2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

PREDICTION OF FUTURE ATTACK INDICATORS BASED ON THE 2024 ANALYSIS OF THREATS FROM MALICIOUS APP DISTRIBUTION SITES IN SOUTH KOREA

Kyung Rae Noh[1], Shinho Lee[2], Eui-Tak Kim[2], Yujin Shim[1], Jonghwa Han[1] & Jung-Sik Cho[1]

[1]Korea Internet & Security Agency, South Korea

[2]Gachon University, South Korea

anthonynoh@kisa.or.kr
lee1029ng@gachon.ac.kr
kingket@gachon.ac.kr
luvtdw@kisa.or.kr
jhhan@kisa.or.kr
jungsik@kisa.or.kr

ABSTRACT

With cyber threats rapidly increasing, early detection of signs of attack and swift identification of attackers' motives and targets are gaining ever greater importance.

Previously, the Korea Internet & Security Agency (KISA) faced challenges in performing in-depth threat analyses and correlation across data collected by individually operated detection systems, and significant reliance was placed on specialized personnel. In order to overcome these limitations, KISA's Digital Incident Detection Team launched the Cyber-Spider project in 2022. This project integrates normalized data from various detection systems into a centralized data lake and performs automated correlation analyses to proactively detect and respond to emerging cyber threats.

In this study, the patterns of malicious URLs used in various smishing attacks were analysed through pattern mining and tracking based on 10,358,700 smishing-related data points reported to Cyber-Spider in 2024 (text messages, phishing URLs, malicious app distribution URLs, etc.). This paper proposes a method of pre-detecting future phishing attacks and using the results as predictable indicators targeting domains created and collected on a daily basis through Cyber-Spider and registered nameservers (NSs) based on patterns analysed through the application of sub-domain and path combination.

1. INTRODUCTION

Early detection of signs of attack and swift identification of attackers' motives and targets are becoming ever more important. In particular, phishing attacks – which seek to deceive users through socially engineered messages – steal personal details or financial information via various platforms including email, voice and SMS. According to Korea Internet & Security Agency (KISA) statistics, the number of incidents of smishing (a type of phishing attack involving SMS) in Korea has increased rapidly since 2023, exhibiting an increasing trend each year [1]. To detect and respond to cyber attacks, KISA's Digital Incident Detection Team has been promoting the Cyber-Spider project since 2022. It implements the pre-emptive detection of and response to cyber threats through integrated storage of normalized data obtained from detection systems operated by KISA and automated relationship analysis based on the stored data.

SMS phishing attacks often utilize frequently accessed information such as that of specific brands, government or finance-related institutions, or family and friends to gain users' trust and encourage their interaction. The phishing URL included in the message and distributed to multiple users uses a domain name generated using a combination of a brand or organization name familiar to users and a registered domain generation algorithm (RDGA), which seeks to create and register a large number of domains in a short period of time [2]. This hybrid attack technique is defined as registered domain-brand squatting URL (RD-BSU). Unlike traditional random-number-based domain generation algorithms (DGAs) [3], the RD-BSU technique generates domain names and URLs in a format that enables easy recognition by people. Attackers register them with a nameserver (NS) and use them for malicious content distribution. This characteristic makes detection using existing DGA detection models difficult, increasing the likelihood of bypassing blacklist-based response systems.

With respect to smishing attacks that have recently occurred in Korea, this study categorized impersonation scams using social engineering techniques (financial fraud, impersonation of public organizations, fake obituary notices, wedding invitations, parcel delivery, etc.) based on 10,358,700 smishing-related data points collected by Cyber-Spider in 2024 (text messages, phishing URLs, malicious app distribution URLs, etc.). Then, for the malicious app distribution URLs falling under each impersonation type, information was divided into sub-domain, main domain and top-level domain (TLD), and path and pattern mining analysis was conducted. In addition, by investigating the nameservers the phishing URLs were registered with, the relationship between the phishing URLs and nameservers displaying a common pattern was analysed. This paper proposes a method of applying a pre-patterned sub-domain and path combination to the gTLDs and ccTLDs (.kr) generated and collected on a daily basis through Cyber-Spider and the registered nameservers, and consequently blocking future phishing attacks pre-emptively, using the data as predictable indicators.

The rest of this paper is organized as follows: section 2 details the Cyber-Spider project promoted by KISA's Digital Incident Detection Team. Section 3 presents the results of statistical analysis on the TLDs and nameservers of domains used as phishing URLs in smishing attacks, along with the statistics on smishing reported to Cyber-Spider in 2024. Section 4 explains (based on the statistics presented in the previous section) the results of pattern analysis for the normalized and mass-produced phishing URLs among those collected, and the results of relationship analysis for the domains and their nameservers. Section 5 presents a method for predicting phishing domains to be generated in 2025 and the verification results, based on the pattern mining analysis results from the previous section. Finally, our conclusion is presented along with details of future studies.

2. CYBER-SPIDER PROJECT

KISA's Digital Incident Detection Team carries out operations to detect and respond to cyber attacks and threats occurring across the ICT infrastructure of the Republic of Korea. In the past, individual detection systems in various fields – such as network, web and mobile – were operated for cyber attack detection. However, there were limitations in terms of effective

incident detection and response. In particular, there was a significant difficulty in being able to use tracked data (such as the infrastructure, etc. used in the attacks, as well as the attackers' strategies and motives) as a basis for predictions and pre-emptive response. To overcome these difficulties, KISA's Digital Incident Detection Team developed the Cyber-Spider project. Through the integrated storage, in a data lake, of information collected by the individual threat detection systems specializing in the various ICT fields (web, network, mobile device), this project provides a foundation for relationship analysis among the accumulated threat data.

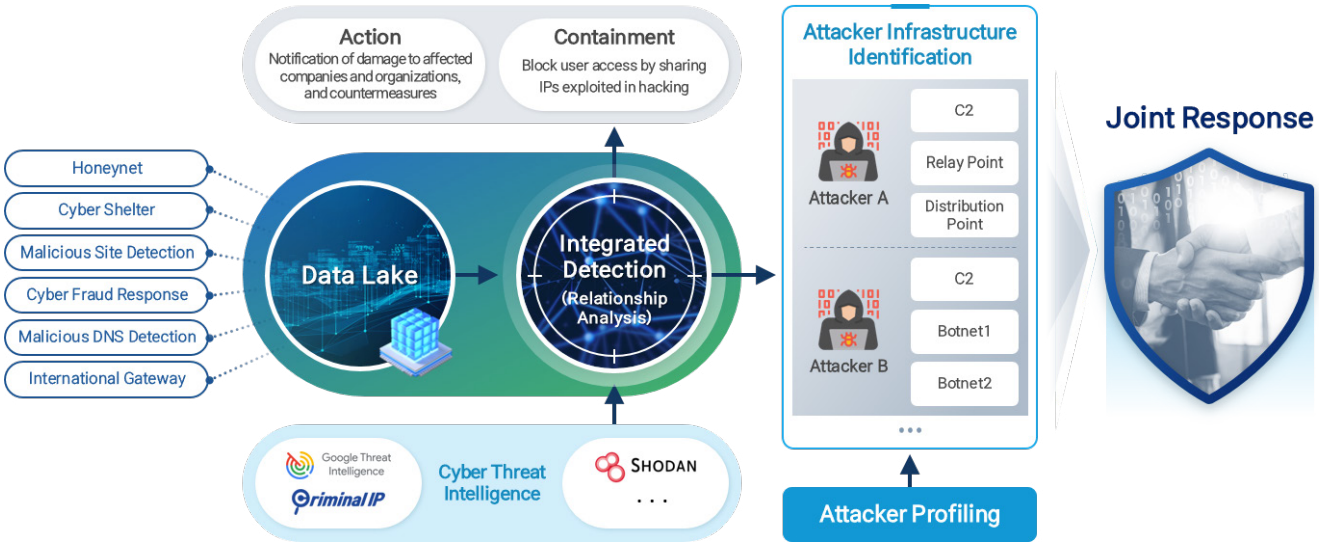

Figure 1: Cyber-Spider flowchart.

