Prediction of Future Attack Indicators based on the 2024 Analysis of Threats from Malicious App Distribution Sites in South Korea

September 26, 2025

Kyung Rae Noh (Anthony)
anthonynoh@kisa.or.kr

Table of Contents

Prediction of Future Attack Indicators based on the 2024 Analysis of Threats from Malicious App Distribution Sites in South Korea

01 Introduction and Research Background

02 Cyber-Spider System Overview

03 2024 Smishing Statistical Analysis

04 Relationship Analysis Using NS and Smishing URL Pattern Mining

05 2025 Pre-detection Experiment

06 Conclusion and Future Research Directions

Cyber Threat Response Center for Private Sector

Response

Ministry of Science and ICT

KISA KOREA INTERNET & SECURITY AGENCY

KrCERT/CC

Public Investigation

Prosecution Service

National Police Agency

- Cyber incident investigation request

Public National Security

National Security Office

National Cyber Security Center

National Cyber Crisis Management Center

- Threat intelligence sharing, joint incident investigation

Private Internet Service Provider

11 operators including KT, SKB, LGU+ (ISP)

- Malicious site blocking
- Sharing information related to security incidents

Private Security Companies

Operating domestic intelligence consortium including AhnLab

- Continuous threat intelligence sharing

Private Citizens

- Phishing damage consultation and prevention/response
- Infected device treatment guidance

Private Enterprises

- Latest threat security notifications
- Vulnerability assessment and incident response

Private Foreign Government Agencies/CERT

NIST, FIRST, APCERT, etc.

- Mutual sharing of domestic and international threat intelligence
- Hacking group tracking, joint cyber domain response

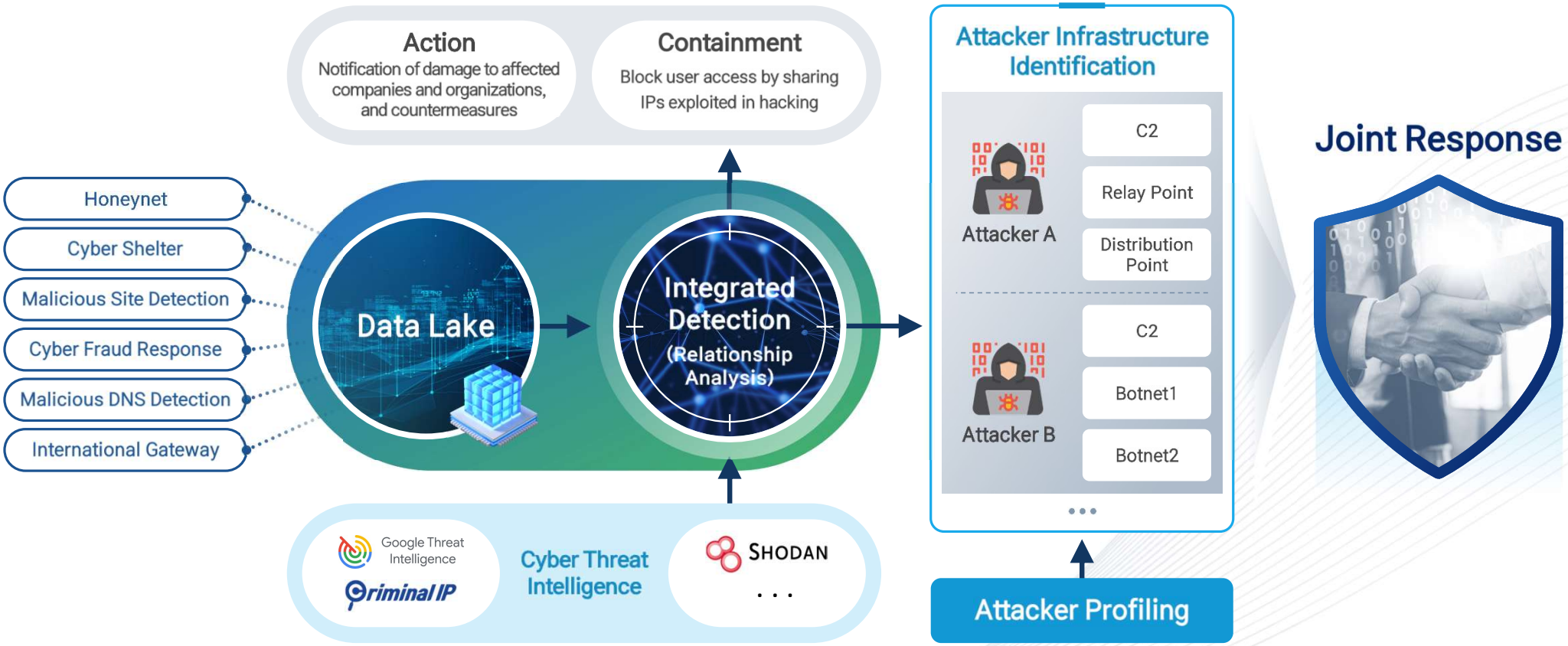
Private Global Companies

Google, MS, Trend Micro, etc.

- Threat intelligence sharing

CYBER-SPIDER PROJECT

Cyber Attack Integrated Detection and Response Framework(C-SPIDER)

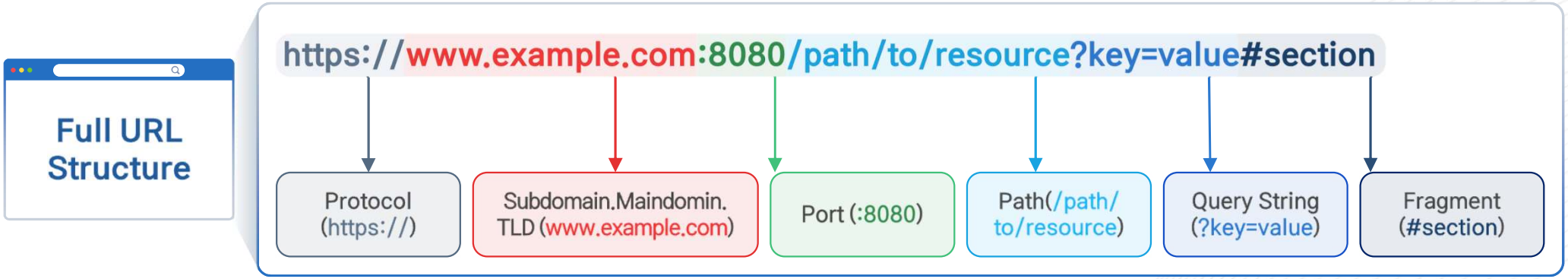


Introduction

Analyzed 2,136 deduplicated smishing messages from 10,358,700 total messages collected by KISA's Cyber-Spider in 2024

