

# 인공지능을 활용한 사이버위협 모니터링 기술

AIS 2021

고려대학교 정보보호대학원

해킹대응기술연구실



**KOREA**  
UNIVERSITY



**AI Spera**  
AI Security Professional Era



# About me (김휘강)

Co-Founder, AI.Spera (2017-)

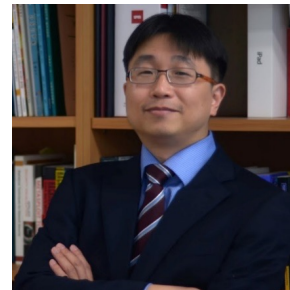
Professor, School of Cybersecurity, Korea Univ. (2010.3-present)

## Recent works

- International Conferences: NDSS AutoSec, ACSAC, NDSS, WWW (TheWebConference) 등 전산 및 보안분야 Top conference 에 논문 다수 게재
- International Journals: IEEE Trans. on Industrial Informatics, IEEE Trans. on Vehicular Technology, Vehicular Communications, IEEE Trans. on Information Forensics and Security 등 다수의 차량 보안 분야 Top journal 에 논문 다수 게재
- International Standard
  - Main Editor, ITU-T SG17/Q13, X.1375 "Guidelines for intrusion detection system for in-vehicle networks" (published)
  - Main Editor, ITU-T SG17/Q13, X.ipscv "Methodologies for intrusion prevention systems for connected vehicles" (on-going work)
  - Main Editor, ITU-T SG17/Q7, X.sec-grp-mov "Security guideline for group movement service platform" (on-going work)

## Machine Learning 기반 차량 해킹방어대회 main organizer (2017-present)

- <http://datachallenge.kr/challenge18/vehicle/introduction/> (AI기반 차량도난탐지, 2018 정보보호R&D 데이터챌린지)
- <http://datachallenge.kr/challenge17/car/challenge/> (차량 네트워크 이상징후 탐지 알고리즘 구현, 2017 정보보호R&D 데이터챌린지)
- <http://datachallenge.kr/challenge19/convergence-security/vehicle/introduction/> (자동차용 침입탐지, 2019 정보보호 R&D 데이터챌린지 - 융합보안챌린지)
- <https://www.k-csc2020.com/p3/c1/> (K-사이버 시큐리티 챌린지 2020 자동차 해킹 공격/방어)
- <https://sec-challenge.kr/main>, 사이버보안챌린지 2021



# 0. 들어가며

---

## ■ Cyber Threat Intelligence

- 다양한 위협들에 대한 선제적인 정보 확보에 필수
- Attack surface management (공격표면관리) 를 통한 취약점

## ■ 위협정보 기반 공격 표면 모니터링 관리에 쓰일 수 있는 요소 기술

- Attack Graph 기반 공격 경로 시뮬레이션 + MITRE ATT&CK
- DGA (Domain Generation Algorithm)
- 유사도메인 검색을 통한 잠재적 phishing domain 발견
- Crawling + Banner info. Handling + OCR

# 1. Attack Graph + MITRE ATT&CK

---

- BAS (Breach and Attack Simulation) 등 다양한 simulation 에 응용되는 기반 기술
  - 확률 모델, 취약점 기반, 시나리오 기반, profiling 기반으로 시뮬레이션하는데 사용됨
  - 가장 취약한 (가장 높은 확률로 침투해 들어올 것으로 예상되는) 잠재 경로 산정, 패치 우선순위 결정에 활용
  - 특히 MITRE ATT&CK 과 결합하여 Cyber Threat Actor group 정보를 hyper parameter 로 받아 시뮬레이션 하는 등 효용성이 높아지고 있는 추세
- 
- Attack IQ, Threat Simulator 와 같은 상용 제품
  - 또는 Infection Monkey 와 같은 Open source
  - 주요 논문들에서 공개한 framework
    - 1. MITRE CALDERA (<https://github.com/mitre/caldera>)
    - 2. 고려대학교 해킹대응기술연구실 repository (<https://github.com/hksecurity/Red-Blue-Agents> )

