

Detailing Daily Domain Hunting

pylos.co/2022/11/23/detailing-daily-domain-hunting/

Joe

11/23/2022



Updated 23 Nov 1355 MST: Added some additional observations related to logon spoofing infrastructure.

Domain “hunting” is a process of identifying new (or at least, newly identified) network infrastructure associated with threat actors of interest. Such a process does not start in a void, but rather requires understanding tendencies and patterns associated with adversary infrastructure creation and management. This is especially effective when viewing individual network observables – or indicators – as natural composite objects, items that accrue multiple sub-observations relating to the given object’s creation, use, and potentially even intention.

One historical example of such activity is ThreatConnect’s analysis of (then) long-running infrastructure tendencies linked to APT28, also known as FancyBear, but associated with Russian Military Intelligence (GRU) 85th Main Special Service Center (GTsSS). ThreatConnect’s reporting publicized patterns used by intelligence professionals for several years prior, using a combination of x509 certificate information, domain registration tendencies, and domain hosting patterns to identify new APT28 infrastructure with high confidence as it was created. Unfortunately, the adversary largely migrated away from these patterns shortly after the blog’s publication, but the overall idea remains a solid mechanism to systematize external threat hunting as well as implementing an intelligence-driven pivoting process.

There are multiple ways to approach domain hunting and tracking. One reasonable mechanism is to utilize internal visibility of newly-observed network objects or external feeds such as DomainTools to look for infrastructure objects fitting certain patterns based on domain sub-characteristics. Using this methodology, the following domain came to light on 22 November 2022:

msn-imap[.]com

Even at first glance, this appears suspicious given naming conventions, spoofing a combination of MSN and IMAP services. Further research, in this case using DomainTools Iris Investigate, shows further details that call this item out as likely malicious:

Inspect: msn-imap.com

Domain Profile | Screenshot History | Whois History | Hosting History | SSL Profile

Tags: Find or create a tag to add... + Add

Screenshots: No screenshot available.

Risk Score

75 Overall Score	Spam Threat Profile
----------------------------	-------------------------------

Registrant, Ip Address, Domain Name

Supporting Evidence

56 Phishing	31 Malware	75 Spam	15 Proximity
-----------------------	----------------------	-------------------	------------------------

Domain Details

Recently Resolved As

msn-imap.com	92.38.135.213
--------------	---------------

[View pDNS](#)

Email

- 9a79981fef9b4a20f8c1bb437683c833-39526143@contact.gandi.net ~1 share this value
- abuse@support.gandi.net ~2,928,260 share this value
- dns@openprovider.eu ~830,616 share this value

Registrant

- REDACTED FOR PRIVACY ~113,153,324 share this value
- Country: Netherlands - (NL)

Registrant Org

- REDACTED FOR PRIVACY ~46,948,527 share this value

DomainTools Iris Screenshot

No screenshot available.

Name Servers

- [ns1.openprovider.nl](#) ~844,500 share this value
- [ns2.openprovider.be](#) ~0 share this value
- [ns2.openprovider.be](#) ~838,415 share this value
- [ns3.openprovider.eu](#) ~837,260 share this value

IP Address

- [92.38.135.213](#) ~1 share this value

IP Location

92.38.135.213

- Country: Korea, Republic Of
- Region: Seoul Teukbyeolsi
- City: Seoul
- ISP: G-core Labs S.a.

ASN

- [AS202422](#) G-CORE LABS S.A., KR

SSL

- No Results

Domain Status

- Active

Whois History

- 1 record have been archived since 2022-11-20

[View Whois History](#)

Name Server History

- 1 change on 2 unique name servers over 0 years

DomainTools Iris ScreenShot

We can spot several items that look suspicious here – anonymized registration, dedicated hosting (on IP address 92.38.135.213), suspicious authoritative name server use – but unfortunately there’s very little to pivot on to learn more about this item (or identify related infrastructure) using just domain information.