The detection systems in each field individually inspect malicious acts and collect a wide range of threat information, such as malicious and suspicious IPs and URLs, attack situation, and C2 server details. These systems also attain additional threat information by cooperating with various cyber threat intelligence (CTI) services both in Korea and abroad, as well as domestic and overseas information and investigation agencies and mobile network operators. Based on the accumulated data, attacks targeting domestic ICT infrastructure can be identified through relationship analysis. The intents and targets of the identified attackers or attack groups are analysed, and – based on the result – swift actions can be taken and security notices sent to the relevant domestic institutions and enterprises. At the same time, by immediately blocking the IPs and domains that have been clearly identified as malicious through cooperation with domestic mobile network operators, damages caused by cyber attacks are prevented. Moreover, information on cyber attacks and threats detected through Cyber-Spider is shared with various domestic and international public organizations and global security companies in real time, and a common response system to prevent the spread of damages across the globe is established.

In this study, an in-depth analysis was conducted on smishing attacks that occurred in the Republic of Korea in 2024 and the phishing URLs included in those attacks, using information collected through Cyber-Spider. Based on the insight obtained from the analysis, this paper explains the analysis process for domains that appear to be specified for future smishing attacks.

3. STATISTICS AND DOMAIN ANALYSIS FOR SMISHING THREATS IN 2024

This section presents the results of statistical analysis of smishing attacks that occurred in the Republic of Korea in 2024 and the phishing URLs used in those attacks. Based on a total of 2,136 data points obtained through the integration of data from 10,358,700 text messages and final phishing URLs reported to Cyber-Spider after removal of redundant values, the results of statistical analysis on the data are presented and interpreted, including the results of an analysis conducted on the TLDs used in the domains of the phishing URLs and the results of statistical analysis of nameservers associated with the domains. Figure 2 shows the results of a relationship analysis conducted on the nameservers of the 2,136 phishing URLs by category as reported to Cyber-Spider in 2024.

Smishing message statistics

The smishing attacks reported to Cyber-Spider in 2024 were designed to encourage users – using social engineering techniques – to install malicious apps. We divided these attacks broadly into five categories according to the theme of social engineering they used: financial fraud, institutional impersonation fraud, obituary notices, wedding invitations, and parcel delivery. Figure 3 shows the distribution of the smishing attacks among the five categories.

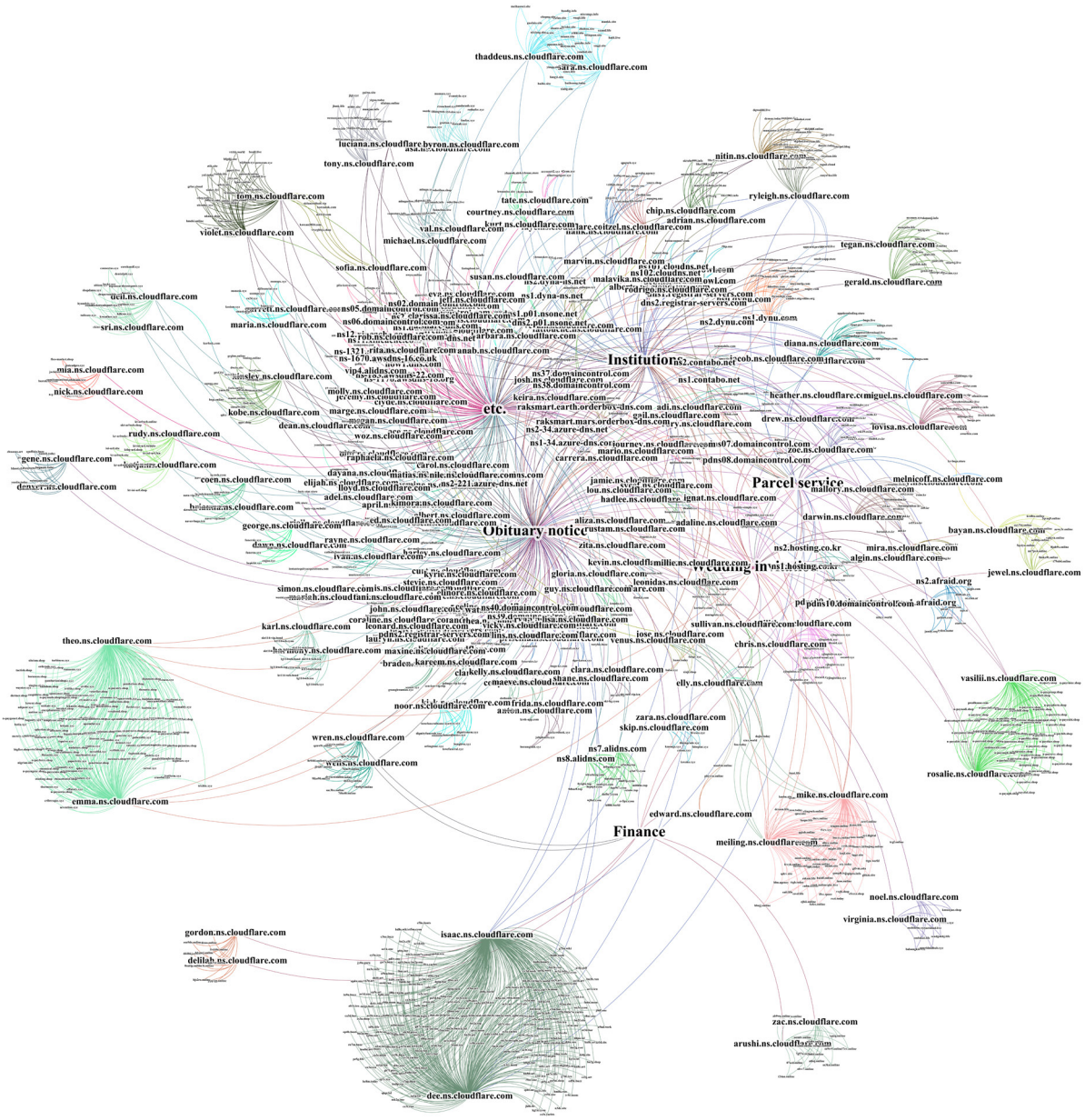

Figure 2: Results of relationship analysis of 2,136 phishing URLs and nameservers by category as reported to Cyber-Spider in 2024.