# 1. Attack Graph + MITRE ATT&CK (demo)

네트워크 도플로지 시뮬레이터


163.152.127.184:40080/?uploaded\_topology=

Select topology json file: 파일 선택 선택된 파일 없음 Upload topology

Use Default Topology Use Uploaded Topology

Refresh and Draw Topology Export Current Topology as json

Edit



Asset Info Block Rule Risk Info Attack Path Attack Scenario

Start analysis

Status: done

ID	
Risk Score	
Related CVEs	

## 2. DGA (Domain Generation Algorithm)

---

### ■ DGA란

- Domain Generation Algorithm의 약자
- 도메인 이름(domain name)을 생성하는 알고리즘을 의미
- 주로 악성코드에 DGA가 내장되어 임의의 도메인을 생성함
  - 매우 많은 도메인 이름을 임의로 생성함
  - 생성한 도메인은 C&C 서버와 통신하는 지점이 됨
  - 매우 많은 도메인 이름을 생성하기 때문에 효율적인 도메인 차단이 힘들
  - 따라서 악성코드는 C&C 서버를 통해 계속해서 업데이트되고 공격 명령을 수신할 수 있음

### ■ DGA 출현 이전 악성코드

- 미리 생성된 도메인 리스트가 악성코드 내부에 삽입됨
  - 미리 생성되었기 때문에 도메인이 정적(static)인 특징을 지님
- 방어자는 악성코드 분석을 통해 해당 도메인 리스트를 확보할 수 있음
- 악성 도메인이 재빨리 막힐 가능성이 높음
- 악성 도메인이 막힐 경우 공격자는 새로운 도메인이 삽입된 악성코드 변종을 유포
- 악성 도메인이 막힐 경우 공격자는 새로운 도메인에 대한 C&C 서버 구축

## 2. DGA (Domain Generation Algorithm)

### ■ DGA의 기본 특징

- 알고리즘이 공격자의 입장에서는 충분히 predictable해야 함
  - Predictability를 위해 알고리즘에 seed를 이용
    - Seed 값을 알면 똑같은 도메인을 재생성할 수 있음
  - Predictability를 위해 알고리즘에 시간에 따라 변화하는 파라미터를 전달
- 알고리즘이 방어자의 입장에서는 최대한 unpredictable해야 함

```
def generate_domain(year, month, day):  
    """Generates a domain name for the given date."""  
    domain = ""  
  
    for i in range(16):  
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFFF0) << 17)  
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFF8)  
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFFE) << 12)  
        domain += chr(((year ^ month ^ day) % 25) + 97)  
  
    return domain + ".com"
```

```
print(generate_domain(2019, 6, 11))
```

```
tjavhlnkjxomkmh.com
```

[DGA의 간단 예시 – From Wikipedia]



## 2. DGA - sites examples

### ■ DGA vs. normal (benign) names

#### Cryptolocker

etledwndgunmrt  
obgfmoyfwptep  
bugvesrwqxdjoa  
qxavdikemhepxk  
ohgnphscwbyvuse  
fbvegghechlth  
ihyrtyunnaltjm  
auxiyeexsfccj  
tknbivcmbekpwh  
gtpjifumwqpn  
cnqggglwruclrgp  
aucdtwkdfyewc

#### Goz

eiaupamojzhlrciwkeghyxd  
tkdabqnkrgdozhithhypz  
uswodcmnvemqfmzxynjdnvhyvbe  
ohhyhypphvgutucgiemfgdhai  
ydgwmzhgaxoxfyzvcpvqgmfxro  
kbcirszzxscgeukcizjrntclvp  
eiseiondsgkbnzvgwdehxda  
ytwkplzlobljxkljhushyxyt  
hswvovkduhlbfugqxpfnjzn  
vwdjxoqworljhirgetwh  
xcbeeieymbguwdcabueipzwg  
pdqfrsvgkkuwvmvgpvwayyzleu

#### NewGoz

1erk1aq2tfv3eldy8ikv1f0nxs8  
i5ep5311fuanclytynl1mmkio4  
zj7llmpk5fo87dtcg81e2j07c  
vehvq1swdu9vuhfqvrcjxr46  
1ncn8kn675d4o6dc4hh1f0se4r  
1v11tu8z5okt61njpiy1xoprmr  
sd345o1rq011a1ms3qlley5yvu  
1jz5kklbpm53r2pdymmri043  
17adaod1oih6t91x358vyshspil  
1e95km61jytx813ozodwofkggu  
970z95v4nzglqmt2c37ib43h  
5a3d2xgu8lq31bbf72q717o6c