We can dig further by looking at the hosting address. In this case, using [Censys Search](#) we can profile this further:

92.38.135.213 HISTORICAL

As of: Nov 22, 2022 8:54am UTC | [See Latest](#)

[Summary](#) [Explore](#) [History](#) [WHOIS](#)

[Raw Data](#)

Basic Information

Reverse DNS	onkrdot.info
OS	Ubuntu Linux
Network	GHOST (LU)
Routing	92.38.135.0/24 via AS202422
Protocols	22/SSH, 25/SMTP, 80/HTTP, 443/HTTP



Geographic Location

Province	Gwangju
Country	South Korea (KR)
Coordinates	35.1496, 126.9156
Timezone	Asia/Seoul

22/SSH TCP

Observed Nov 21, 2022 at 5:31pm UTC

[VIEW ALL DATA](#)

Software

- Ubuntu Linux 20.04
- OpenBSD OpenSSH 8.2

Details

Host Key

Algorithm	ecdsa-sha2-nistp256
Fingerprint	2f94e03bb97d21d1c36d6659613388bea07d10dfa81abb50ea8b9ac6b663f013

Negotiated

Key Exchange	curve25519-sha256@libssh.org
Symmetric Cipher	aes128-ctr [🔒] aes128-ctr [🔒]
MAC	hmac-sha2-256 [🔒] hmac-sha2-256 [🔒]

Censys Search Screenshot

Software

[VIEW ALL DATA](#)

- [linux](#)
- [Postfix](#)
- [Ubuntu Linux](#)

Details

Banner	220 onkrdot.info ESMTP Postfix (Ubuntu)
EHLO	250-onkrdot.info 250-PIPELINING 250-SIZE 10240000 250-VRFY 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING
Start TLS	220 2.0.0 Ready to start TLS

TLS

Fingerprint

JA3S [475c9302dc42b2751db9edcac3b74891](#)

Handshake

Version Selected	TLSv1_3
Cipher Selected	TLS_CHACHA20_POLY1305_SHA256

Leaf Certificate

[8e5fc62dccc79ac902da74dc00d2ed36c4e7f7ccee7b201ecded0b3c1bcb29f9](#)
CN=vps.hostry.com
CN=vps.hostry.com

Censys Search Screenshot

80/HTTP TCP

Observed Nov 22, 2022 at 12:21am UTC

Software

[VIEW ALL DATA](#)

[GO](#)

[Ubuntu Linux](#)

[Apache HTTPD 2.4.41](#)

Details

http://92.38.135.213

Request	GET /
Protocol	HTTP/1.1
Status Code	302
Status Reason	Found
Body Hash	sha1:7b1c377cea51ac93e6f84ab5e60dc597cb25e0c1
HTML Title	302 Found
Response Body	EXPAND

443/HTTP TCP

Observed Nov 22, 2022 at 12:21am UTC

Software

[VIEW ALL DATA](#)

[GO](#)

[Ubuntu Linux](#)

[Apache HTTPD 2.4.41](#)

Details

https://92.38.135.213

Request	GET /
Protocol	HTTP/1.1
Status Code	200
Status Reason	OK
Body Hash	sha1:c002186216f972bb72f8193cdab9717452aad212
HTML Title	404 Not Found
Response Body	EXPAND

TLS

Fingerprint

JA3S [15af977ce25de452b96affa2addb1036](#)

Censys Search Screenshot

Now we're starting to get more details on how this object might be used by an adversary, as well as other observables that can be used for searching, hunting, and follow-on pivoting. Among other items, we've learned the following:

- The adversary's infrastructure characteristics:
 - Ubuntu Linux
 - Postfix SMTP server
 - Apache HTTP/HTTPS server
 - Use of Let's Encrypt SSL/TLS certificates
- JA3S hashes for various TLS services
- Additional potential indicators, such as the domain onkrdot[.]info associated with the SMTP server

One item that immediately stands out is the SMTP server. Given our original domain's email theme, we can hypothesize that this server may be utilized for future phishing infrastructure or email relay activity. However, we also have HTTP/HTTPS servers that appear active – but in a strange way. As seen in the above screenshot, an HTTPS request returns a status code of 200 (success), but the page content (based on the HTML title) says “404 Not Found.” What is going on here?