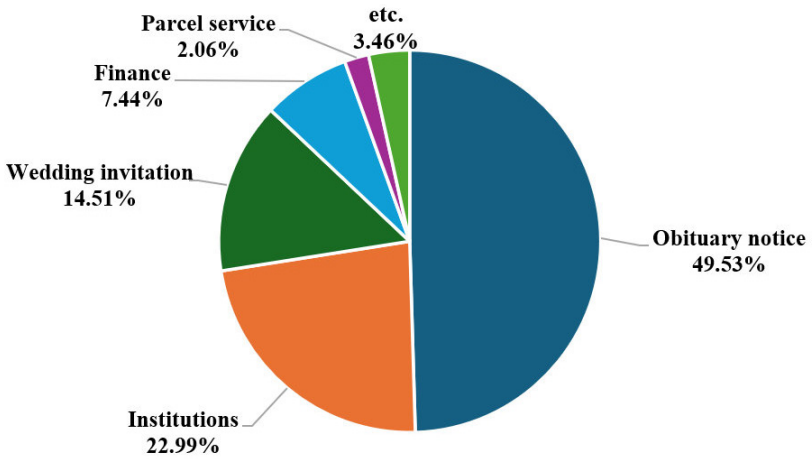

Figure 3: Smishing attacks by category in 2024.

The category with the largest share was obituary notices, which accounted for 1,058 out of 2,136 URLs (49.53%); next was institutional impersonation with 491 URLs (22.99%), followed by wedding invitation impersonation with 310 URLs (14.51%), financial fraud with 159 URLs (7.44%), and parcel delivery-related impersonation with 44 URLs (2.06%). Table 1 shows the number of smishing attacks that occurred in each of the five categories per month.

Category	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	1058
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**	**2136**

Table 1: Number of smishing occurrences by month.

As shown in Table 1, obituary notice and institutional impersonation smishing attacks occurred continuously between January and December. The wedding invitation impersonation started in May, as did financial fraud-related smishing attacks. After September, however, the number of financial fraud attacks dropped off. Figure 4 shows the monthly cumulative distribution of smishing attacks for each of the five categories.

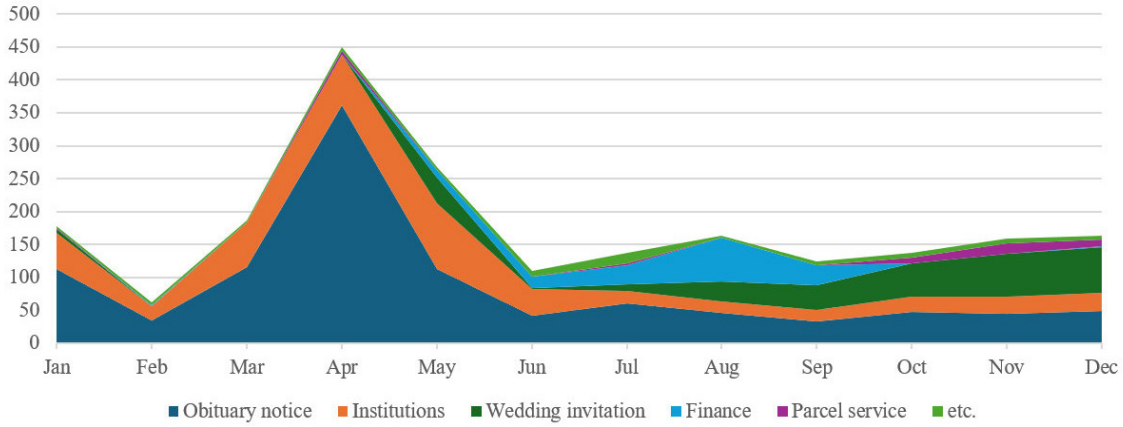

Figure 4: Monthly cumulative smishing distribution by category in 2024.

Top-level domain (TLD) statistics

Next, the TLDs used in the phishing URLs included in the smishing attacks were analysed. A total of 79 TLDs were used across the 2,136 URLs. The most frequently used TLD was .shop, which was used 390 times (18.27%), followed by .xyz (357 times, 16.72%) and .com (344 times, 16.11%). Figure 5 shows the ten most frequently used TLDs.

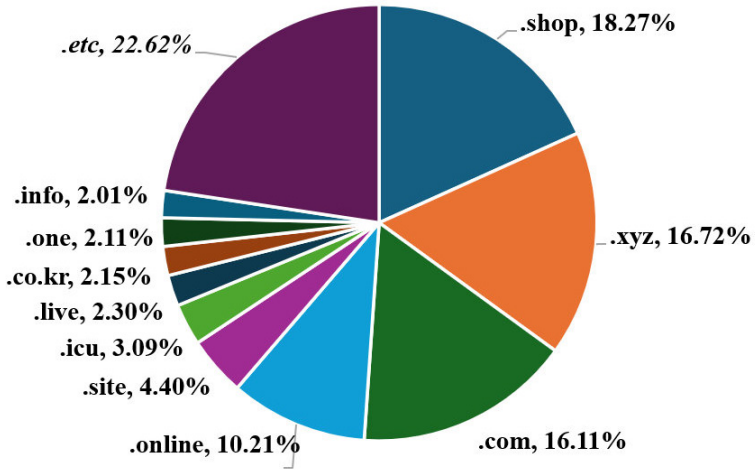

Figure 5: The top 10 TLDs used in the URLs of malicious app distribution sites.

As a result of investigating the TLD types in relation to the domains used in phishing URLs, the attackers were found to have used gTLDs for 2,040 out of 2,136 domains (95.50%). For the remaining 96 domains (4.50%), ccTLDs (.co.kr, .kr, .me, .pw, .cc, .is, .com.ar, .tw, .cn, .idv.tw, .si, .at) were used. Table 2 lists the spread of TLD use in the 2,136 phishing URLs.

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%

Table 2: TLD types in the domains of malicious app distribution sites.

Nameserver (NS) statistics

In this section, the statistics on the nameservers associated with 2,136 phishing URLs are explained. *Cloudflare* was the nameserver used most frequently by the phishing URLs (3,736 times, 87.45%). Table 3 shows the nameservers, the respective country information, and the number of registrations by NS.

Nameserver	Country	Count	Ratio	Nameserver	Country	Count	Ratio
cloudflare.com	US	3,736	87.45%	dyna-ns.net	US	4	0.09%
azure-dns.net	US	147	3.44%	xincache.com	CN	2	0.05%
azure-dns.com	CA	147	3.44%	cloudns.net	JP	2	0.05%
dynu.com	US	86	2.01%	duckdns.org	US	2	0.05%
alidns.com	US	46	1.08%	dnsowl.com	US	2	0.05%
afraid.org	US	20	0.47%	dns.com	US	2	0.05%
nsone.net	SG	16	0.37%	share-dns.com	HK	1	0.02%
domaincontrol.com	US	16	0.37%	awsdns-37.org	HK	1	0.02%
hosting.co.kr	KR	14	0.33%	share-dns.net	HK	1	0.02%
orderbox-dns.com	JP	10	0.23%	awsdns-18.org	US	1	0.02%
contabo.net	DE	8	0.19%	awsdns-16.co.uk	HK	1	0.02%
registrar-servers.com	JP	6	0.14%	awsdns-22.com	US	1	0.02%

Table 3: Statistics on nameservers used in malicious app distribution sites.

