; content:"Host: 192.168.0.4"; sid:10013; rev:1;)
alert tcp any any -> any any (msg:"NAS 접속 시도 UDP"; content:"GET /"; content:"Host: 192-168-0-4.park0205.direct.quickconnect.to"; sid:100004; rev:1;)
alert udp any any -> any any (msg:"NAS 접속 시도 UDP"; content:"GET /"; content:"Host: 192-168-0-4.park0205.direct.quickconnect.to"; sid:100005; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"TCP Packet Check"; flow:established; sid:100015; rev:1;)
alert udp any any -> $HOME_NET any (msg:"UDP Packet Check"; flow:established,to_server; sid:100016; rev:1;)
```

기술 소개 ELK 흐름도

ELK 대시보드에 공격 정보를 출력하기 위해 IDS 장비에서 보내주는 로그 절차입니다.



기술 소개 Alert to Slack

ElastAlert를 사용하여 보안 모니터링 중 발생한 이벤트에 대하여 slack 연동하여 실시간 알람 기능 제공



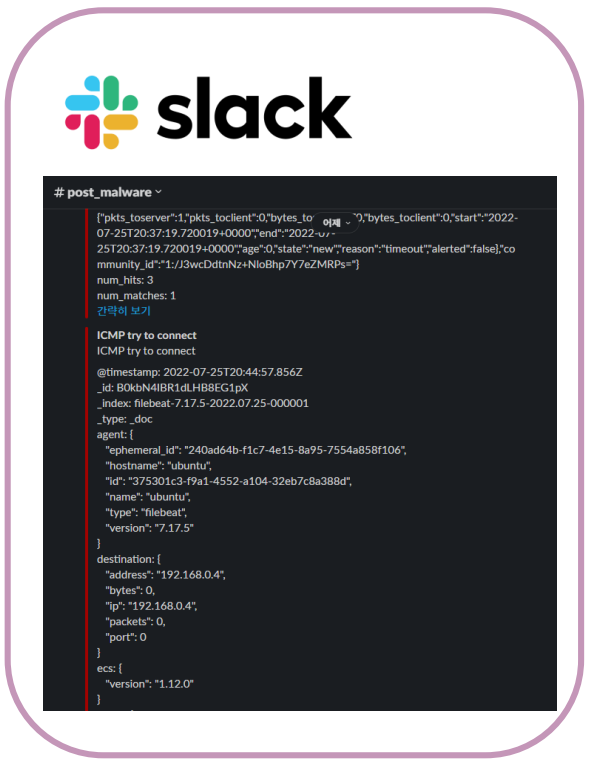
ElastAlert