To simplify our research, we can utilize another service – urlscan.io – to handle our interactions for us. And this serves up something strange:

404 Not Found

nginx

Website Capture from URLScan

This may seem unhelpful, but we've identified an interesting mismatch. Examination of the server through application fingerprinting indicates we are interacting with an [Apache webserver](#), while the server itself is displaying a custom webpage modeled off of (but not exactly mirroring) an [Nginx webserver](#) 404 landing page. While not a sign of obvious maliciousness, this mismatch and customization provides an interesting foothold for further exploration. One easy follow-on item lies within urlscan itself, where we can look for instances of similar landing pages based on the content hash of the delivered page – 9b43f670273b6a12b2b6894a9e29157c1859717594e98ccc5fb3eea05e71f4ed. This reveals something VERY interesting:

Search for domains, IPs, filenames, hashes, ASNs

hash:9b43f670273b6a12b2b6894a9e29157c1859717594e98ccc5fb3eea05e71f4ed|

Search

X

Help

Search results (35 / 35, sorted by date, took 40ms)

Showing All Hits

Details: Hidden

URL	Age	Size	IPs
msn-imap.com/	Public 21 hours	429 B	1
23.106.122.16/	Public 29 days	481 B	1
komale.eu/	Public 30 days	481 B	1
kakaocop.com/	Public 1 month	481 B	1
daum-policy.com/	Unlisted 2 months	429 B	1
daum-privacy.com/	Unlisted 2 months	429 B	1
daum-policy.com/	Unlisted 2 months	429 B	1
koreailmin.com/	Public 2 months	481 B	1
koreailmin.com/	Public 2 months	481 B	1
guser.eu/	Public 2 months	481 B	1
koreailmin.com/	Public 2 months	481 B	1
koreailmin.com/	Public 2 months	481 B	1
210.92.18.164/	Public 2 months	481 B	1
koreailmin.com/	Public 2 months	481 B	1
koreailmin.com/	Public 2 months	481 B	1
koreailmin.com/	Public 2 months	481 B	1
daum-security.com/	Unlisted 3 months	429 B	1
23.106.122.16/	Public 3 months	481 B	1
23.106.122.16/	Public 3 months	481 B	1
oncloudvip.info/	Unlisted 3 months	429 B	1
googlesecurity.com/	Public 3 months	481 B	1
navercorp.center/	Unlisted 4 months	429 B	1
accountskk.certuser.info/	Public 4 months	429 B	1
210.92.18.161/	Public 4 months	429 B	1

URLScan Pivot Results

We seem to have stumbled upon something reasonably unique, and linked to a variety of additional infrastructure – many of which spoof a variety of legitimate services. Among the items covered in this, we can see:

- Korean web portal [Daum](#)
- Korean web portal [Naver](#)
- Google services
- Various mail, cloud, and certificate themes

Infrastructure is overwhelmingly concentrated in Korean or East Asian hosting providers, and all items appear to be created between March and November 2022 (see Table 1 below for a list of all identified indicators).

Additionally, looking at pDNS records (in this case from VirusTotal) for the IP addresses from urlscan shows additional infrastructure of interest likely linked to this campaign:



210.92.18.161 (210.92.18.0/24)
AS 45382 (EHOSTICT)

