

What Wicked Webs We Un-weave

prevailion.com/what-wicked-webs-we-unweave/

March 15, 2022

WIZARD SPIDER

WHAT WICKED WEBS WE UN-WEAVE



PREVAILION

THREAT INTEL REPORT

15 March 2022

What Wicked Webs We Un-weave: Wizard Spider once again proving it isn't you, it isn't me; we search for things that you can't see

Authored by: Matt Stafford and Sherman Smith

Executive summary:

In late January 2022, Prevailion's Adversarial Counterintelligence Team (PACT) identified extensive phishing activity designed to harvest credentials for Naver. Naver is a popular South Korean online platform comparable to Google, that offers a variety of services (e.g., email, news, and search, among many others). For this reason, a large cache of valid credentials for Naver is potentially very valuable: it can provide access to the personal Naver accounts of a wide variety of victims while also providing access to several other enterprise logins as a result of password reuse. Two intriguing facets of this investigation quickly became apparent to PACT's analysts: the sheer volume and focus of malicious activity by a single entity, focused exclusively on harvesting Naver credentials (more than 500 domains), and substantiated overlaps with infrastructure historically associated with WIZARD SPIDER (a Russia-based, financially-motivated threat actor involved in initial access and ransomware operations). This overlap is significant because it may indicate a current geographic targeting preference by one of the most active cyber crime groups in existence and would provide valuable insight into that group's operational workflow. However, PACT's analysis unearthed additional circumstantial evidence supporting previous assessments that posit an emerging, top-tier "infrastructure as a service for cybercriminals". This potential service, if it exists, would explain the WIZARD SPIDER overlap as well as PACT's additional findings.

Update: 30 MAR 2022

Google's Threat Analysis Group (TAG) published a report on 24 Mar 2022 titled, *Countering threats from North Korea*. In this report, TAG details the operations of North Korean state-backed threat actors engaged in active exploitation of a RCE vulnerability in Google Chrome. TAG lists several domains they assess are owned by the threat actors, one of which is "disneycareers[.]net". This domain immediately caught PACT's attention, as it was one of the anomalous findings we documented in our initial report (below). To quickly summarize: PACT identified this (apparently unrelated) domain hosted on dedicated infrastructure that was primarily being used to host extensive Naver-themed phishing activity. Two weeks ago (see update to this blog on 18 Mar 2022), Google TAG published their assessment that an Initial Access Broker (IAB) with ties to the Conti ransomware gang was using this infrastructure as well. Prior to that, RiskIQ and Microsoft had identified at least three distinct clusters of activity (WIZARD SPIDER, zero-day exploitation used to deploy unique Cobalt Strike BEACON payloads, and initial access tooling like BazarLoader and Emotet). PACT considers it notable and highly unusual that multiple research teams have observed such a wide spectrum of activity occurring on this infrastructure: phishing, initial access operations, targeted ransomware, and state-backed espionage have all been well documented.

TAG's disclosure of additional domains allowed PACT's analysts to conduct additional pivots. Further overlaps were indeed observed, but generally amounted to additional "ancillary evidence" (to borrow a phrase from RiskIQ): 5 domains published by TAG were linked to PACT's previous findings via pDNS, but all these previous resolutions were part of shared hosting infrastructure that cannot be definitively tied to a single actor or customer. However, PACT found the level of overlap noteworthy: over 80 domains listed as part of the Cobalt Strike infrastructure documented by RiskIQ were linked to the following 5 domains from TAG's report: chainnews-star[.]com, gbclabs[.]com, blockchainnews[.]vip, giantblock[.]org, ziprecruiters[.]org. The pDNS overlaps formed by these domains is *in addition to* the current overlap seen with disneycareers[.]net, which TAG assesses is part of the recent North Korean-backed Chrome exploitation activity and hosted on what multiple vendors have assessed to be non-public IP "172.93.201[.]253". This same IP was the first critical node identified in PACT's investigation, as a large number of Naver-themed phishing pages with a common registrant resolved to this IP.