#### Legit

fujifilm  
dallasdoglife  
startups  
askganesha  
wildcatdirectory  
cherokeeherald  
admaster  
directory2009  
theupsstore  
expediamail  
dyad-inc  
qimaging

- Benign - Human pronounceable, readable, relatively short
- Malicious – human unpronounceable, unreadable, relatively long



## 2. DGA - 탐지 및 해결 방안 (deep learning)

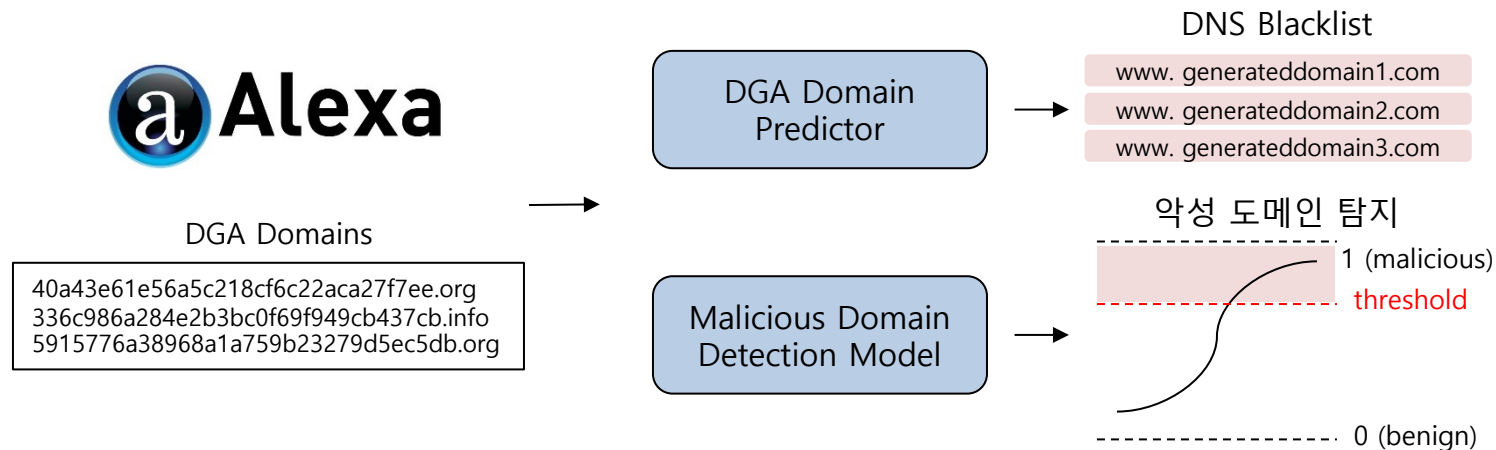
---

### ■ DGA 탐지

- 블랙리스트로 차단하는 방법에는 한계점이 존재
  - Public blacklist의 경우, 차단 도메인의 범위가 적음
  - Commercial vendor blacklist의 경우, vendor마다 차단 도메인이 서로 달라 통일성이 없음
- 최근 기계학습과 빅데이터를 통한 DGA 탐지 방법이 연구되고 있음
  - Contextual information을 이용
    - NXDOMAIN network response, WHOIS information, passive DNS 등의 정보를 이용
    - 도메인 이름의 legitimacy를 평가
  - Deep learning을 이용
    - LSTM, CNN 등의 모델 이용