X Community Score ✓

DETECTION DETAILS **RELATIONS** COMMUNITY 1

Passive DNS Replication (38) ⓘ

Date resolved	Detections	Resolver	Domain
2022-11-10	0 / 95	VirusTotal	nidpon.navemail.space
2022-11-05	1 / 96	Georgia Institute of Technology	serviceprotect.eu
2022-11-05	0 / 95	Georgia Institute of Technology	navemail.space
2022-11-04	0 / 95	VirusTotal	accountslog.navemail.space
2022-11-04	2 / 96	VirusTotal	accountseros.serviceprotect.eu
2022-11-04	2 / 96	VirusTotal	loginssig.serviceprotect.eu
2022-11-04	0 / 95	VirusTotal	www.serviceprotect.eu
2022-10-18	0 / 95	VirusTotal	nidpon.servicemember.info
2022-10-12	0 / 95	VirusTotal	t1dm.certuser.info
2022-10-11	0 / 96	VirusTotal	wwwlog.navemail.eu

VirusTotal pDNS Information

At this stage we've collected a lot of information about various infrastructure created (and potentially used) in 2022 with similar themes, characteristics, and other observables. Yet it is important not to lose overall context as to *what* we might be looking at – so some external enrichment and research is required to learn more.

With no actual threat to go off of (yet), we can start our search looking for entities that typically host phishing infrastructure (either for sending email, or as landing pages for links) in East Asia (and especially South Korea), that focus on spoofing legitimate services with an emphasis on South Korean major web portals. Based on [multiple reports](#) from [various entities](#), one threat group stands out matching these characteristics: [North Korean-related entity Kimsuky](#).

While we cannot be certain at this stage, based on an initial suspicious feeling around one suspect domain, we have uncovered an entire ecosystem of related infrastructure that may be related to an in-progress Kimsuky-associated campaign, likely with a focus on website spoofing and phishing. Defenders, especially those with reason to believe they may be targeted by this North Korean-linked threat actor, should take the indicators provided in Table 1 and search historical logs to see if they have interacted with any of these infrastructure items as an initial defensive measure. Going forward, threat intelligence researchers can incorporate the characteristics in infrastructure creation documented in this report and the various linked resources to build a new hunting-and-pivoting profile for infrastructure related to this entity. Overall, network indicator research and refinement can yield fantastic results if you know both where to look, and what to look for.

Table 1 – Indicators From Research

Source Item	Hosting IP	Hosting Provider	Name Server	Registrar	Create Date
118.128.149[.]119	118.128.149.119	LG Dacom Boranet	N/A	N/A	N/A
210.92.18[.]161	210.92.18.161	EHOSTICT	N/A	N/A	N/A
210.92.18[.]164	210.92.18.164	EHOSTICT	N/A	N/A	N/A

23.106.122[.]16	23.106.122.16	LeaseWeb Asia Pacific Pte. Ltd.	N/A	N/A	N/A
61.82.110[.]46	61.82.110.46	Korea Telecom	N/A	N/A	N/A
61.82.110[.]60	61.82.110.60	Korea Telecom	N/A	N/A	N/A
accountskk.certuser[.]info	N/A	N/A	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-06-07
authuser[.]info	N/A	N/A	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-06-07
certuser[.]info	N/A	N/A	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-06-07
daum-policy[.]com	92.38.160.140	G-Core Labs S.A.	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-09-25
daum-privacy[.]com	92.38.160.134	G-Core Labs S.A.	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-09-25
daum-security[.]com	92.38.160.213	G-Core Labs S.A.	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-08-21
googlernails[.]com	N/A	N/A	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-03-03
googlmeil[.]com	209.99.40.222	Confluence Networks Inc	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-05-31
googlesecurity[.]com	27.102.66.162	Daou Technology	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-03-01
guser[.]jeu	23.106.122.16	LeaseWeb Asia Pacific Pte. Ltd.	cloudns.net	PDR Ltd.	2022-09-12
kakaocop[.]com	74.119.239.234	PDR	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-10-12
komale[.]jeu	210.92.18.164	Sudokwonseobubonbu	cloudns.net	PDR Ltd.	2022-10-20
koreailmin[.]com	74.119.239.234	PDR	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-09-02
main.in[.]net	N/A	N/A	N/A	PDR Ltd. d/b/a PublicDomainRegistry.com	2021-04-02
msn-imap[.]com	92.38.135.213	G-Core Labs S.A.	openprovider.nl	GANDI SAS	2022-11-20
navemail[.]space	210.92.18.180	Sudokwonseobubonbu	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-09-12
navercorp[.]center	209.99.40.222	Confluence Networks Inc	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2021-08-31
navernail[.]jeu	N/A	N/A	cloudns.net	PDR Ltd.	2022-07-13
oncloudvip[.]info	92.38.135.166	G-Core Labs S.A.	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-08-22
onkrdot[.]info	N/A	N/A	N/A	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-10-02
servicemember[.]info	N/A	N/A	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-07-21