A noteworthy outcome of an analysis conducted on the *Cloudflare* phishing URLs is that these domains are registered through load balancing with a nameserver consisting of two pairs. These domains were found to have been registered in a total of 1,868 types. Figure 6 shows the top ten nameservers with main domains registered in the form of two pairs.

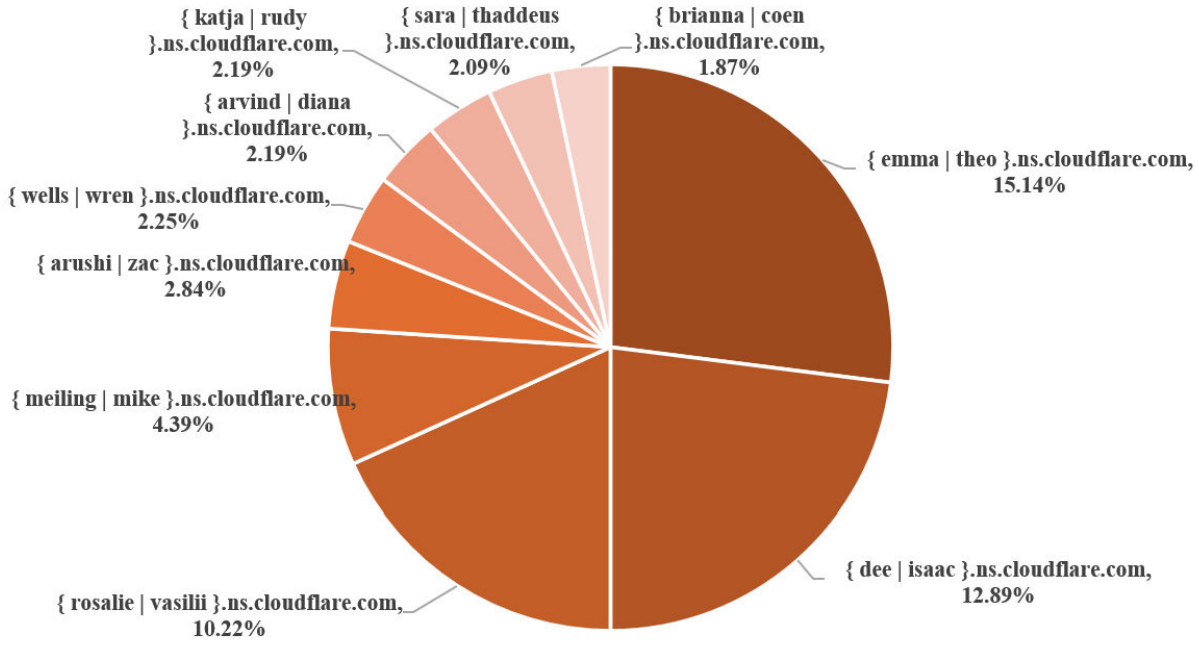

Figure 6: Top 10 Cloudflare nameservers consisting of two pairs.

{ emma | theo }.ns.cloudflare.com was ranked first with 283 registrations (15.14%), followed by { dee | isaac }.ns.cloudflare.com with 241 registrations (12.89%) and { rosalie | vasilii }.ns.cloudflare.com with 191 registrations (10.22%).

In the following section, a relationship analysis is conducted on the phishing URLs registered to the top three *Cloudflare* nameservers: [{ emma | theo }, { dee | isaac } and { rosalie | vasilii }].ns.cloudflare.com. Then, based on the analysis, we present the results of a pre-inspection conducted on the domains newly generated and collected by Cyber-Spider.

4. RELATIONSHIP ANALYSIS USING NAMESERVER AND PHISHING URL PATTERN MINING

In this section, we analyse the generation techniques for the domains of malicious app distribution sites through pattern mining on the domains and nameservers of the malicious app distribution sites reported to Cyber-Spider in 2024. All of the reported domains were generated using a technique similar to that of RDGAs registered to the nameservers. For some of the domains, the brand-squatting technique appeared to have been used concurrently to achieve fast domain generation and make response by detection systems difficult. As the domains specified with the hybrid RD-BSU technique have been found to be those registered in [{ emma | theo }, { dee | isaac } and { rosalie | vasilii }].ns.cloudflare.com – which are the nameservers of two pairs explained in section 3 – we present the results of pattern mining analysis on the corresponding phishing URLs.

Relationship analysis of malicious app distribution sites using institutional impersonation in path information

The 241 domains registered in { dee | isaac }.ns.cloudflare.com are URLs with a pattern consisting of the combination of main domain (which appears to have been generated in a format similar to that of RDGAs) and the institutional impersonation path information. The main domain is composed of small English letter + number + small English letter (four digits in all), and is identified to be a phishing URL with the pattern of:

{*}.{***^[a-z0-9]{4}$}.{TLD***}/apk/{***Institution Name***}.apk

Table 4 lists examples showing changes in the patterns of path information for institutional impersonation smishing attacks and the corresponding phishing URLs by each date when such changes started.

Date	Smishing	Phishing URL
2024-01-02	[*The건강보험]신체검사 진단서 전송완료.내용보기 http://lzv.bn2g.yachts	lzv.bn2g.yachts/apk/nhis.apk
2024-01-02	[*건강지키미]건강검사 진단서 전송완료.내용보기 http://vizo.m2gs.hair	vizo.m2gs.hair/apk/nhis.apk
2024-01-02	2023年 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	[국제발신] [교통24]신호위반 사실확인. *벌칙금부과 내용발송되었습니다. 내용확인: http://gov.bh2g.lat	gov.bh2g.lat/apk/govkorea.apk
2024-11-09	[국외발신][교통24]교통법위반(*신호위반)사실확인내용이 발송되었습니다.내용보기: http://gov.as1k.icu	gov.as1k.icu/apk/govkorea.apk

Table 4: Institutional impersonation smishing (National Health Insurance Service, Traffic Civil Service 24, Government 24).

As shown in Table 4, the institutional impersonation URLs have domain names in a format similar to that of RDGAs. However, the URL path is designed to encourage installation of the malicious app by inserting the names of public organizations – such as National Health Insurance Service (nhis), Traffic Civil Service 24 (efine) and Government 24 (gov and govkorea) – into the path (/apk/...), thus giving the appearance of being related to one of these government organizations. In a smishing attack a user may install the malicious app based on a level of trust assumed due to the presence of these brands or institutions in the URL path. Figure 7 shows malicious app distribution sites impersonating each institution (nhis, efine, gov).

Figure 7: Phishing sites impersonating National Health Insurance Service, Traffic Civil Service 24 and Government 24.

As for the TLDs used in the 241 institutional impersonation phishing URLs, the domains were found to have been generated using 45 types. In addition, as shown in Table 5, the domains were found to have been generated mostly by using low-priced TLDs [4]. All of these domains were those registered in { dee | isaac }.ns.cloudflare.com. Figure 8 shows the relationship analysis results of domains registered in { dee | isaac }.ns.cloudflare.com.