Additional feedback from the information security community (hat tip to Zetalytics) turned PACT onto what we assess to be an additional node in this dedicated infrastructure: "23.82.19[.]179". PACT identified 38 **new***/previously-unknown Naver-themed phishing domains after identifying this IP address. 21 previously-known Naver-themed domains were seen resolving to *both* this IP as well as "23.81.246[.]131", which formed the initial link between the Naver credential phishing activity and the reported WIZARD SPIDER infrastructure. Further strengthening PACT's assessment that "23.82.19[.]179" is a part of this cluster of malicious infrastructure is the fact that registrant persona "gameproducers@outlook[.]com" registered **all** newly-identified domains; this same registrant was identified in PACT's original reporting. Threat Actor TTP overlaps were also observed and provided added confidence: IP "23.82.19[.]179" serves HTTP/302 redirects to Naver-themed phishing pages hosted on 000webhostapp.com, which was a technique PACT observed previously. Furthermore, this IP is part of Leaseweb, Inc.'s US-based dedicated hosting infrastructure, which PACT identified as the actor's preferred vendor and geographic location.

*note: PACT included these 38 newly-identified domains in the IOC annex of our report, below.

In summary, the publication of additional information surrounding this infrastructure has led to further uncertainty. The only assessment of near certainty that can be made in light of recent research is that there is a definite nexus of malicious use around this infrastructure. Recent reporting has not altered PACT's initial assessment of moderate confidence: an as-yet unreported criminal hosting service exists on this infrastructure. The wide variety of malicious activity and distinct operational goals, initially observed by Microsoft and RiskIQ, deserve special attention and analysis.

Update: 18 MAR 2022

Google's Threat Analysis Group (TAG) published a blog on 17 Mar 2022 titled, [Exposing initial access broker with ties to Conti](#). In this report, TAG references the findings of both Microsoft's MSTIC and RiskIQ's Team Atlas that PACT also references below, and builds on the hypotheses and findings of all firms involved in the tracking and analysis of the criminal enterprise unfolding across the infrastructure that PACT details in our report. TAG identifies and names a Threat Actor (EXOTIC LILY) operating as an Initial Access Broker (IAB) on this infrastructure. They also corroborate many previous findings: use of this infrastructure to deploy common tooling centered around a financially-motivated nexus and an association with WIZARD SPIDER. To quote TAG: "Initial access brokers are the opportunistic locksmiths of the security world, and it's a full-time job."

PACT used the indicators that TAG published to identify additional overlaps in an effort to provide further value to the security community. PACT analysts found circumstantial evidence and TTP overlaps that, taken together, serve to reinforce previous research and strengthen the common intelligence picture. Overlaps such as the threat actor's hosting provider preference (Leaseweb USA, Inc): several IPs from this hosting provider's network appeared as critical nodes in PACT's investigation. There was also CDN hosting overlap seen via pDNS sources: TAG identified "modernmeadow[.]co" as one of the "recent domains used in email campaigns," and PACT identified that it shared resolutions with Akamai IPs along with "yeruje[.]com". RiskIQ had previously [identified](#) this domain as a C2 for the unique Cobalt Strike Malleable C2 Profile that they fingerprinted and tracked as part of the activity cluster exploiting CVE-2021-40444. Additional TTP overlaps were seen in how the threat actor's core infrastructure does not appear to be commercial shared web hosting, as there are no historic resolutions; and in how they use self-signed certificates. The threat actor's predilection for avoiding WHOIS Privacy services, leaving unredacted registrant information available for researchers, was also observed in some of the domains that TAG provided. These observable TTPs were noted by PACT in our initial publication.

When overlaid with PACT's pre-existing research, TAG's findings reinforce our own: the operations of EXOTIC LILY "appear to be closely linked" with the deployment of Conti ransomware. The operational requirements of an IAB would certainly explain the activity that PACT observed: the robust domain name buildup targeting Naver. An IAB would need to send many emails and design spear-phishing messages that seemed convincing and credible to potential victims; they would also be required to maintain the level of resilience required to sustain operations in the face of domain attrition caused by phishing protection services. TAG's assessment that EXOTIC LILY appears to operate as a distinct entity that utilizes shared infrastructure reinforces PACT's assessment that "this infrastructure appears to support separate, discrete campaigns; it also supports operational mechanisms along multiple links of the killchain." PACT lacks the visibility to confirm that EXOTIC LILY is the group operating the Naver-themed phishing on this infrastructure, but the criminal nexus of the infrastructure itself is now well documented. This infrastructure, and its intended use, certainly match the needs of an initial access broker; when paired with the overlap to known WIZARD SPIDER infrastructure, it supports the hypothesis that this may be the same threat actor.