serviceprotect[.]eu	210.92.18.180	Sudokwonseobubonbu	cloudns.net	PDR Ltd.	2022-07-18
usersec[.]info	N/A	N/A	cloudns.net	PDR Ltd. d/b/a PublicDomainRegistry.com	2022-06-09

Table 1 – Indicators Related To Identified Activity

Additional Research

One thing that bothers me about the above are the “N/A” items for hosting – so, I decided to do some pDNS lookups in DomainTools to find out if there were subdomains hosted with these items. I was not disappointed:

Subdomain	Hosting	First Observed	Last Observed
loginslive.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
accountsmt.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
loginsmcmf.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
loginsioup.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
t1dm.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
mysql06.certuser[.]info	210.92.18[.]161	24 Oct 2022	14 Nov 2022
accountsms.certuser[.]info	210.92.18[.]161	20 Sep 2022	03 Nov 2022
loginslive.certuser[.]info	210.92.18[.]161	31 Aug 2022	14 Nov 2022
account.authuser[.]info	118.39.76[.]109	20 Jun 2022	21 Jun 2022
loginslive.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
accountsmt.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
accountsms.certuser[.]info	185.105.35[.]11	14 Nov 2022	14 Nov 2022
mysql06.certuser[.]info	210.92.18[.]161	24 Oct 2022	14 Nov 2022
staticnidlog.navernail[.]eu	210.92.18[.]161	24 Oct 2022	13 Nov 2022
remote.navernail[.]eu	210.92.18[.]161	20 Sep 2022	13 Nov 2022
vpn.navernail[.]eu	210.92.18[.]161	14 Sep 2022	14 Sep 2022
accountsig.servicemember[.]info	210.92.18[.]161	21 Sep 2022	21 Sep 2022
loginsig.servicemember[.]info	210.92.18[.]161	21 Sep 2022	21 Sep 2022

Table 2 – pDNS Responses Revealing Subdomains

But wait – there’s more! We also have a few IP addresses from our original “haul” that didn’t appear related to any other infrastructure at first pass. Additional pDNS searching looking for responses yields more domains and subdomains:

IP	Domain	First Seen	Last Seen
210.92.18[.]164	contentnts.slogin[.]eu	14 Nov 2022	14 Nov 2022
210.92.18[.]164	accounts.oksite[.]eu	05 Nov 2022	05 Nov 2022
210.92.18[.]164	cmember[.]eu	01 Nov 2022	01 Nov 2022
210.92.18[.]164	accountslog.puser[.]eu	30 Oct 2022	30 Oct 2022
210.92.18[.]164	accounts.slogin[.]edu	28 Oct 2022	09 Nov 2022

210.92.18[.]164	natescorp[.]com	28 Oct 2022	09 Nov 2022
210.92.18[.]164	accounts.auser[.]eu	06 Oct 2022	07 Oct 2022
210.92.18[.]164	account.koreailmin[.]com	12 Sep 2022	12 Sep 2022
210.92.18[.]164	mailuser[.]info	06 Sep 2022	06 Sep 2022
23.106.122[.]16	accounts.guser[.]eu	27 Oct 2022	28 Oct 2022
23.106.122[.]16	accounts.googlesecurity[.]com	16 Aug 2022	09 Oct 2022
23.106.122[.]16	mobile.navernnail[.]com	23 Jun 2022	23 Jun 2022
61.82.110[.]60	nidm.navernnail[.]com	03 May 2022	03 May 2022
61.82.110[.]60	nidlogin.navernnail[.]com	25 Apr 2022	02 May 2022

Table 3 – pDNS Responses By IP Address

We can keep going back and forth between domains and IP addresses as long as we'd like, collecting indicators like so many Pokémon. But more usefully, we continued to refine our understanding of adversary infrastructure creation tendencies. Additionally, with the important caveat that pDNS data is not complete, we established rough timelines of when different infrastructure items appear to be “active” – allowing us to guide defenders as to when activity was most likely to have occurred.