TLD	Price	Count	Ratio
.one	$1	26	10.83%
.art	$2	19	7.92%
.icu	$1	17	7.08%
.buzz	$1	16	6.67%
.run	$1	14	5.83%
.bar	$2	13	5.42%
.mom	$1	11	4.58%
.yachts	$1	11	4.58%
.cfd	$1	9	3.75%
.sbs	$1	9	3.75%
.boats	$1	8	3.33%
.work	$2	8	3.33%
.lat	$1	7	2.92%
.life	$1	6	2.50%
.cyou	$1	5	2.08%

TLD	Price	Count	Ratio
.lol	$1	5	2.08%
.me	$2	4	1.67%
.shop	$1	4	1.67%
.wiki	$2	4	1.67%
.beauty	$1	3	1.25%
.info	$3	3	1.25%
.pw	$1	3	1.25%
.site	$1	3	1.25%
.skin	$1	3	1.25%
.top	$1	3	1.25%
.golf	$4	2	0.83%
.hair	$1	2	0.83%
.pics	$1	2	0.83%
.press	$1	2	0.83%
etc.	-	15	6.25%

Table 5: Price and use ratio of each TLD used in institutional impersonation.

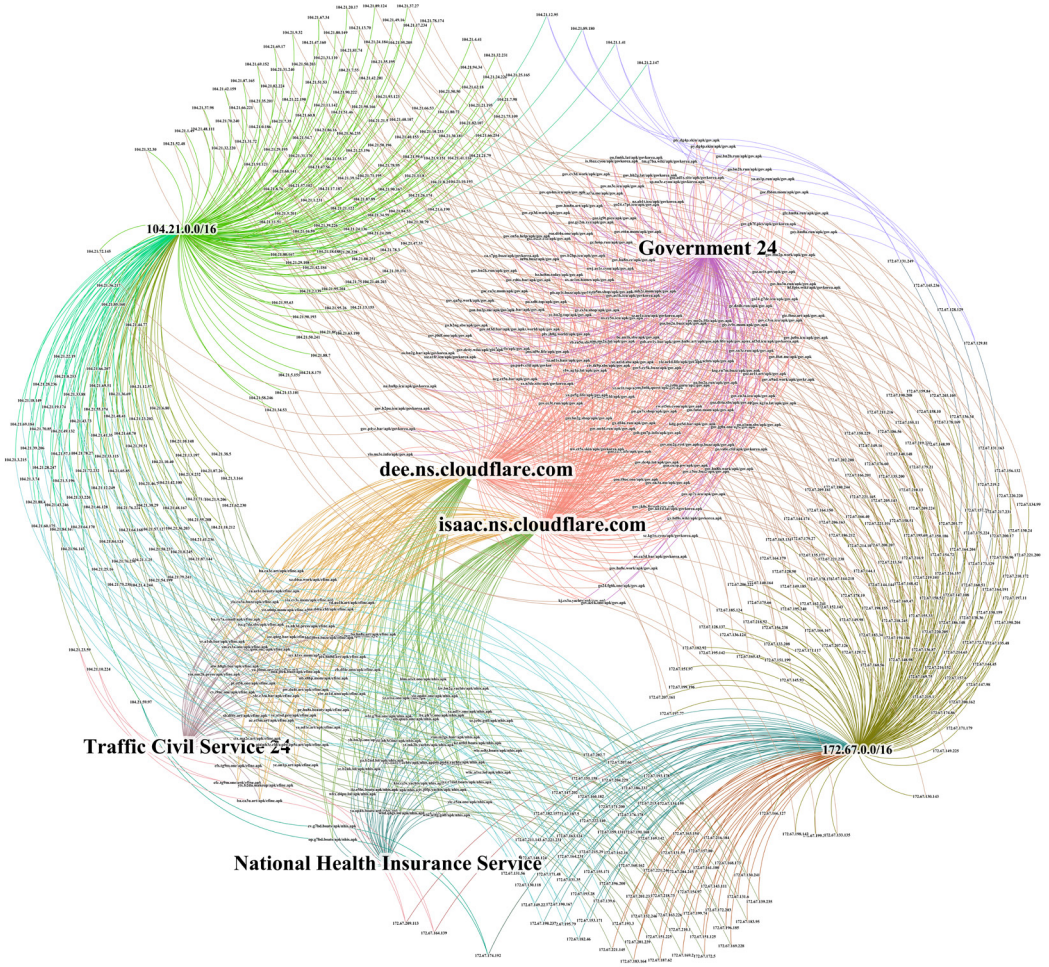

Figure 8: Relationship analysis of institutional impersonation domains registered in { dee | isaac }.ns.cloudflare.com.

Relationship analysis of malicious app distribution sites using wedding invitation impersonation with brand name domains

The phishing URL in the {*}.n-pay{*}.shop/{*} pattern – which started to appear in July – appears to be a domain created using RDGAs and brand-squatting to impersonate a brand called *N-Pay*. It was identified as wedding invitation impersonation smishing. Table 6 shows examples of smishing distribution through generation of URLs using the {*}.n-pay{*}.shop/{*} domain pattern.

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/feflle6	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 되었어요자식결혼식 꼭 참석하시길바랍니다장소:https://buly.kr/9t95n32	j7jn6.n-paylity.shop/ehg.html
2024-08-17	둘이 부족함을 채워 하나가 되었어요 자식결혼식 꼭 참석하시길바랍니다장소:https://buly.kr/GvlPQ85	d5f7h.n-paylity.shop/lb.html
2024-08-18	둘이 부족함을 채워 하나가 되었어요 자식결혼식 꼭 참석하시길바랍니다장소:https://buly.kr/3NH4Cx7	h1hhl.n-paylity.shop/3gve.html
2024-08-21	두 사람이 인생이란 여행을 함께 떠나려고 합니다자녀결혼식 꼭 와주시길바랍니다주소: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 기쁘겠습니다식장:gourl.kr/iKQPbt	ou263.n-payciall.shop/vh.html

Table 6: Wedding invitation impersonation smishing.

Date	Smishing	Phishing URL
2024-09-18	♥9월18일 자식결혼식에 소중한 분들을 모십니다♥꼭 오셔서 축하해주세요주소:https://tinyurl.com/TXRT1	a2tgk.n-payicsid.shop/xkhq.html
2024-09-19	♥9월19일 자식결혼식에 소중한 분들을 모십니다♥꼭 오셔서 축하해주세요식장:http://go9.co/Xkk	a19vw.n-payicsid.shop/bll.html
2024-09-21	자식 결혼합니다 21일 꼭 저희 결혼식장에 참여 바랍니다식장:https://tinyurl.com/BGFCX1	ww7to.n-payorcy.shop/38s.html
2024-09-23	♬24일 제 자식 결혼식에 오셔서 많은 축복과 참여 부탁합니다 식장: gourl.kr/tt5H6	agj8q.n-payplen.shop/95c7d5.html
2024-09-24	↗26일 저의 결혼식에 다들 참석 하셔서 축복 부탁드립니다^^ 식장: gourl.kr/fgr5rr	4r3jq.n-payplen.shop/3s6a9.html
2024-09-25	24일 자식 결혼합니다소중한 자리 꼭 와서 함께 축복해주세요식장:https://tinyurl.com/HGYXZ	4gknd.n-payorcy.shop/4ujod.html

Table 6 contd.: Wedding invitation impersonation smishing.