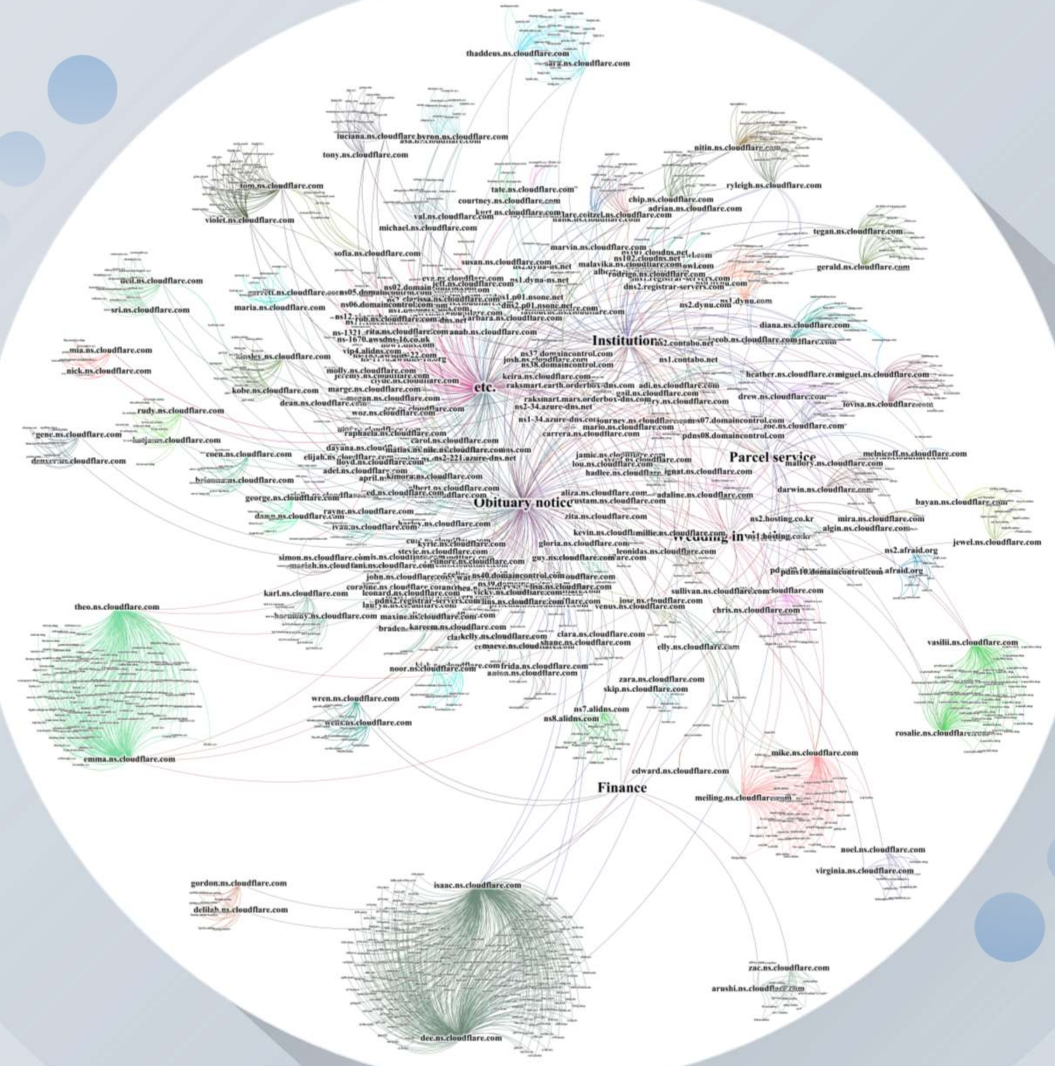
Conducted profiling to identify specific smishing attack groups

- Performed pattern mining analysis by dividing information into Sub domain, Main Domain, Top-Level Domain (TLD), and Path



- Tracked relationships between phishing URLs showing common patterns and their Name Servers (NS)
- Proposed utilizing patterned information from daily generated gTLD and ccTLD (.kr) domains and their registered NS as predictive indicators to proactively block future phishing attacks