## 2. DGA - 탐지 및 해결 방안 (deep learning)

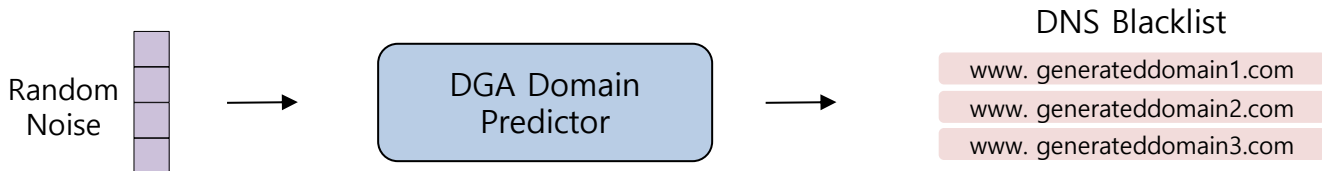
### ■ GAN 을 이용하는 방법



## 2. DGA - 탐지 및 해결 방안 (deep learning)

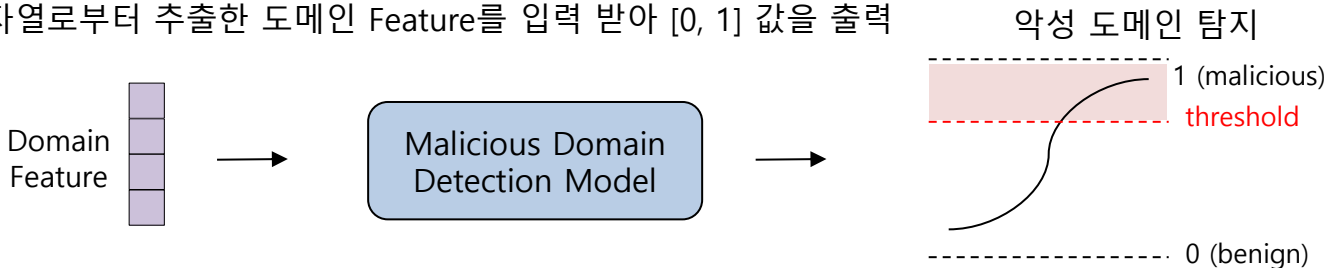
### ■ DGA 도메인 생성 모델 (DGA Domain Predictor)

- 임의의 난수로부터 잠재적인 악성 도메인을 생성하는 모델
  - 정상 도메인과 유사한 도메인을 생성



### ■ DGA 도메인 탐지 모델 (Malicious Domain Detection Model)

- 도메인 주소 문자열을 기반으로 악성여부를 판별하는 모델
  - 도메인 문자열로부터 추출한 도메인 Feature를 입력 받아 [0, 1] 값을 출력



## 2. DGA – 참고: 정상 도메인 데이터셋

### ■ Amazon's Alexa top million sites



SEO AND COMPETITIVE ANALYSIS SOFTWARE

# Find, Reach, and Convert Your Audience

Get better marketing results by finding untapped opportunities to grow your business.

**START YOUR FREE TRIAL**

[TAKE TOUR](#) [GUIDES](#) [BLOG](#) [LOG IN](#)

[SOLUTIONS](#) ▼ [TOOLS](#) ▼ [PRICING](#)

**START YOUR FREE TRIAL**

The screenshot shows the Alexa website interface. At the top, there's a navigation bar with 'Menu', the Alexa logo, a search bar, and 'Take To'. Below the navigation bar, it says 'Total keywords : 109,546'. There are buttons for 'Use Cases +', 'Filters +', and 'Toggle columns' with options for 'Organic', 'Paid', and 'Both'. The main table displays keyword data with columns for 'Keywords', 'Popularity', 'Average Traffic Score', 'Competition', and 'reverb'. Each row includes a star icon, a keyword, a popularity bar chart, and numerical values for each metric.

Keywords	Popularity	Average Traffic Score		Competition		reverb
		Popularity	Average Traffic Score	Organic	Paid	
☆ fender bassbreaker	31	44	3	65	6	62
☆ guitar	55	42	13	67	4	-
☆ fender player series	34	42	8	64	12	64
☆ fender hot rod deluxe	33	42	8	70	16	64
☆ fender meteora	27	41	5	64	4	63
☆ gibson les paul	43	40	8	73	11	67
☆ guitars	40	40	9	65	13	52
☆ player stratocaster	19	40	2	65	7	52
☆ electric guitar	46	39	5	71	4	58
☆ telecaster	42	39	6	70	3	61