The URLs in the {*}.n-pay{*}.shop/{*} pattern as listed in Table 6 appear to have been created for one-time use by specific users or to make distribution tracking difficult with sub-domain and path consisting of random characters. Based on a main domain created as shown in Figure 9, however, it can be deduced that the phishing site can be accessed through an attempt using the random characters of sub-domain and path. The use of this method is presumed to be aimed at securing the survival time of phishing sites upon their blocking – generally through control – when a large number of sites are distributed with random sub-domain or path information added.

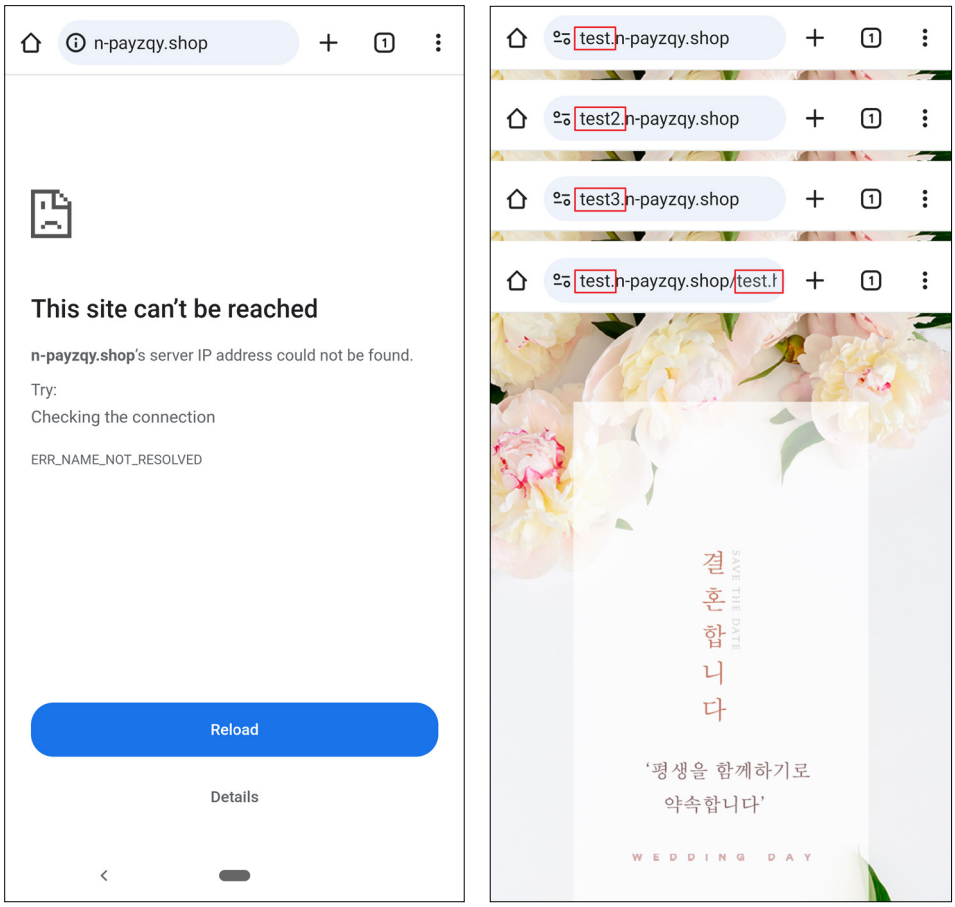

Figure 9: Operational conditions of wedding invitation impersonation phishing sites.

On investigating the registered nameservers of URLs related to 205 wedding invitation impersonation scams reported using the {*}.n-pay{*}.shop/{*} pattern, the domains were found to have been registered to the nameservers [{ rosalie | vasilii } and { emma | theo }].ns.cloudflare.com. 170 domains were found to have been registered to { rosalie | vasilii }.ns.cloudflare.com and 35 to { emma | theo }.ns.cloudflare.com. Figure 10 shows the relationship of the 205 wedding invitation impersonation domains with the {*}.n-pay{*}.shop/{*} pattern.

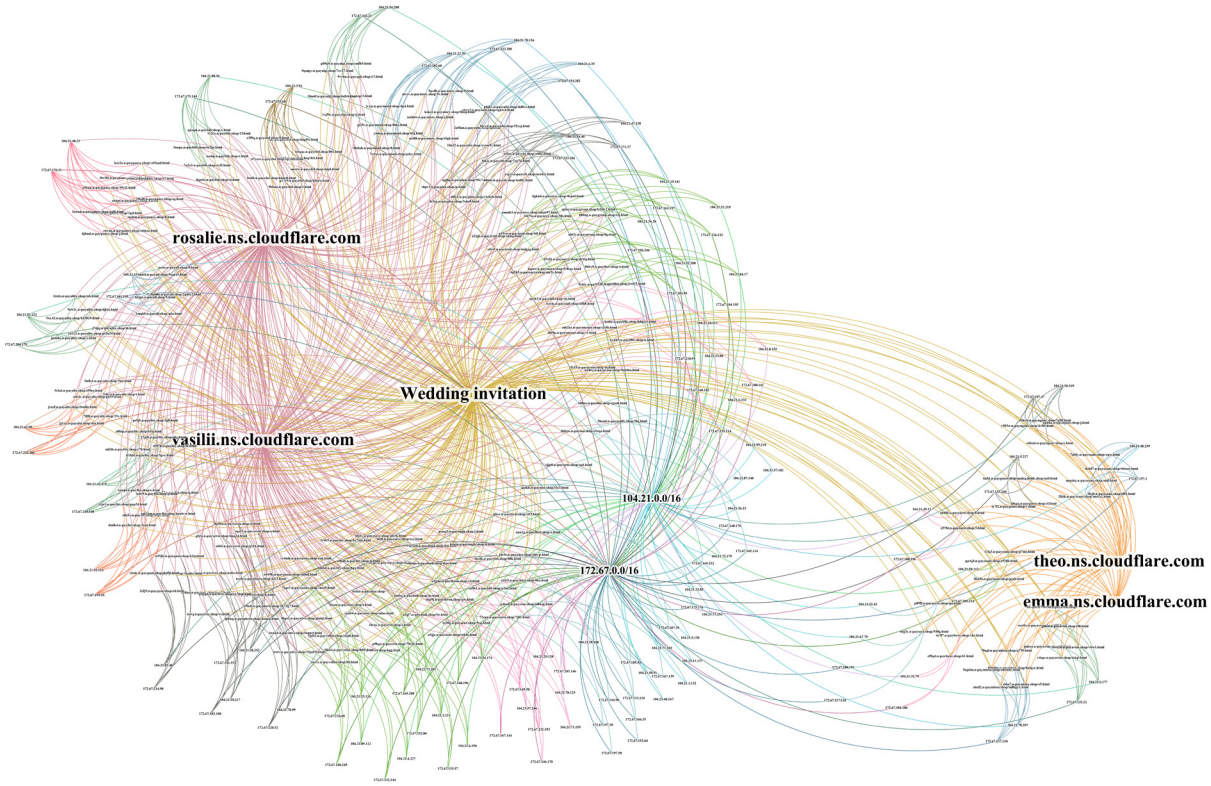

Figure 10: Relationship analysis of wedding invitation impersonation domains registered in [{ rosalie | vasilii } and { emma | theo }].ns.cloudflare.com.