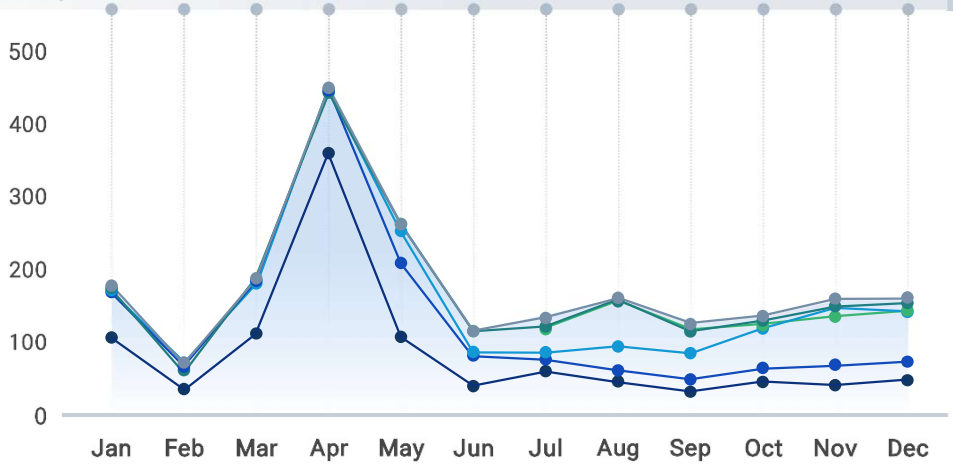
Introduction

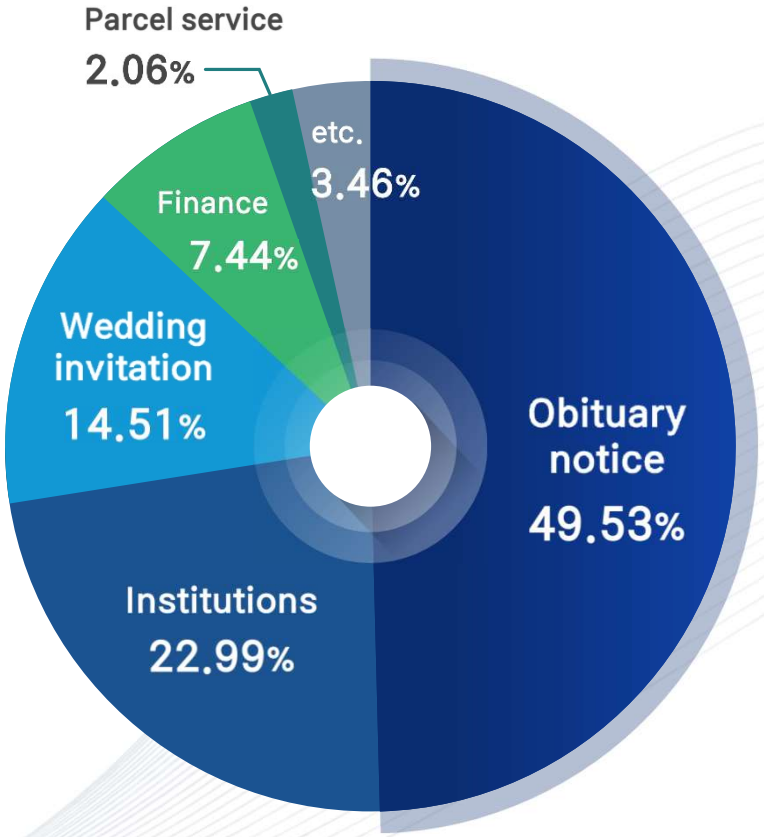


Statistical Analysis and Domain Analysis of Smishing Threats in 2024

Monthly Smishing Incident Count

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Obituary notice	112	35	116	361	112	41	61	46	33	48	44	49	1,058
Institutions	56	21	67	78	100	41	18	17	17	23	26	27	491
Wedding invitation	5	-	1	-	39	1	10	31	38	50	65	70	310
Finance	-	1	-	-	12	18	30	66	31	-	-	1	159
Parcel service	2	-	-	5	-	-	2	-	-	9	16	10	44
etc.	3	5	2	6	5	8	16	3	5	7	8	6	74
Total	178	62	186	450	268	109	137	163	124	137	159	163	2,136



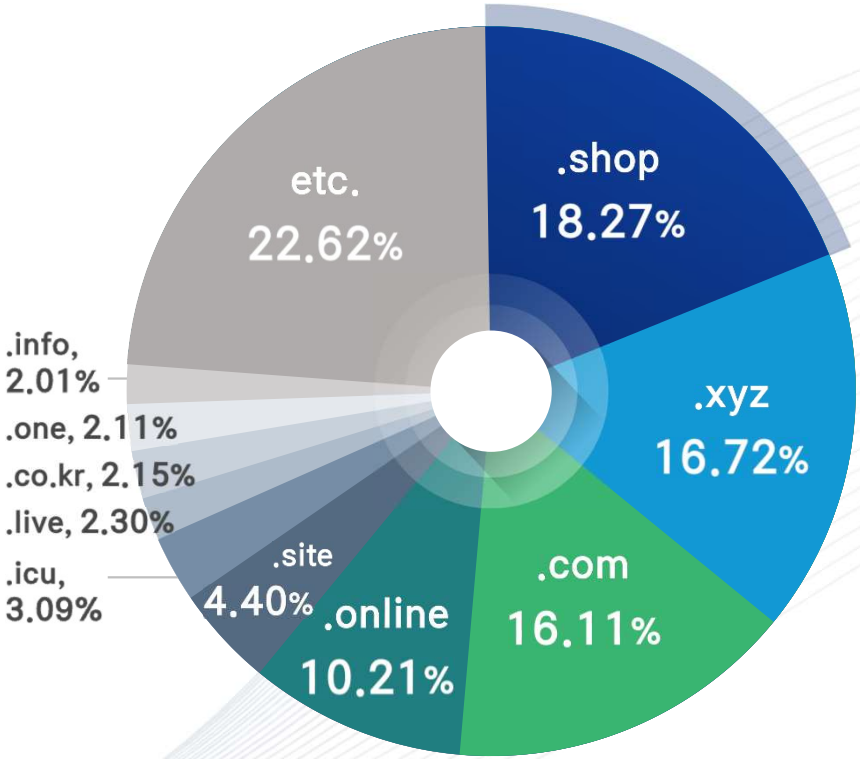


Statistical Analysis and Domain Analysis of Smishing Threats in 2024

Top 10 TLD Statistics Used in Smishing URLs

- 2,040 domains (95.50%) used gTLD

TLD	Types	Count	Ratio	TLD	Types	Count	Ratio
.shop	gTLD	390	18.27%	.bond	gTLD	23	1.08%
.xyz	gTLD	357	16.72%	.art	gTLD	20	0.94%
.com	gTLD	344	16.11%	.org	gTLD	20	0.94%
.online	gTLD	218	10.21%	.buzz	gTLD	19	0.89%
.site	gTLD	94	4.40%	.world	gTLD	18	0.84%
.icu	gTLD	66	3.09%	.store	gTLD	18	0.84%
.live	gTLD	49	2.30%	.run	gTLD	14	0.66%
.co.kr	ccTLD	46	2.15%	.bar	gTLD	14	0.66%
.one	gTLD	45	2.11%	.mom	gTLD	11	0.52%
.info	gTLD	43	2.01%	.yachts	gTLD	10	0.47%
.life	gTLD	43	2.01%	.app	gTLD	10	0.47%
.cyou	gTLD	34	1.59%	.sbs	gTLD	9	0.42%
.kr	ccTLD	32	1.50%	.cfd	gTLD	9	0.42%
.top	gTLD	31	1.45%	.boats	gTLD	8	0.37%
.today	gTLD	26	1.22%	etc.	-	115	5.38%