## 2. DGA – 참고: DGA 도메인 데이터셋

### ■ DGA 도메인 데이터셋 구축

- 수집한 악성코드 내 DGA 알고리즘을 이용하여 DGA 도메인 생성

DGA 명	생성한 도메인 개수	DGA 명	생성한 도메인 개수	DGA 명	생성한 도메인 개수
bamital	20,000	dyre	20,000	murofet_v1	20,000
banjori	20,000	explosive	20,000	murofet_v2	20,000
bedep	172	flashback	20,000	murofet_v3	20,000
blackhole	733	fobber	20,000	mydoom	20,000
cclean	20,000	goz	20,000	necurs	20,000
chinad	20,000	gozi	19,939	newgoz	20,000
conficker	20,000	hesperbot	20,000	nymaim	20,000
corebot	20,000	kraken_v1	19,989	nymaim2	20,000
cryptolocker	20,000	kraken_v2	20,000	pacrypt	20,000
dircrypt	20,004	locky_v2	20,006	panda_banker	20,000
dnscchanger	20,000	locky_v3	20,000	pitou	20,000
dromedan	20,000	matsnu	20,000	proslkefan	20,000

### 3. 유사도메인 검색을 통한 잠재적 phishing domain 검출

---

- 전세계의 모든 Domain name list 를 대상으로 유사 도메인 검색
- 검출된 domain 들의 현재 risk score (reputation score) 를 검색
- 단, 현재는 risk score 가 낮은 악성 도메인도 존재 (도메인 확보를 먼저 해두고 공격 착수에는 들어가지 않은 파킹 상태에 있는 도메인)
- 유사도메인 검색시, string similarity 는 token 기반 거리 (Jaro-Winkler distance), edit 기반 거리 (Levenshtein distance) 등을 응용하여 스코어링



### 3. 유사도메인 검색을 통한 잠재적 phishing domain 검출

■ SOURCE: RMR (d-rmr.com) by AI Spera



Domain

**westpac.com**

Count 23

Last Run Time 2021-09-14 09:01:45

Registered Time 2020-12-15 09:00:00



westpac-info.com



ES

Registrar Hosting Concepts B.V. d/  
b/a Registrar.eu

Created Date 2021-08-23

Connected IP Address 5.199.162.111 **Critical**  
/ Score

westpac-login.com



Registrar NameCheap, Inc.

Created Date 2021-04-14

Connected IP Address 66.29.131.168 **Safe**  
/ Score

westpac-mobile.com



FR

Registrar CSC Corporate Domains, I  
nc.

Created Date 2018-01-08

Connected IP Address 51.91.60.4 **Low**  
/ Score

### 3. 유사도메인 검색을 통한 잠재적 phishing domain 검출

■ SOURCE: RMR (d-rmr.com) by AI Spera



Domain



**ooribank.com**

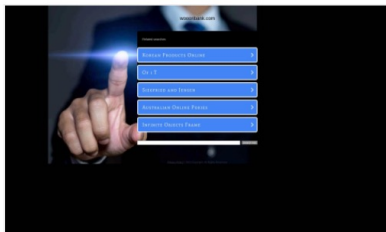
Count 9

Last Run Time 2021-09-14 09:03:20

Registered Time 2020-12-15 09:00:00



**ooribank.com**



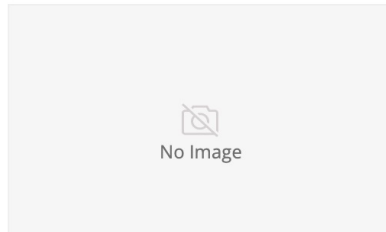
DE

Registrar 123-Reg Limited

Created Date 2021-06-05

Connected IP Address 185.53.178.10 Low  
/ Score

**ooribank.com**



DE

Registrar 123-Reg Limited

Created Date 2021-06-19

Connected IP Address 185.53.177.10 Low  
/ Score

**ooribank.info**



US

Registrar P.A. Viet Nam Company Limited

Created Date 2018-03-05

Connected IP Address 104.248.156.216 Low  
/ Score

## 4. Crawling + Banner info. Handling + OCR

---

### ■ Crawling

- Non intrusive, Fast scanning
- False-positive 를 최소화 하기 위한 문자열 처리 기술 필요

### ■ 배너 정보 (서비스 어플리케이션 및 OS 정보)

- 알려진 취약점 정보 (예: CVE 기반 목록) 에 해당되는 버전/OS 인지 확인하여 신속한 **Attack Surface Management** 에 활용 가능