5. PREDICTION OF FUTURE ATTACK INDICATORS IN Q1 2025

In this section, we conduct time series analyses on the trends of institutional impersonation (National Health Insurance Service, Traffic Civil Service 24 and Government 24) and nameservers used to register wedding invitation (*N-Pay*) impersonation domains in 2024 and Q1 of 2025 based on the pattern mining results of the previously analysed phishing sites. In addition, we explain the results of pre-detecting phishing attacks by predicting phishing URLs through pre-inspections on the domains newly generated and collected by Cyber-Spider prior to the domain reports for March 2025, based on the analysed trend for Q1 of 2025.

Figure 11 shows the results of a time series trend analysis of the number of institutional impersonation phishing incidents that occurred each month for each impersonated institution, from January 2024 to March 2025. In January 2024 there were 29 phishing URLs impersonating the National Health Insurance Service; this number gradually decreased until March 2024. At the same time, the number of phishing URLs impersonating Traffic Civil Service 24 increased. From March 2024, however, the number of phishing URLs impersonating Traffic Civil Service 24 decreased. Simultaneously, the number of phishing URLs impersonating Government 24 increased, and attacks impersonating this institution were maintained until February 2025. From February 2025, the number of phishing URLs impersonating Traffic Civil Service 24 once again increased. All of the phishing URLs impersonating the different institutions were found to be registered to the { dee | isaac }.ns.cloudflare.com nameserver, as shown in Figure 12.

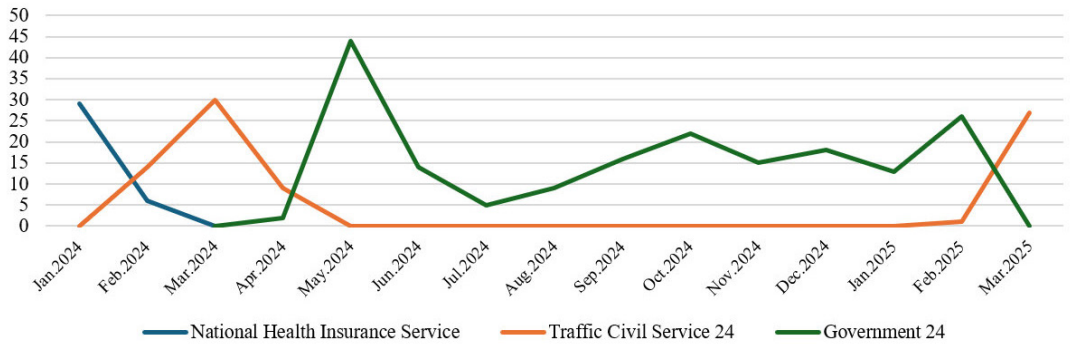

Figure 11: Time series trend for institutional impersonation phishing URLs.

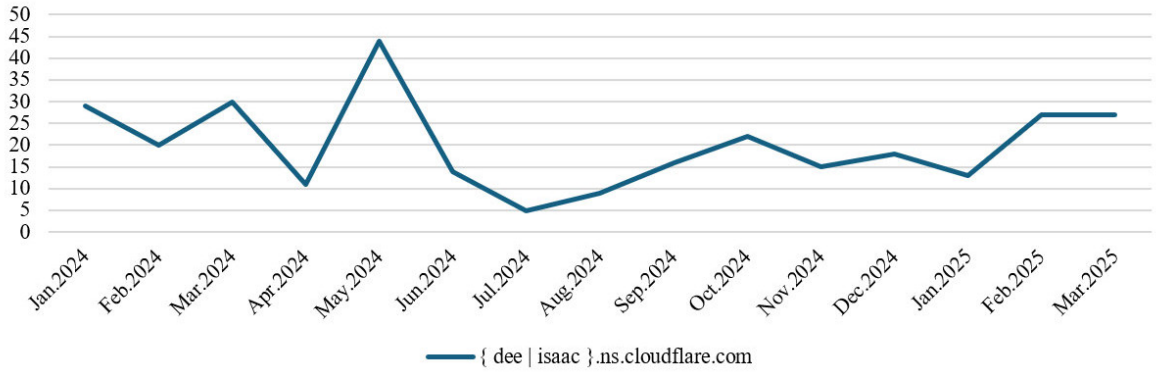

Figure 12: Time series trend of nameservers associated with institutional impersonation phishing URLs.

In the case of the number of phishing URLs in the {*}.n-pay{*}.shop/{*} pattern, which started in July 2024 (wedding invitation impersonation), a steady upward trend was identified, as shown in Figure 13. For this group, as shown in Figure 14, the number of phishing URLs registered to { rosalie | vasilii }.ns.cloudflare.com increased until November 2024 but started to decline gradually thereafter. Phishing URLs registered to { emma | theo }.ns.cloudflare.com first appeared in November 2024 and gradually increased at the same time as URLs registered to { rosalie | vasilii }.ns.cloudflare.com were decreasing. No domain registrations were identified to { rosalie | vasilii }.ns.cloudflare.com after February 2025.

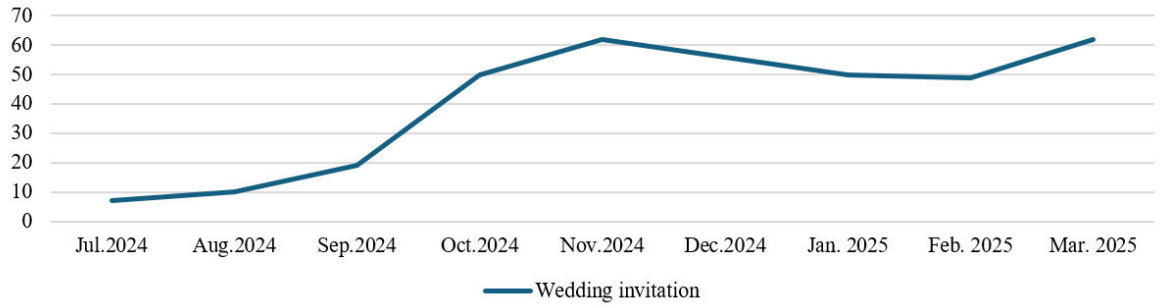

Figure 13: Time series trend for wedding invitation impersonation phishing URLs.

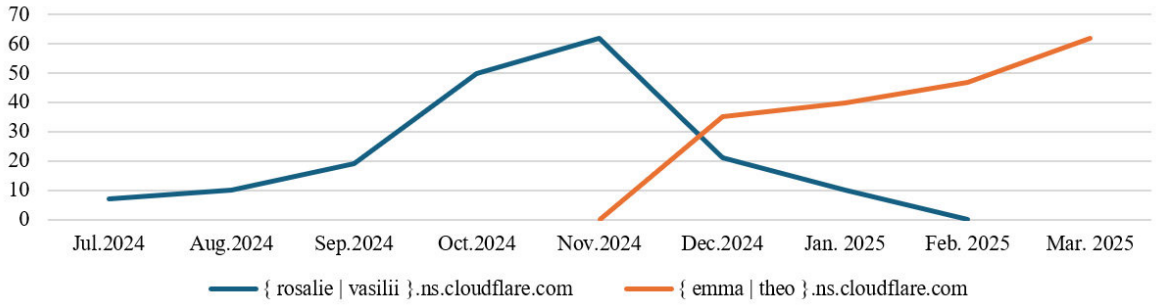

Figure 14: Time series trend of nameservers associated with wedding invitation phishing URLs.