Part I: Introduction & Context

In September of 2021, [RiskIQ's Team Atlas](#) and [Microsoft's Threat Intelligence Center \(MSTIC\)](#) jointly published technical reports on a cluster of malicious activity that exploited CVE-2021-40444, a vulnerability in MSHTML that allows remote code execution on a victimized Windows system. The operational roots of this activity reportedly began in February of 2021. Both RiskIQ and Microsoft observed significant overlap in the network infrastructure used in this campaign with network infrastructure associated with WIZARD SPIDER. WIZARD SPIDER (aka UNC1878) is a large, Russia-based, criminal enterprise that has operated the Trickbot, Bazar, and Anchor families of malicious Remote Access Trojans (RATs) and has been observed deploying the Conti and Ryuk ransomware families in "Big-Game Hunting" campaigns that target large enterprises.^(1,2,3) The overlaps that Microsoft and RiskIQ observed were related to supporting infrastructure, in the form of non-public IP addresses, used by WIZARD SPIDER as Command and Control (C2) nodes for Cobalt Strike, which the group used as a post-intrusion tool prior to the deployment of Ryuk and Conti ransomware. Additional overlap was seen via domain registrant information (specifically the registrant email address) provided when purchasing the domains used to create TLS certificates (thus enabling TLS encryption for the Cobalt Strike C2 traffic between victim and attacker).

RiskIQ's Team Atlas provided an exhaustive list of IP addresses and TLS certificates (and their associated domain names) that were attributed to WIZARD SPIDER's C2 infrastructure [here](#).

This list provided PACT with the ability to cross reference and corroborate the Naver-themed phishing activity that PACT observed with WIZARD SPIDER's operations.

It is important to note, however, that both research teams observed anomalies during their investigations that indicate this overlap may not be indicative of an operation by WIZARD SPIDER, but may instead be indicative of multiple actors using the same network infrastructure. This overlap could be caused by multiple operators exploiting known compromised hosts, a “form of command-and-control infrastructure as a service for cybercriminals”, or some other shared resource not owned by a single threat actor⁴.

Fast forward 4 months: during the conduct of routine investigation and analysis of malicious web-based infrastructure, PACT identified a domain of interest (mailmangecorp[.]us) via a [tweet](#) by [Joe Slowik](#). With this initial finding, PACT analysts began methodically illuminating a network of **targeted** phishing infrastructure designed to harvest valid login credentials for Naver. The Naver Corporation operates a large, regional, and popular online platform that provides dozens of customer-facing services (e.g., email, search, social, payment) and can be compared to a South Korean Google. While investigating the hosting infrastructure being used to serve the Naver-themed phishing pages, PACT analysts identified overlaps with the WIZARD SPIDER infrastructure, mentioned above, from RiskIQ’s and Microsoft’s joint reporting. This blog will detail PACT’s findings and methodology, the noted overlaps with WIZARD SPIDER infrastructure, as well as key takeaways that may shed new light on the alternate hypotheses put forward by both Microsoft and RiskIQ.

Part II: Findings

Ila: Naver-themed Phishing Activity

By the end of PACT’s investigation, 542 unique domains had been identified as part of this malicious cluster of web infrastructure, 532 of which were assessed with high confidence to be part of the ongoing phishing campaign targeting Naver logins; the oldest domain identified by PACT was registered in August of 2021, other registrations are as recent as February of 2022. The remaining domains were of unknown provenance, part of previously reported historic malicious infrastructure that PACT tracked as part of this cluster, or were otherwise anomalous but related via linkages in hosting or registration. The full list of 532 Naver-themed phishing domains are included in the annex to this report.

The “critical nodes*” of PACT’s investigation turned out to be IP addresses and, when available, domain registrant personas (identified and tracked by the registration email address used to register the domain). The first critical node identified was IP 172.93.201[.]253; it quickly became apparent to PACT’s analysis that a large number of Naver-themed phishing pages with a common registrant (mouraesse@gmail[.]com) resolved to this IP.

navercorp.000webhostapp.com

2a02:4780:dead:6f97::1 

[Lookup](#) [Go To](#) [Rescan](#)
[Add Verdict](#) [Report](#)

Submitted URL: <http://mailservicecorp.site/?ZVRPg7R9rk9dQptrNELeURhCwTrMzwhg=ZVRPg7R9rk9dQptrNELeURhCwTrMzwhg&ref=bm90c2lsbHk=>

Effective URL: <https://navercorp.000webhostapp.com/?ref=bm90c2lsbHk=>

Submission: On November 10 via manual (November 10th 2021, 5:03:08 am UTC) from  — Scanned from 

[Summary](#) [HTTP 4](#) [Redirects](#) [Links 12](#) [Behaviour](#) [Indicators](#) [Similar 152](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary


This website contacted 5 IPs in 2 countries across 5 domains to perform 4 HTTP transactions. The main IP is 2a02:4780:dead:6f97::1, located in United States and belongs to AWEX, CY. The main domain is navercorp.000webhostapp.com. TLS certificate: Issued by RapidSSL TLS DV RSA Mixed SHA256 2020... on July 10th 2021. Valid for: a year.