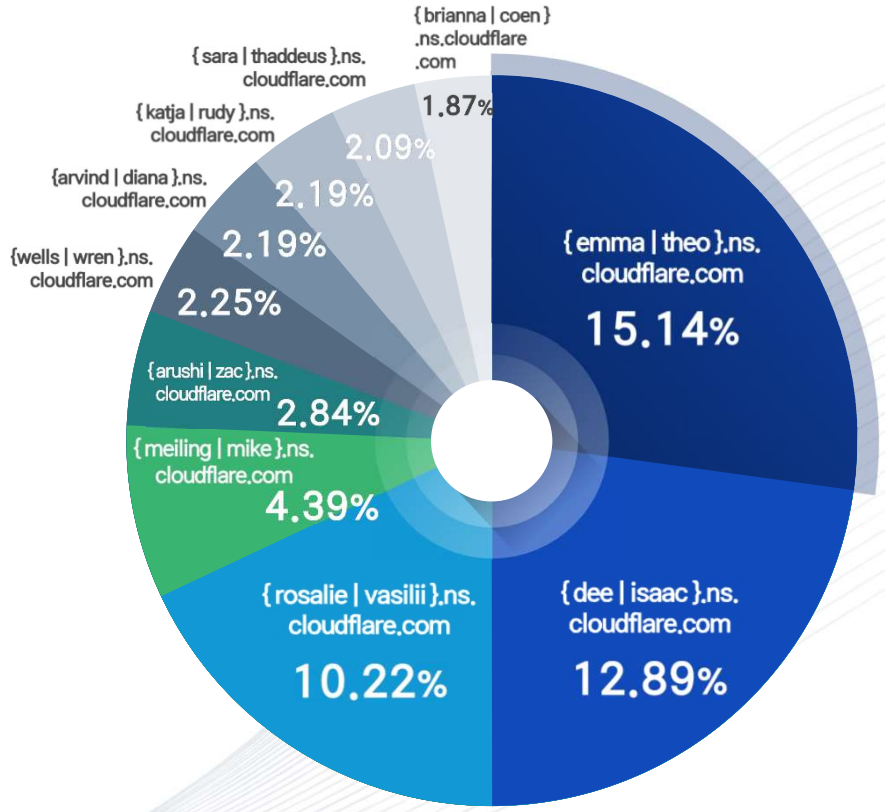
Statistical Analysis and Domain Analysis of Smishing Threats in 2024

Top 10 NameServer Statistics Registered in Smishing URLs

- Cloudflare was the most utilized NameServer with 3,736 cases (87.45%)
  - Registered as NameServers in pairs of two

Nameserver	Country	Count	Ratio
cloudflare.com	US	3,736	87.45%
azure-dns.net	US	147	3.44%
dynu.com	US	86	2.01%
alidns.com	US	46	1.08%
afraid.org	US	20	0.47%
nsone.net	SG	16	0.37%
domaincontrol.com	US	16	0.37%
hosting.co.kr	KR	14	0.33%
orderbox-dns.com	JP	10	0.23%
contabo.net	DE	8	0.19%

- Focused analysis on URLs registered with Top 3 NameServers

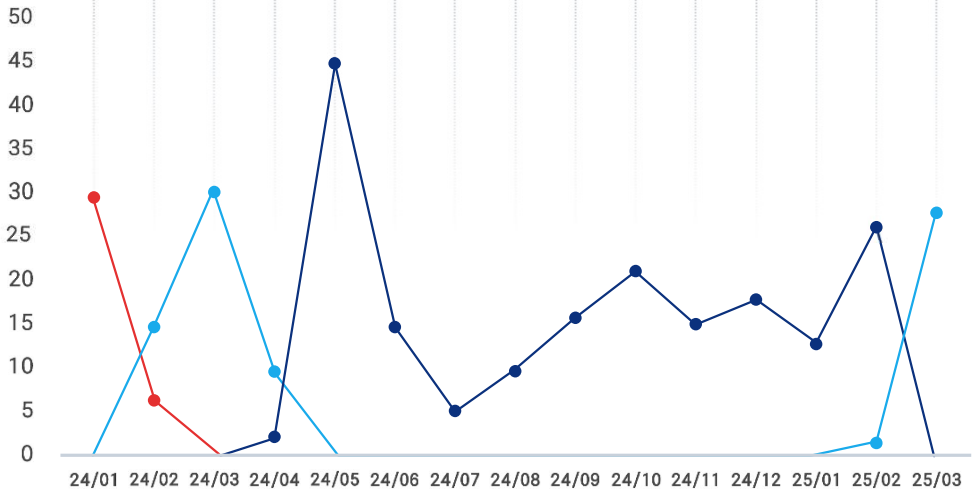


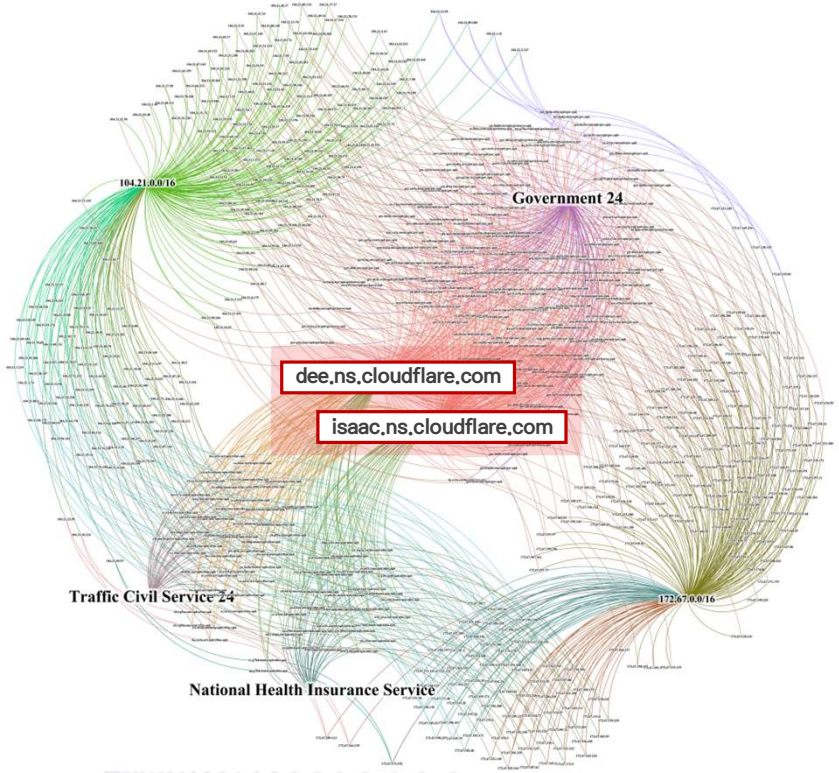
Relationship Analysis Using NS and Smishing URL Pattern Mining