Through the time series analyses, the institutional impersonation phishing URLs were presumed to be the domains registered to { dee | isaac }.ns.cloudflare.com, and the wedding invitation impersonation phishing URLs were found to have completed domain registration by moving the nameserver from { rosalie | vasilii }.ns.cloudflare.com to { emma | theo }.ns.cloudflare.com.

Based on the tracking results, pre-monitoring was conducted on domains newly generated and collected by Cyber-Spider for one month in March 2025 and which had the same patterns as those belonging to the institutional impersonation and wedding invitation impersonation groups. Among the new domains, 326 were detected as malicious app distribution sites and an average of 10.5 new domains were found to have been generated per day. Among these sites, 251 were domains already reported for smishing. However, the remaining 75 (23%) were pre-detected ahead of the domain reports. Figure 15 shows stacked graphs of domains reported to Cyber-Spider and pre-detected domains (before the reports) in March 2025.

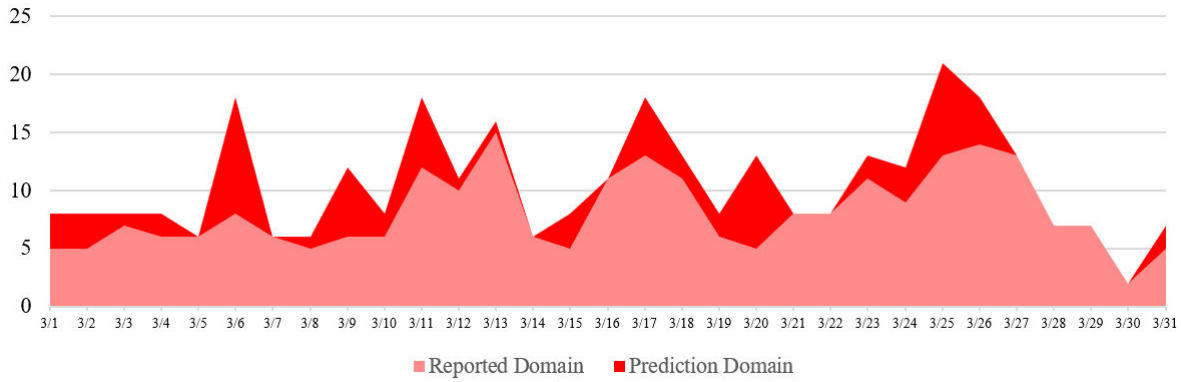

Figure 15: Stacked graphs showing domains reported to KISA and collected by Cyber-Spider, and domains that had been pre-detected before reports.

6. CONCLUSION

In this study, an in-depth investigation was conducted on the domain patterns and registration infrastructure of malicious app distribution sites by analysing 10,358,700 smishing-related data points collected in 2024 through Cyber-Spider. According to the study results, the attackers were using a hybrid-type RD-BSU pattern to combine the characteristics of brand-squatting and RDGAs based on the domains of legitimate institutions or public organizations.

As indicated by the analysis results, the smishing attacks that occurred in Korea in 2024 used a range of social engineering lures such as obituary notices (49.53%), impersonation of public organizations (22.99%), wedding invitations (14.51%), financial fraud (7.44%), and parcel delivery (2.06%). The domains created based on RD-BSU represented approximately 34.9% of all smishing-related data, with 87.45% of these domains concentrated in the *Cloudflare* nameserver. Within *Cloudflare* in particular, the concentration of malicious domains in specific nameservers was detected. Through pattern mining analysis on the domains and nameservers, two key attacks – institutional impersonation and wedding invitation impersonation – were identified. Institutional impersonation scams were concentrated in { dee | isaac }.ns.cloudflare.com, and wedding invitation impersonation scams displayed a pattern of moving from { rosalie | vasilii }.ns.cloudflare.com to { emma | theo }.ns.cloudflare.com. These patterns indicate a possibility of the attacker groups being the same or having a close relationship.

The most noteworthy outcome of this study is the development of a future attack prediction model through domain pattern analysis. Through a pre-inspection of newly created domains in Cyber-Spider for one month, a total of 326 malicious app distribution sites were detected, with detection prior to the actual smishing report succeeding for 75 of them (23%). This is an important outcome in proving the effectiveness of pattern-based prediction.

Based on the study results, KISA's Digital Incident Detection Team is strengthening pre-emptive response to cyber threats by applying the patterned sub-domain and path combination to the domains created on a daily basis using the Cyber-Spider system. In addition, through cooperation with domestic mobile network operators, KISA is keeping citizens' damage to a minimum by immediately blocking the malicious domains detected. KISA is actively sharing the analysis methodology and detection technique developed through this study and the threat information collected in real time with global security companies as well as the relevant organizations in Korea and abroad. In particular, as the RD-BSU-type attacks detected in Korea are highly likely to be spread across borders, KISA is strengthening cooperation with the cybersecurity agencies of major countries such as CISA in the US, JPCERT/CC in Japan, and ENISA in Europe, and building a threat information sharing system through the Asia-Pacific Computer Emergency Response Team (APCERT). Based on partnerships with international security companies, KISA is also contributing to global-level malicious domain blocking and response by swiftly exchanging information on domain registration infrastructure. International cooperation is an essential strategy for effective response to cyber threats that exceed the scope of response of a single nation. KISA aims to contribute to the joint response to cyber crimes committed across international borders and to the establishment of a safer internet environment by sharing the pattern-based prediction model and RD-BSU detection technique developed through this study with global cybersecurity communities.

Directions for future studies include upgrading the prediction model using machine learning and deep-learning-based techniques, expanding the scope of analysis to include diverse cyber threats in addition to smishing, and establishing a global cyber threat response system based on an international cooperation network. Especially for hybrid attack techniques such as RD-BSU, effective response is difficult with the existing blacklist-based detection system or DGA detection model. Therefore, a multidimensional analysis approach in connection with the domain registration infrastructure needs to be developed.

REFERENCES

[1] KISA Insight 2024 vol.07. https://www.kisa.or.kr/skin/doc.html?fn=20241031_143409_623.pdf&rs=/result/2024-10/.

[2] Barnett, J. RDGAs: The Next Chapter in Domain Generation Algorithms. Infoblox. 17 July 2024. https://blogs.infoblox.com/threat-intelligence/rdgas-the-next-chapter-in-domain-generation-algorithms/.

[3] Antonakakis, M.; Perdisci, R.; Nadji, Y.; Vasiloglou, N.; AbuNimeh, A.; Lee, W.; Dagon, D. From throw-away traffic to bots: Detecting the rise of DGA-based malware. In 21st USENIX Security Symposium, 2012. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final127.pdf.

[4] TLD-LIST. https://tld-list.com/.