```

0 connect from 2022-07-26 05:33 KST to 2022-07-26 05:48 KST: 4 / 4 hits
0 connect from 2022-07-26 05:33 KST to 2022-07-26 05:48 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:49 KST
its thread 0 pending alerts sent at 2022-07-26 05:49 KST
[{}]
9.999915 seconds
0 connect from 2022-07-26 05:34 KST to 2022-07-26 05:49 KST: 4 / 4 hits
0 connect from 2022-07-26 05:34 KST to 2022-07-26 05:49 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:50 KST
its thread 0 pending alerts sent at 2022-07-26 05:50 KST
[{}]
9.999751 seconds
0 connect from 2022-07-26 05:35 KST to 2022-07-26 05:50 KST: 4 / 4 hits
0 connect from 2022-07-26 05:35 KST to 2022-07-26 05:50 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:51 KST
its thread 0 pending alerts sent at 2022-07-26 05:51 KST
[{}]
9.999725 seconds
0 connect from 2022-07-26 05:36 KST to 2022-07-26 05:51 KST: 4 / 4 hits
0 connect from 2022-07-26 05:36 KST to 2022-07-26 05:51 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:52 KST
its thread 0 pending alerts sent at 2022-07-26 05:52 KST
[{}]
9.999725 seconds
0 connect from 2022-07-26 05:37 KST to 2022-07-26 05:52 KST: 4 / 4 hits
0 connect from 2022-07-26 05:37 KST to 2022-07-26 05:52 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:53 KST
its thread 0 pending alerts sent at 2022-07-26 05:53 KST
[{}]
9.999756 seconds
0 connect from 2022-07-26 05:38 KST to 2022-07-26 05:53 KST: 4 / 4 hits
0 connect from 2022-07-26 05:38 KST to 2022-07-26 05:53 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:54 KST
its thread 0 pending alerts sent at 2022-07-26 05:54 KST
[{}]
9.999756 seconds
0 connect from 2022-07-26 05:39 KST to 2022-07-26 05:54 KST: 4 / 4 hits
0 connect from 2022-07-26 05:39 KST to 2022-07-26 05:54 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:55 KST
its thread 0 pending alerts sent at 2022-07-26 05:55 KST
[{}]
9.999757 seconds
0 connect from 2022-07-26 05:40 KST to 2022-07-26 05:55 KST: 4 / 4 hits
0 connect from 2022-07-26 05:40 KST to 2022-07-26 05:55 KST: 4 query hits (4 already seen), 0 mat
figuration change check run at 2022-07-26 05:56 KST
its thread 0 pending alerts sent at 2022-07-26 05:56 KST
[{}]

```

Alert to Slack



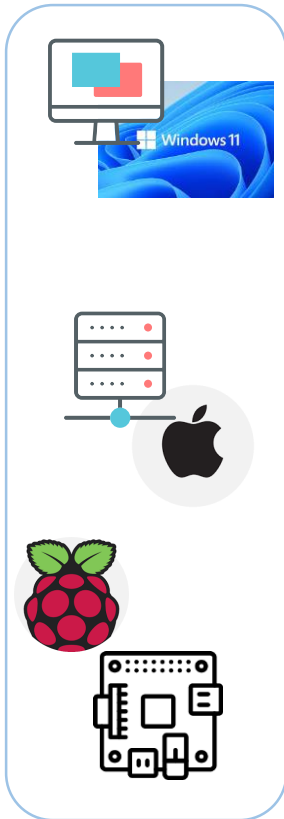
slack

```

# post_malware
[{"pkts_toserver":1,"pkts_totclient":0,"bytes_to_server":0,"bytes_totclient":0,"start":2022-07-25T20:37:19.720019+0000,"end":2022-07-25T20:37:19.720019+0000,"age":0,"state":"new","reason":"timeout","alerted":false,"community_id":"","j3wcDdtNz+NioBhp7Y7eZMRPs="}]
num_hits: 3
num_matches: 1
간략히 보기
ICMP try to connect
ICMP try to connect
@timestamp: 2022-07-25T20:44:57.856Z
_id: B0kbn4lBR1dlH88EC1pX
_index: filebeat-7.17.5-2022.07.25-000001
_type: _doc
agent: {
  "ephemeral_id": "240ad64b-f1c7-4e15-8a95-7554a858f106",
  "hostname": "ubuntu",
  "id": "375301c3-f9a1-4552-a104-32eb7c8a388d",
  "name": "ubuntu",
  "type": "filebeat",
  "version": "7.17.5"
}
destination: {
  "address": "192.168.0.4",
  "bytes": 0,
  "ip": "192.168.0.4",
  "packets": 0,
  "port": 0
}
ecs: {
  "version": "1.12.0"
}

```

기술 소개 서버 구성도



Host Name	IP Address	purpose	Domain Name	비고
Host	10.100.111.202	Host PC	-	AttackTest PC
Host Name	IP Address	purpose	Domain Name	비고
ELK	192.168.0.6	Log	Log	Suricata 탐지률을 통해 공격 패킷 탐지 로그들을 대시보드화 시켜 Slack통신을 통한 Send Message
Host Name	IP Address	purpose	Domain Name	
Alert	192.168.0.6	Slack	Alert to Slack	

Host Name	IP Address	purpose	비고
Razpi	192.168.0.2	Suricata	NAS 패킷 미러링을 통해 탐지률에 등록된 공격 패킷 탐지

C:\Users\ddvop\Desktop\NAS\tw.py - Sublime Text (UNREGISTERED)

www.BANDICAM.com

Edit Selection Find View Goto Tools Project Preferences Help