Relationship Analysis of Government Agency Impersonation Smishing URLs and NS

- 241 domains registered to { dee | isaac }.ns.cloudflare.com
- Time series analysis of government agency impersonation based on monthly incident counts

	24/01	24/02	24/03	24/04	24/05	24/06	24/07	24/08	24/09	24/10	24/11	24/12	25/01	25/02	25/03
National Health Insurance Service	29	6	-	-	-	-	-	-	-	-	-	-	-	-	-
Traffic Civil Service 24	-	14	30	9	-	-	-	-	-	-	-	-	-	1	27
Government 24	-	-	-	2	44	14	5	9	16	22	15	18	13	26	-



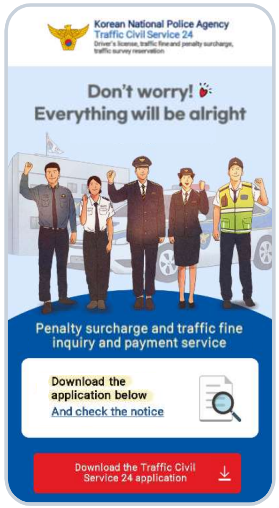


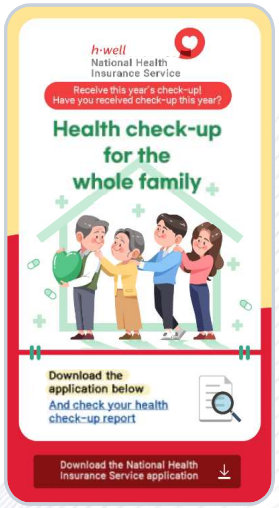
Relationship Analysis Using NS and Smishing URL Pattern Mining

Pattern Analysis of Government Agency Impersonation Smishing URLs

- URL patterns composed of path information combinations that impersonate agencies
  - Domain Pattern – {*}.{^[a-z0-9]{4}$}.{TLD}/apk/{impersonated_name}.apk

Date	Smishing	Phishing URL
2024-01-02	[*The건강보험]신체검사 진단서 전송완료.내용보기 http://lzv.bn2g.yachts	lzv.bn2g.yachts/apk/nhis.ap
2024-01-02	[*건강지키미]건강검사 진단서 전송완료.내용보기 http://vizo.m2gs.hair	vizo.m2gs.hair/apk/nhis.apk
2024-01-02	2023년 개인 건강검사진단서 전송완료.내용보기 http://ibe.gh7w.yachts	ibe.gh7w.yachts/apk/nhis.apk
-	-	-
2024-02-20	[민원24(이파인)]교통법위반 벌점 통지서(발송)내용확인 http://efs.tg9m.one	efs.tg9m.one/apk/efine.apk
2024-02-20	[*교통민원24(이파인)] 교통법위반 과태료 고지서부과(발송) 내용확인 http://yic.qs6t.one	yic.qs6t.one/apk/efine.apk
2024-02-20	[민원24(이파인)]교통법위반 벌점 통지서(발송)내용확인 http://efc.tg9m.one	efc.tg9m.one/apk/efine.apk
-	-	-
2024-04-28	[민원24] 법적기준초과로 민원접수되셨습니다.접수내용: http://yb.eu5n.sbs	yb.eu5n.sbs/apk/gov.apk
2024-04-29	[*민원24] 법적기준초과로 민원접수되셨습니다. 접수내용: http://yc.az1d.sbs	yc.az1d.sbs/apk/gov.apk
2024-05-01	[Web발신] {*정부24} 법적기준초과로 민원접수되셨습니다. 접수내용: http://bc.an1k.sbs	bc.an1k.sbs/apk/gov.apk
-	-	-
2024-11-07	[국외발신][교통경찰]교통법위반(신호위반)범칙금청구 내용발송되었습니다.내용확인: http://gov.kn1d.lat	gov.kn1d.lat/apk/govkorea.apk
2024-11-08	[국외발신][교통경찰]교통법위반(신호위반)범칙금청구 내용발송되었습니다.내용확인: http://gov.kn1d.lat	gov.bh2g.lat/apk/govkorea.apk
2024-11-09	국외발신][교통24]교통법위반(신호위반)사실확인 내용이 발송되었습니다.내용보기: http://gov.as1k.icu	gov.as1k.icu/apk/govkorea.apk
-	-	-