[navercorp.000webhostapp.com](#) scanned 4 times on urlscan.io [Show Scans 4](#)

152 similar pages on different IPs, domains and ASNs found [Show Scans 152](#)

urlscan.io Verdict: No classification 

Live information

Google Safe Browsing:  Malicious for navercorp.000webhostapp.com
Current DNS A record: 145.14.144.212 (AS204915 - AWEX, CY)
Domain created: May 11th 2016, 09:34:12 (UTC)
Domain registrar: Hostinger, UAB

Screenshot

[Live screenshot](#) [Full Image](#)



Page URL History

[Show full URLs](#)

1. <http://mailservicecorp.site/?ZVRPg7R9rk9dQptrNELeURhCwTrMzwhg=ZVRPg7R9rk9dQptrNELeURhCwTrMzwhg&ref=bm90c2lsbHk=> [HTTP 302](#)
<https://navercorp.000webhostapp.com/?ref=bm90c2lsbHk=> [Page URL](#)

Image 2: Naver-themed domain hosted on IP 172.93.201[.]253 displaying an HTTP/302 redirect to a spoofed Naver login page on “000webhostapp[.]com”:

Pivoting on the registrant email “mouraesse@gmail[.]com” allowed PACT to identify that several domains registered with this email address were seen resolving to another IP address, 23.81.246[.]131. This IP address became a critical node in PACT’s investigation and formed the initial link between the Naver credential phishing activity with the alleged WIZARD SPIDER infrastructure. However, before we detail our findings on these observed overlaps, there are additional critical nodes that are wholly within the distinct cluster of Naver-themed phishing activity:

- Registrant email addresses “peterstewart0326@gmail[.]com” and “kimkl0222@hotmail[.]com”, which appear to have been used jointly and by the same actor, registered over 100 Naver-themed phishing domains.
- Registrant email addresses “tree99111@hotmail[.]com” and “jhonsteven0001@hotmail[.]com”, which also appear to have been used jointly and by the same actor, registered 69 domains, some of which had previously resolved to critical node 23.81.246[.]131.

navercorpd.online

31.220.50.16 🇨🇵

Submitted URL: <http://navercorpb.website/>
Effective URL: <https://navercorpd.online/?ref=>

Submission: On December 15 via manual (December 15th 2021, 4:29:44 pm UTC) from IE 🇮🇪 — Scanned from FR 🇫🇷

Summary HTTP 4 Redirects Links 11 Behaviour Indicators Similar 152 DOM Content API Verdicts

Summary

This website contacted 4 IPs in 4 countries across 4 domains to perform 4 HTTP transactions. The main IP is 31.220.50.16, located in Cyprus and belongs to AS-HOSTINGER, CY. The main domain is navercorp.d.online. TLS certificate: Issued by cPanel, Inc. Certification Authority on November 30th 2021. Valid for: 3 months.

navercorpd.online scanned 2 times on urlscan.io

Show Scans 2

152 similar pages on different IPs, domains and ASNs found

Show Scans 152

urlscan.io Verdict: No classification 🟢

Live information

Google Safe Browsing: 🚫 Malicious for navercorp.d.online

Domain created: November 2nd 2021, 23:06:12 (UTC)

Domain registrar: Hostinger, UAB

Screenshot

Live screenshot Full Image



Page URL History

Show full URLs

1. <http://navercorpb.website/> HTTP 302
<https://navercorpd.online/?ref=> Page URL

Page Statistics

4	100 %	25 %	4	4
Requests	HTTPS	IPv6	Domains	Subdomains
4	4	252 kB	398 kB	0
IPs	Countries	Transfer	Size	Cookies

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
			IP Address	AS Autonomous System		
1 → 1	198.244.135.244 🇫🇷		16276 (OVH)			
2	31.220.50.16 🇨🇵		47583 (AS-HOSTINGER)			
1	23.58.217.145 🇩🇪		16625 (AKAMAI-AS)			
1	2606:4700::6810:135e 🇺🇸		13335 (CLOUDFLARENET)			
4			4			

Image 4: critical node IP address 198.244.135.[.]244 observed serving HTTP/302 redirects, a TTP overlap with the Naver-phishing actor