Unfortunately, it appears most of the infrastructure identified is no longer “live.” But there’s more that we can do looking at other resources. For example, we can attempt to find mappings to file objects through resources such as VirusTotal. Similar to urlscan, we can search for the hash of the displayed, fake “404” page, which identifies additional items:

ITW Urls (81)

Scanned	Detections	Status	URL
2022-11-21	3 / 91	200	https://daum-master.com/
2022-11-20	4 / 91	200	http://navercorp.world/
2022-11-20	4 / 91	200	https://navercorp.world/
2022-11-14	0 / 90	200	http://59.21.113.148/
2022-11-01	0 / 90	200	http://natescorp.com/
2022-10-31	2 / 90	404	http://23.106.122.16/dashipatch.php
2022-10-24	0 / 90	200	http://23.106.122.16/dashipatch.php?name=Image
2022-11-04	1 / 90	200	http://kakaocop.com/
2022-10-20	1 / 90	200	http://92.38.160.210/
2022-11-20	10 / 91	200	http://login.daum-protect.com/

ITW Domains (46)

Domain	Detections	Created	Registrar
daum-master.com	4 / 96	2022-09-02	PDR Ltd. d/b/a PublicDomainRegistry.com
navercorp.world	5 / 96	2022-08-23	-
natescorp.com	0 / 96	2022-10-25	-
kakaocop.com	1 / 96	2022-10-12	PDR Ltd. d/b/a PublicDomainRegistry.com
login.daum-protect.com	10 / 96	2022-09-26	-
nid.daum-protect.com	10 / 96	2022-09-26	-
servicemember.info	3 / 96	2022-07-21	-
guser.eu	10 / 96	-	-
koreailmin.com	3 / 96	2022-09-02	PDR Ltd. d/b/a PublicDomainRegistry.com
mailuser.info	0 / 96	2022-09-02	-

VirusTotal Result

For Fake Nginx 404 Page

More interestingly, we can contingently verify that these campaigns are tied to credential theft via website spoofing by looking at the full submitted URL for one of the domains in question:

The screenshot displays the VirusTotal interface for a submitted URL. On the left, a circular progress indicator shows a score of 4 out of 91. A red banner at the top states "4 security vendors flagged this URL as malicious". The URL is truncated, showing the domain "accounts.auser.eu". Below the URL, there are tabs for "DETECTION", "DETAILS", "TELEMETRY", and "COMMUNITY". The "DETAILS" tab is active, showing "Categories" (Forcepoint ThreatSeeker: dynamic content, Comodo Valkyrie Verdict: media sharing) and "History" (First Submission: 2022-10-06 18:13:26 UTC, Last Submission: 2022-11-21 23:59:14 UTC, Last Analysis: 2022-11-21 23:59:14 UTC). The text "URL Submitted To" is visible on the right side of the interface.

VirusTotal

While we can't completely confirm with available information, it does appear that there is a "passthrough" on the link that on submission will redirect the user (or input) to the legitimate Gmail site.

Ideally, we would find a file – an email, a payload, or some other object – that would allow us to link the infrastructure to follow-on capabilities. In this case, a cursory research effort fails to identify any such objects, limiting our ability to take this further. But, if this actor – likely Kimsuky – is of interest to you, the following provides an interesting overview of how this actor appears to utilize infrastructure to facilitate credential capture for services such as Google, Naver, Daum, and others.