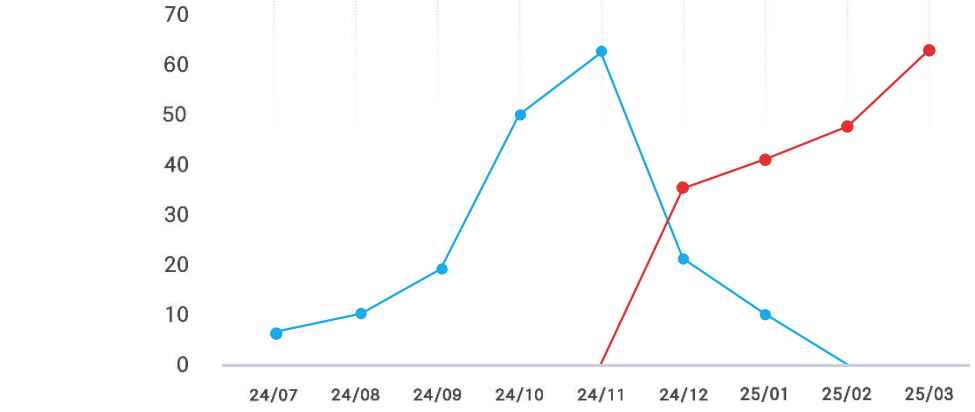


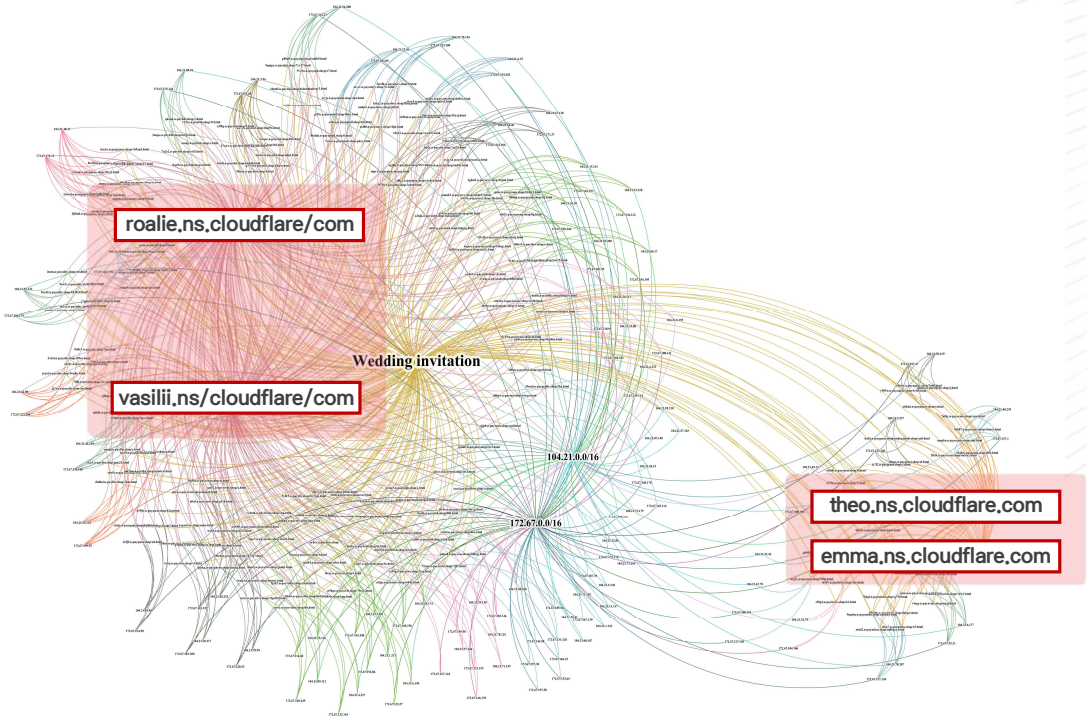
Relationship Analysis Using Pattern Mining of NS and Smishing URLs

Relationship Analysis of Wedding Invitation Impersonation Smishing URLs and NS

- 205 domains registered to [{ rosalie | vasilii }, { emma | theo }].ns.cloudflare.com
- Time series trends of NameServers that registered wedding invitation impersonation domains

	24/07	24/08	24/09	24/10	24/11	24/12	25/01	25/02	25/03
{ rosalie | vasilii } .ns.cloudflare.com	7	10	19	50	62	21	10	-	-
{emma | theo } .ns.cloudflare.com	-	-	-	-	-	35	40	47	62



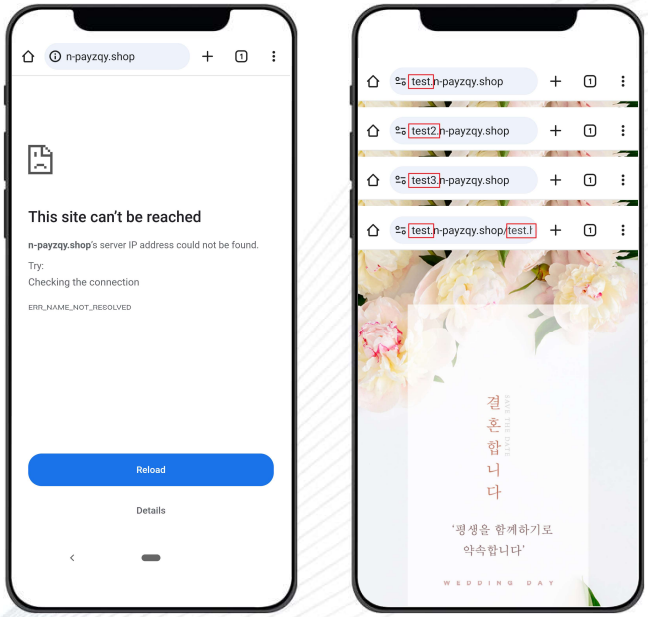


Relationship Analysis Using Pattern Mining of NS and Smishing URLs

Relationship Analysis of Malicious App Distribution Sites Impersonating Wedding Invitations with Brand Name Domains

- Brand-Squatting impersonating N-Pay brand and Phishing URLs utilizing RDGAs
- Domain Pattern – {*}.n-pay{*}.shop/{*}