```

test.py - CCIT
tw.py - CCIT
tw.py - NAS
ab.py
test.py - NAS

1 import requests
2 import time
3 from urllib import parse
4 from selenium import webdriver
5 from urllib.parse import urlparse
6 from selenium.common.exceptions import NoSuchElementException
7 import os.path
8
9 session_id = 'JSESSIONID'
10 session_value = '8F9393F17A57071985653EE47CA'
11 cookies = {session_id : session_value}
12 driver = webdriver.Chrome()
13 driver.implicitly_wait(3)
14
15 ### admin page find ###
16 find_admin_page = open("C:/Users/ddvop/Desktop/NAS/admin_page_find.t
17 total_success = 0
18 k = 0
19 total_pass = 0
20 attack=[]
21 find_admin = []
22 lines = find_admin_page.readlines() # Read admin_page Pattern
23 print('[!] URL Admin Page Test')
24 driver.get('https://park0205.jp5.quickconnect.to/')
25 time.sleep(11)
26 for i in lines:
27     attack.append(i[:-1] + '.jsp')
28     url = 'https://park0205.jp5.quickconnect.to/'+str(attack[k])
29     time.sleep(0.5) # 지속적인 Request 패킷에 대한 sleep 0.5초 후에 R
30     print(url)
31     res = requests.get(url, cookies=cookies) # Request
32     if res.status_code == 200:
33         driver.get(url) #
34         time.sleep(3)
35     search_box = driver.find_element_by_xpath('//*[@id="a"l')
  
```

```

search_box = driver.find_element_by_xpath('//*[@id="a"l')
[+] pass1
https://park0205.jp5.quickconnect.to/webcamnow.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/webchat.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/webcheck.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/webcom.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/verizon.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/versant.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/versatilebulletinboard.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/verso.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/vertical.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/horizon.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/verylost.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/vhcs.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/datakommunikation.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/webcortex.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/webct.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/webdesignh.jsp
[+] pass1
  
```

```

[!] Total : [0]pass1 : 17
[!] Total : [0]Success : 0
Traceback (most recent call last):
  File "C:\Users\ddvop\Desktop\NAS\tw.py", line 65, in <module>
    time.sleep(6)
KeyboardInterrupt
^C
C:\Users\ddvop\Desktop\NAS>tw.py
  
```

```

DevTools listening on ws://127.0.0.1:56524/devtools/browser/ab642642-fd9a-4dff-b2a4-becea30b009f
[!] URL Admin Page Test
https://park0205.jp5.quickconnect.to/admin1.jsp
[19444:18308:0728/090425.850:ERROR:device_event_log_impl.cc(214)] [09:04:25.850] Bluetooth: bluetooth_adapter_winrt
c:1074 Getting Default Adapter failed.
C:\Users\ddvop\Desktop\NAS\tw.py:35: DeprecationWarning: find_element_by_xpath is deprecated. Please use find_eleme
(by=By.XPATH, value=xpath) instead
search_box = driver.find_element_by_xpath('//*[@id="a"l')
[+] pass1
https://park0205.jp5.quickconnect.to/webcamnow.jsp
[+] pass1
https://park0205.jp5.quickconnect.to/webchat.jsp
Traceback (most recent call last):
  File "C:\Users\ddvop\Desktop\NAS\tw.py", line 34, in <module>
    time.sleep(3)
KeyboardInterrupt
^C
C:\Users\ddvop\Desktop\NAS>
  
```

Q&A