- 15.235.132[.]77
 - Part of ASN 16276 (OVH Singapore PTE. LTD), along with critical node “198.244.135[.]244”, seen above
 - Provided overlap with domains registered by the “kimk10222@hotmail[.]com / peterstewart0326@gmail[.]com” actor that allowed PACT to identify additional WHOIS domain registrant “gameproductors@outlook[.]com”
- 108.177.235[.]15
 - Part of ASN 395954 (Leaseweb USA, Inc.)
 - Provided overlap with domains registered by the “kimk10222@hotmail[.]com / peterstewart0326@gmail[.]com” actor
 - Displayed TTP overlap (IP seen serving HTTP/302 redirects, notably to the legitimate Naver login page):

Notably, all the IP addresses listed above as *critical nodes*, including 23.81.246[.]131, *do not* appear to be commercial shared web hosting (as historic resolutions only include the Naver phishing activity). Additionally, despite all 5 IP addresses having little information available in public scan data, they all appear to be Windows machines running self-issued TLS certificates.

It is also important for the reader to note the common usage of the HTTP 302 Redirect in order to funnel victims to the intended page. PACT observed HTTP 302 Redirects to both additional Naver-themed phishing domains (seen in *Image 4, above*) and also to several Naver-themed phishing subdomains on Hostinger’s web hosting platform “000webhostapp[.]com”. An example appears below on critical node IP address 23.81.246[.]131 (alongside an expired, self-signed TLS certificate):



Image 5: HTTP/302 redirect to 000webhostapp[.]com (a TTP overlap) identified on critical IP 23.81.246[.]131

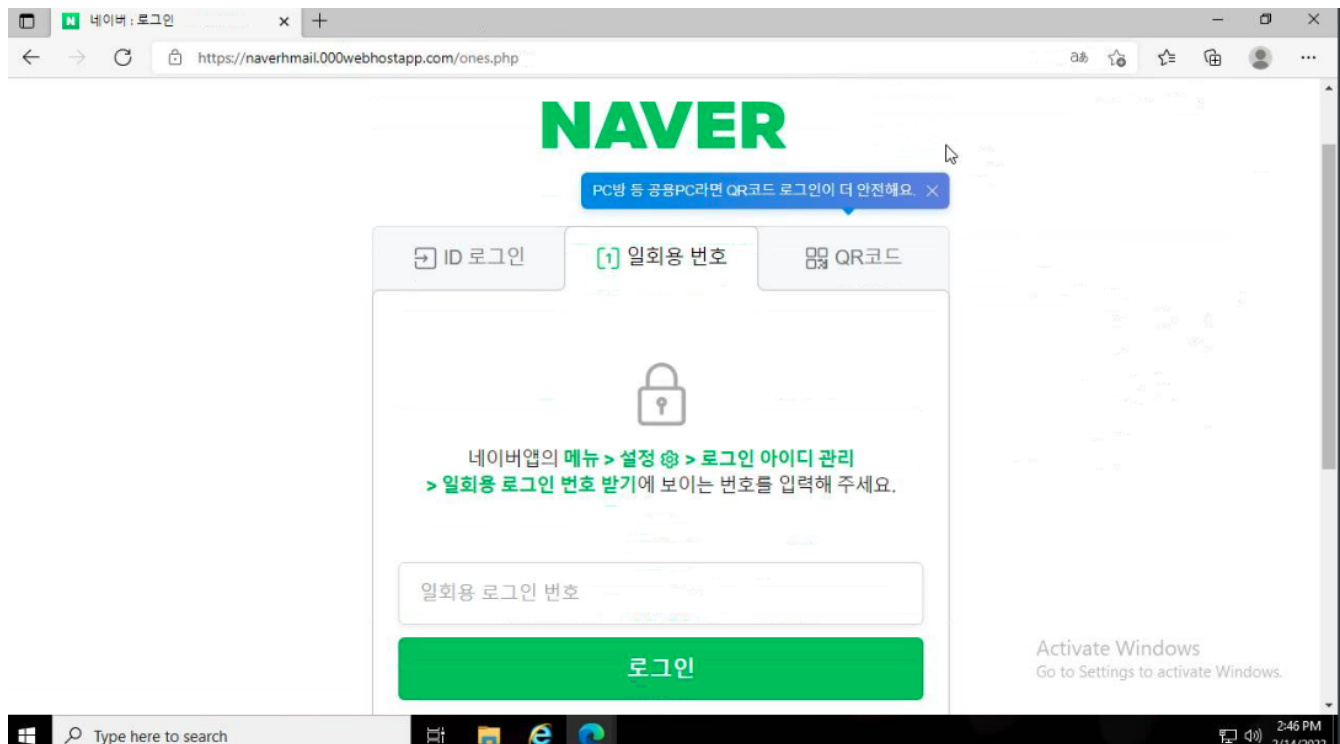
This screenshot of Shodan’s ‘host’ page for 23.81.246[.]131 (last seen date: 2022-02-15) provides insight into how the phishing infrastructure can be set up, independent of the final phishing URL hosted on “000webhostapp[.]com”:

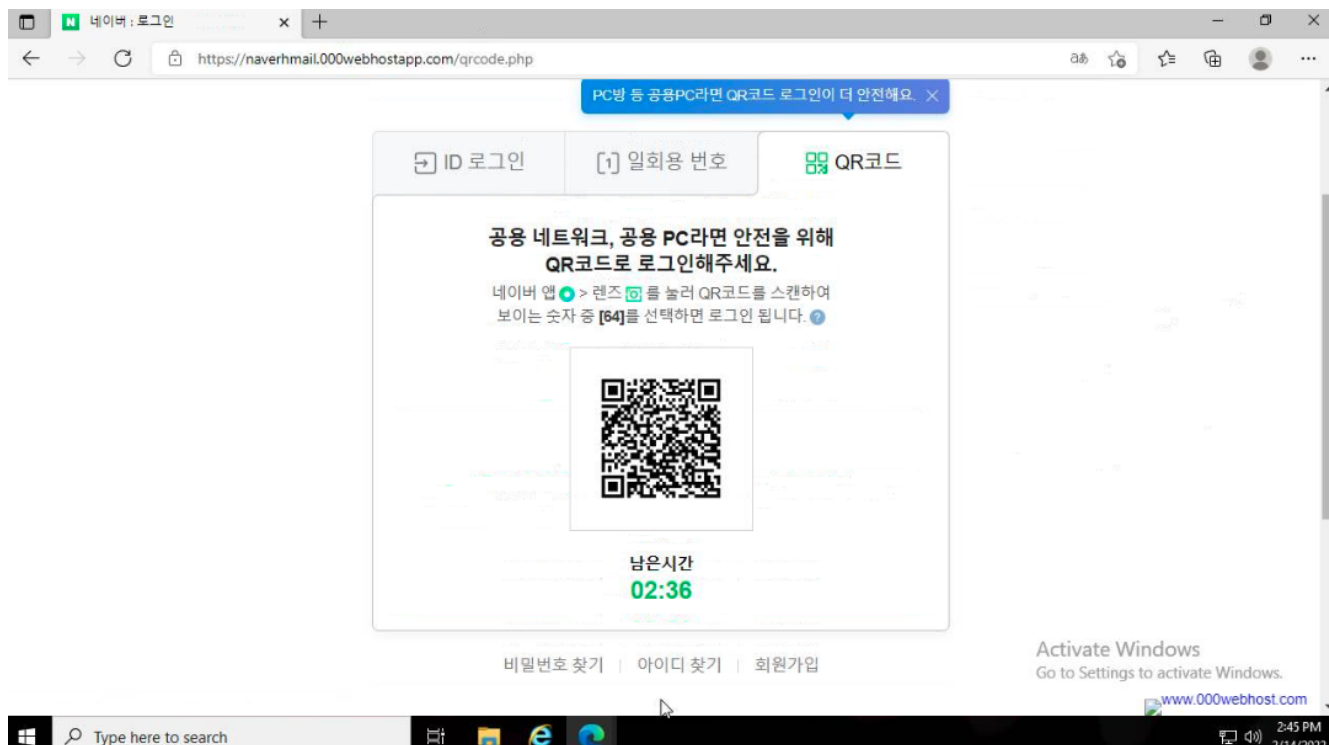
1. Victim clicks or otherwise navigates to one of the 500+ Naver-themed domain names
2. The DNS A-record for an arbitrary number of them is set to an IP address with a web server configured similar to the way that 23.81.246[.]131 is set up (with a generic, catchall HTTP 302 Redirect) to a subdomain of “000webhostapp[.]com”
3. Victim’s browser redirects them to the “000webhostapp[.]com” domain, where they are served a convincing replica of the Naver login page.