Date	Smishing	Phishing URL
2024-07-22	23일 제 자녀의 결혼식장에 여러분을 초청합니다 주소 : https://lihi.cc/kXqY1[M1]	9bbaa.n-payefof.shop/f.html
2024-07-23	25일 제 자식의 결혼식장에 여러분을 초청합니다 식장: https://tinyurl.com/dkjfi22	bosn9.n-payefof.shop/0ci.html
2024-07-25	27일 제 자식의 결혼식장에 여러분을 초청합니다 식장: https://lihi.cc/JpeIN	7xk7j.n-payefof.shop/fmg9w.html
2024-07-25	26일 {이두성}님 자식의 결혼식장에 여러분을 초대합니다 주소 : https://tinyurl.com/fefIle6	47yuw.n-payefof.shop/npyslb.html
2024-07-27	29일 [김부월]님 자식의 결혼식장에 여러분을 초청합니다 식장: t.ly/8JRVq	mcsiw.n-payefof.shop/mtjd.html
2024-07-29	26일 제 자녀의 결혼식장에 여러분을 초대합니다 주소: https://tinyurl.com/3dnk5p74	q17y9.n-payefof.shop/kfsnw.html
2024-07-30	[31일 제 자식의 결혼식장에 여러분을 초대합니다 주소: https://psce.pw/69v3tu	fw6ft.n-payefof.shop/klch4l.html
2024-07-30	[8월1일 전창호님 자녀의 결혼식장에 여러분을 초청합니다 식장: https://lihi.cc/9bQhr	e3f9q.n-payefof.shop/9.html
2024-08-02	31일 최기종님 자식의 결혼식장에 여러분을 초대합니다 주소: https://psce.pw/69v6cd	6wqac.n-payefof.shop/l0w.html
2024-08-16	둘이 만나 부족함을 채워 하나가 되었어요 자식결혼식 꼭 참석하시길바랍니다 장소:https://buly.kr/9t95n32	j7jn6.n-paylity.shop/ehg.html
2024-08-17	둘이 부족함을 채워 하나가 되었어요 자식결혼식 꼭 참석하시길바랍니다 장소:https://buly.kr/GvlPQ85	d5f7h.n-paylity.shop/lb.html
2024-08-18	둘이 부족함을 채워 하나가 되었어요 자식결혼식 꼭 참석하시길바랍니다 장소:https://buly.kr/3NH4Cx7	h1hhl.n-paylity.shop/3gve.html
2024-08-21	두 사람이 인생이란 여행을 함께 떠나려고 합니다자녀결혼식 꼭 와주시길바랍니다 주소:https://ur0.jp/iqofz	mfzlk.n-paylity.shop/c70.html
2024-08-21	ⓗ22일 고애자 자녀의 결혼식장으로 많이 와주세요 식장: gourl.kr/griee	mb2ax.n-payoncoar.shop/s2rlh.html
2024-08-22	자식 결혼합니다 22일 꼭 저희 결혼식장에 참여 바랍니다 주소:https://alie.kr/9MOqhY2	e0hip.n-paylity.shop/b5u.html
2024-08-22	①24일 유명욱 자녀 결혼식에 초대합니다. 식장 : gourl.kr/fgrs79	z0c9p.n-payoncoar.shop/vr.html
2024-08-24	두 사람 여러분 축복에 사랑을 쌈싸먹으러합니다 꼭 참석하시어 축복해주세요 장소:https://han.gl/n91Of	ps9j5.n-paylity.shop/3g8.html
2024-09-13	♥9월13일자식 결혼식에 소중한 분들을 모십니다♥주소:http://go9.co/XhY	zdri1.n-payicsid.shop/imlgzg.html
2024-09-13	[9월13일 정주희 자식 결혼식에 소중한 분들을 모십니다주소:gourl.kr/FbUMX1	qaikb.n-paynlet.shop/l3c3.html
2024-09-15	♥9월15일 자식 결혼식에 소중한 분들을 모십니다♥주소:http://go9.co/XiO	sjjp0.n-paytecto.shop/zgd.html
2024-09-15	ⓖ17일 노승원 자식 결혼식 축북으로 더욱 빛내주시길 바랍니다 식장: gourl.kr/oD5qwh	x08ps.n-paylike.shop/cgso0.html
2024-09-16	ⓖ18일 한상정 자식 결혼식 축북해주시면 더없이 기쁘겠습니다 식장:gourl.kr/sXWHaz	tyn4e.n-payciall.shop/dflt8.html
2024-09-16	♥9월16일 자식결혼식에 소중한 분들을 모십니다♥꼭 오셔서 축하해주세요 https://tinyurl.com/QDXZ1	qliye.n-payetym.shop/ctt3.html
2024-09-18	ⓖ20일 복가영 자식 결혼식장 축북해주시면 더없이 기쁘겠습니다 식장:gourl.kr/iKQPbt	ou263.n-payciall.shop/vh.html
2024-09-18	♥9월18일 자식결혼식에 소중한 분들을 모십니다♥꼭 오셔서 축하해주세요 주소:https://tinyurl.com/TXRT1	a2tgk.n-payicsid.shop/xkhq.html
2024-09-19	[♥9월19일 자식결혼식에 소중한 분들을 모십니다♥꼭 오셔서 축하해주세요 식장:http://go9.co/Xkk	a19vw.n-payicsid.shop/bll.html



Q1 2025 Proactive Detection Monitoring Results

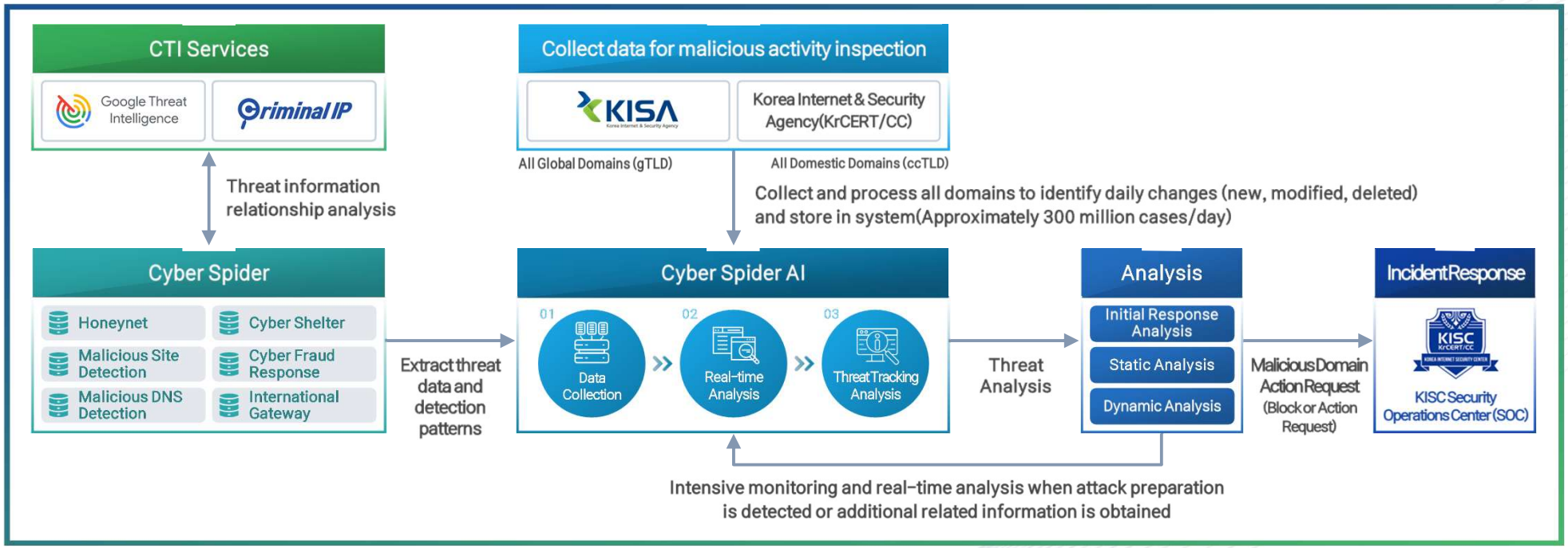
Conducted proactive monitoring on newly generated and collected domains in Cyber-Spider during March 2025