### ■ OCR – 이미지 내에서 문자열 인식하는 AI/패턴인식 기술, 다국어 문자열 인식이 중요

- Open port 에서 text 가 아닌 Image 검출될 경우
- 취약한 IP CCTV 인지, RDP 인지 등 이미지 특성을 식별
- RDP 내에서도 OS, hostname, id 정보를 추출하여 위협 정보 관리에 활용

# 4. Crawling + Banner info. Handling + OCR

## ■ SOURCE: Criminal IP by AI Spera



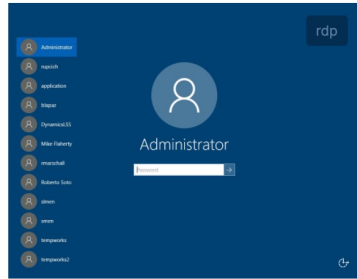
# 4. Crawling + Banner info. Handling + OCR

Found 12,391 Results

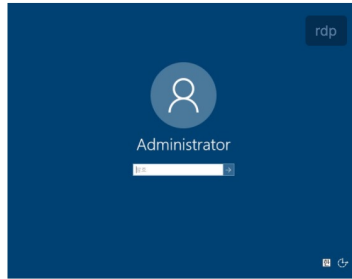
SOURCE: Criminal IP by AI Spera

RDP

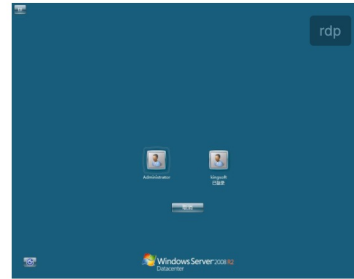
RDP



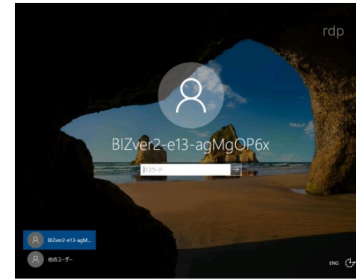
58.243.147  
2021-09-07 23:02:22



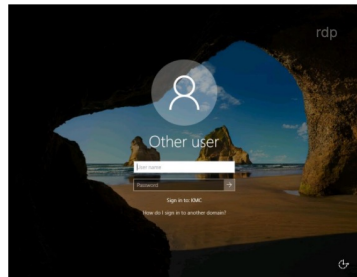
14.129.250  
2021-09-07 22:46:09



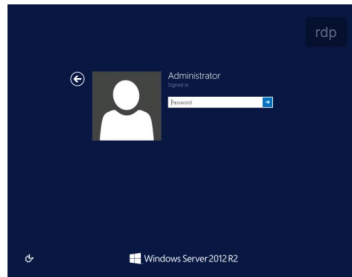
92.151.102  
2021-09-07 21:48:36



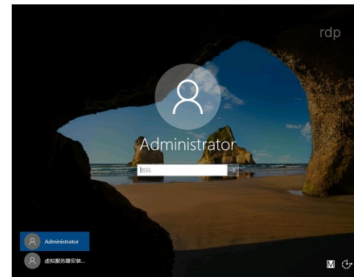
27.92.191  
2021-09-07 21:21:44



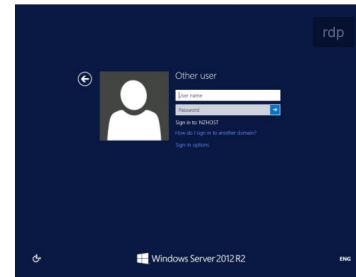
239.249.51  
2021-09-07 20:50:36



156.252.85  
2021-09-07 17:31:03



91.176.163  
2021-09-07 17:11:55

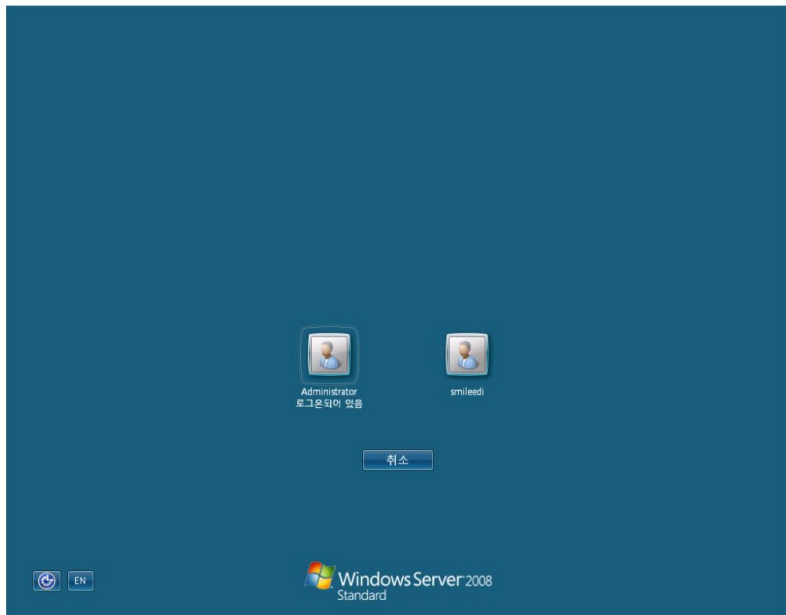


6.144.44  
2021-09-07 16:58:32

## 4. Crawling + Banner info. Handling + OCR

### ■ RDP OCR 예

- IP address, port 정보를 network 상으로 확인
- RDP 스크린 내에서 ID (계정명), 로그인 유무, OS version 상세 정보 습득 가능
- 이를 조직의 위협정보 및 Attack surface management 에 활용



#### RDP

IP	.216.69.27
Port	3389
Screen Content	Administrator,snileedi,로그온되어 있음,취소,Windows Server2008,Standard
Confirmed Time	2021-09-07 00:19:14