4. Victim enters their credentials, which are captured and now compromised.

This setup is designed to withstand the domain attrition commonly suffered by widely-disseminated phishing campaigns, which is generally caused by the phishing domains being identified, reported, and taken down or blocklisted. By disconnecting the final phishing URL from the initial victim-facing URL, the threat actor's infrastructure becomes more resilient. Additionally, this increases the odds that the final URLs hosting the phishkit will be "allowlisted" or not closely inspected (due to the fact that they're being hosted on a legitimate hosting platform).

Phishing for Naver credentials appears to be common, which may indicate the relative value of valid logins. AhnLab's ASEC [reported](#) on Naver phishing activity as well, but the cluster they observed appears distinct as the threat actor's TTPs differed: they didn't use tech-themed domains, they didn't use HTTP 302 Redirects to funnel victims to the final credential-gathering page, and the one-time-use number and QR code functionality weren't configured. The Naver-themed phishing pages that PACT analyzed had working one-time-use number and QR code functionality, although we were unable to verify if users were successfully compromised using these methods.





Images 6 & 7: the Naver phishing pages PACT analyzed supported one-time-password and QR code functionality

The subdomains that PACT was able to identify on “000webhostapp[.]com” serving spoofed-Naver phishing pages are included in the annex at the end of this report. Due to the ease with which the operator can create new subdomains on this hosting platform, this list is likely outdated and/or incomplete.

IIb: Overlaps with Reported WIZARD SPIDER Infrastructure

In section ‘IIa: Naver-themed Phishing Activity’, PACT stated that overlaps were observed between the network infrastructure supporting the Naver phishing activity, and that of historic network infrastructure used by WIZARD SPIDER. This overlap was initially identified via IP 23.81.246[.]131 (seen in *Image 5*, above, displaying TTP overlap).

This IP address was initially discovered by PACT’s analysts during attempts to identify which of the 58 phishing domains registered by “mouraesse@gmail[.]com” were currently resolving, if any. At the time of initial analysis, the domain “navermailcorp[.]com” was resolving to “23.81.246[.]131”, which PACT further identified resulted in the HTTP Redirect to a spoofed Naver login page on “*.000webhostapp[.]com”.

Additional investigation yielded two malware samples, as identified on VirusTotal, that were associated with IP 23.81.246[.]131:

Communicating Files ⓘ			
Scanned	Detections	Type	Name
2022-02-08	43 / 67	Win32 EXE	Ob4b1f2af5257c0aa79fda9b75accef9f4d6181b6d80eea5a1740460ab8514ae.sample
2021-08-24	31 / 67	Win32 EXE	cdc.exe

Image 8: Malicious files seen communicating with IP of interest 23.81.246[.]131

Open source reporting identified and corroborated these malicious samples as Cobalt Strike: the extracted Cobalt Strike Beacon (post-exploitation payload) configuration for one of the samples displays the same watermark identified by a security researcher on Twitter who identified these samples as part of a cluster of activity exploiting CVE-2021-40444. Additionally, the network behavior displayed by the other sample shows HTTP connections to “hubojo[.]com” and “bideluw[.]com”. These two domains are important: they match the extracted Beacon configuration from the first sample, and they both also represent additional, discrete links to 23.81.246[.]131:

- “bideluw[.]com” was observed resolving to this IP via pDNS
- RiskIQ reported that this IP previously served the certificate for “hubojo[.]com”, tying it to a Cobalt Strike C2 server (validating the extracted Beacon configuration from VirusTotal).

These observations all serve to bolster the previous reports of an actor using this infrastructure to support a campaign exploiting CVE-2021-40444 and to host Cobalt Strike.

With these historic findings in mind, PACT found it notable that more than 40 of the Naver-themed phishing domains had resolved to IP 23.81.246[.]131. PACT identified numerous emergent resolutions during the course of the investigation, which suggests that this activity is ongoing and this infrastructure is currently in use. PACT’s analysis continued throughout the pre-publication pipeline, identifying numerous domains registered in March 2022. We will update this report as our investigation progresses and yields additional findings.

In addition to the linkages provided by 23.81.246[.]131, another overlap was observed via IP 23.19.227[.]176. This IP had previously been associated with “naverservice[.]host” (part of the Naver phishing cluster); however, it was also detailed in RiskIQ’s report as part of the same Cobalt Strike C2 infrastructure used by the actor exploiting CVE-2021-40444. In this case, it was tied to “pawbug[.]com”, which PACT independently confirmed via pDNS.

IP 23.106.215[.]141 forms another link to the infrastructure detailed in RiskIQ’s report, via a link between “naverncorp[.]com” and “maloxob[.]com”. The domain “maloxob[.]com” was also identified as a Cobalt Strike C2 server. This IP address also led PACT’s analysts to another domain, cebuwu[.]com, which will be mentioned later in this report.