Institutions Phishing URL Pattern

{^[a-z0-9]{4}$}.{TLD} and { dee | isaac }.ns.cloudflare.com

Wedding invitation Phishing URL Pattern

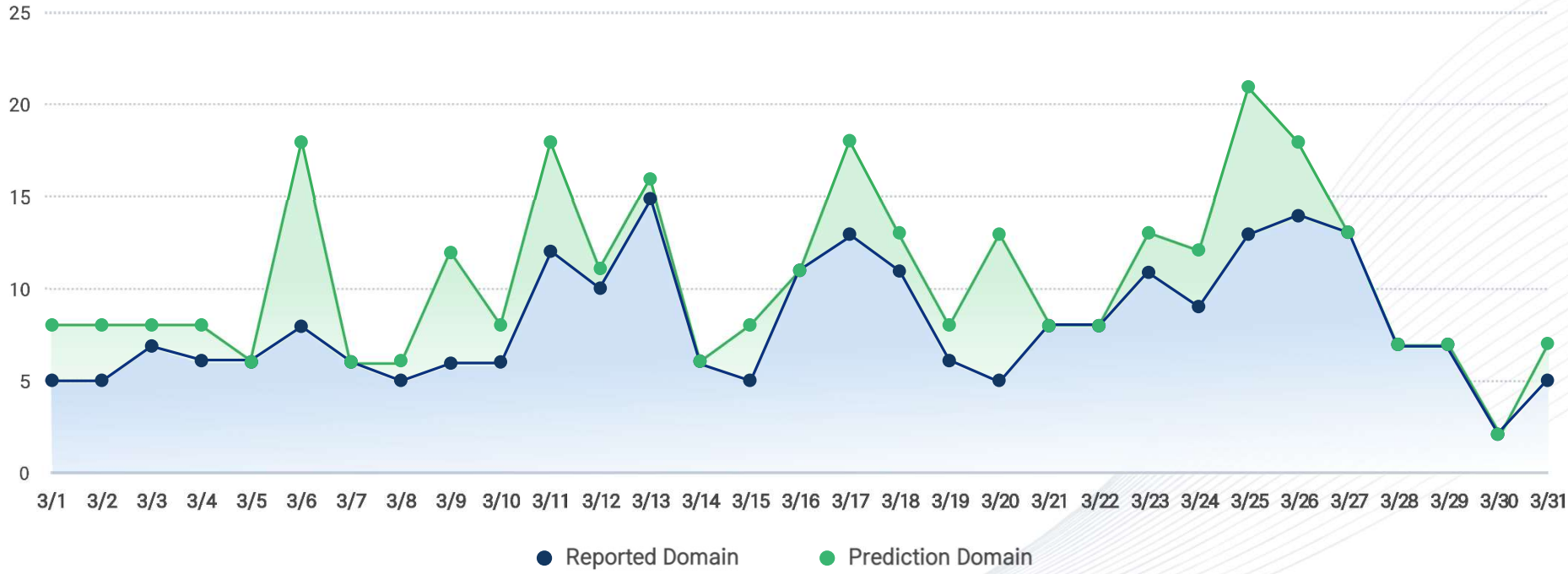
n-pay{*}.shop and { emma | theo }.ns.cloudflare.com



Q1 2025 Proactive Detection Monitoring Results

Proactively detected 326 domains among newly registered domains in March 2025

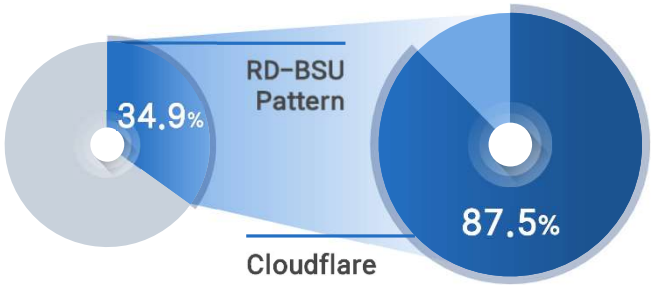
- Average of 10.5 new phishing domains created daily
- Among these, 251 were reported as smishing cases, while 75 unreported domains (23%) were confirmed to be additionally detectable through proactive monitoring



Conclusion

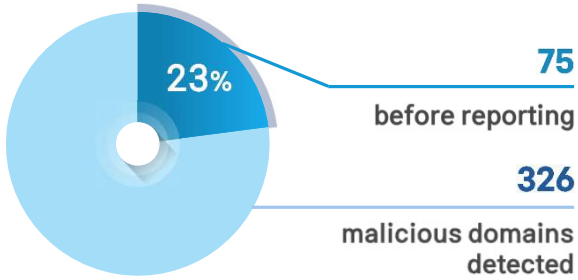
Hybrid RD-BSU Pattern Identified

- 34.9% of smishing domains followed the RD-BSU pattern, among RD-BSU pattern domains, 87.5% were hosted on Cloudflare



Proactive Detection Success

- March 2025: 326 malicious domains detected, 75 (23%) before reporting



Enhanced Real-time Defense and Needed Global Cooperation

- Real-time filtering through Cyber-Spider + telecom blocking integration
- Enhanced threat intelligence sharing and response coordination with national cybersecurity agencies needed

Future Directions

01 Advanced ML/DL Models	02 Broader Threat Coverage	03 Global Partnership
Expand prediction capabilities for new hybrid patterns	Phishing, C2, ransomware analysis expansion	Enhanced CERT collaboration for rapid response systems

Thank you

Prediction of Future Attack Indicators based on the 2024 Analysis of Threats from Malicious App Distribution Sites in South Korea

Kyung Rae Noh (Anthony)

anthonynoh@kisa.or.kr

KISA
Korea Internet & Security Agency