# 4. Crawling + Banner info. Handling + OCR

## ■ Attack Surface Management 에 활용 예

.233.255.137/32

○

.195.235.187/32

○

.194.105.241/32

○

.8.63.245.245/32

○

.8.63.240.126/32

○

.9.99.238.109/32

○

1

2

3

4

5

▶

⋮

Compare the number of opened IPs today with the previous on a number in Today to see the trend over the previous day

Port	A week ago	Yesterday
443	0	24
5000	0	17
80	0	18
445	0	0
53	0	1

Vulnerability of Opened Ports 758

View the Product Name, CVE Name, and CVSS Score if vulnerabilities are detected. When mouseover CVE names, it allows you to view descriptions of vulnerabilities.

CVE	Score	IP Address	Port	CVSS	Product/Version	Vender
<a href="#">CVE-2021-3426</a> 🔍 CWE 1	Critical	<div></div> 33.206.132	80	ADJACENT_NETWORK / Low ADJACENT_NETWORK / Medium	Python / 3.7.8	python
<a href="#">CVE-2021-3177</a> 🔍 CWE 1	Critical	<div></div> 233.206.132	80	NETWORK / High NETWORK / Critical	Python / 3.7.8	python
<a href="#">CVE-2021-28359</a> 🔍 CWE 1	Critical	<div></div> 233.206.132	80	NETWORK / Medium NETWORK / Medium	Python / 3.7.8	python
<a href="#">CVE-2021-28041</a> 🔍 CWE 1	Dangerous	<div></div> 9.99.238.109	22	NETWORK / Medium NETWORK / High	OpenSSH / 8.2p1	openbsd

## 5. 마치며

---

- AI for Security 는 향후 지속적으로 발전할 분야
- 인공지능의 다양한 요소기술을 활용하여 Cyber Threat Intelligence 프로세스를 자동화, 효율화 할 수 있음
- 위협정보 기반 공격 표면 모니터링 관리에 다양한 AI 요소기술 발굴 및 적용을 통해 보안향상을 꾀할 수 있음

*Thank you*

---



**KOREA**  
UNIVERSITY



**AI Spera**  
AI Security Professional Era