2. RiskIQ's analysis provided insight into the domain-generation algorithm and other TTPs of the Threat Actor operating the Cobalt Strike infrastructure. This insight led PACT to make note of two domains that aligned with RiskIQ's assessment of the actor's TTPs: cebuwu[.]com and lertwo[.]com. These two domains overlapped with previous reporting in the following ways:
 - They are between six to eight alphabetic characters in length, which aligns with the Domain Generation Algorithm (DGA) likely used by the threat actor(s).
 - They utilize the ".COM" top level domain (TLD).
 - The domain cebuwu[.]com used the legitimate Certificate Authority "Sectigo".
 - The domain cebuwu[.]com was identified via 23.106.215[.]141, which also links another Cobalt Strike C2 domain reported by RiskIQ (maloxob[.]com) and the Naver-themed activity (via naverncorp[.]com).
 - Likewise, past resolutions link the domain lertwo[.]com to both the Cobalt Strike C2 activity (195.186.208[.]193, 195.186.210[.]241) as well as the naver activity (navrcorp[.]site, navrcorps[.]online, navertechp[.]online). It is likely that these resolutions are the result of shared hosting or a pooled resource with many customers but the overlap is notable nonetheless, as it may indicate an operator preference or behavioral TTP.
3. Investigation of critical node IP 172.93.201[.]253 lead to the discovery of the domain disneycareers[.]net; which appears to be a convincingly crafted mockup of Disney's legitimate careers page: jobs.disneycareers[.]com. The mock site, in addition to being flagged as malicious by Google's Safebrowsing service, is notably *not* served on Akamai's network, nor is it registered with CSC CORPORATE DOMAINS, INC. (as Disney's legitimate site is) but by Namecheap. During the course of investigation the mock site's appearance changed notably, possibly indicating active development. Additionally, the TLS certificate was issued by Sectigo, which matches the behavior noted above regarding the Certificate Authority of choice for the Cobalt Strike C2 domains. The purpose of this mockup domain is unknown, *but the criminal nexus around the rest of the connected infrastructure should be enough to warrant additional scrutiny and could perhaps indicate specific targeting.*

IIIb. Takeaways

PACT concludes it is *highly likely* that the Naver-themed phishing activity is operationally linked to the Cobalt Strike infrastructure identified by RiskIQ (and mentioned by Microsoft). Additionally, PACT wishes to reiterate that these findings may not necessarily mean that WIZARD SPIDER is conducting the discrete clusters of activity that have been identified on this infrastructure. The fact that this infrastructure has been used to close several different links in the killchain across multiple campaigns (and perhaps by separate actors), coupled with the observations detailed by RiskIQ and Microsoft, may lend additional credence to the hypotheses they put forth. It is worth quoting both firms at some length.

Risk IQ states:

- "Despite the historical connections [between WIZARD SPIDER and the Cobalt Strike C2 infrastructure], we cannot say with confidence that the threat actor behind the zero-day campaign is part of WIZARD SPIDER or its affiliates, or is even a criminal actor at all, though it is possible."
- "The overlap with known ransomware infrastructure in this case could mean one of several things. First, that the zero-day operators compromised the infrastructure of the ransomware operators. Second, that the criminal operators are allowing the zero-day operators to piggyback on their existing infrastructure. Third, that the zero-day and ransomware operators are one and the same but engaging in espionage instead of financial crime. Finally, it could mean that both entities could be utilizing the same third party providing Bulletproof Hosting services. *There is strong ancillary evidence that suggests this is the case.*" (emphasis PACT's)

Furthermore, Microsoft states:

“The infrastructure we associate with DEV-0365 has several overlaps in behavior and unique identifying characteristics of Cobalt Strike infrastructure that suggest it was created or managed by a distinct set of operators. However, the follow-on activity from this infrastructure indicates multiple threat actors or clusters associated with human-operated ransomware attacks (including the deployment of Conti ransomware). One explanation is that DEV-0365 is involved in a form of command- and-control infrastructure as a service for cybercriminals.”

PACT’s findings reinforce these assessments: this infrastructure appears to support separate, discrete campaigns; it also supports operational mechanisms along multiple links of the killchain: it has hosted phishing domains, initial exploitation tools, and C2 servers.

PACT found the latter especially notable, as the Naver-themed phishing activity that was initially discovered does not appear to be the work of a ransomware group directly. In many cases, pre-ransomware activity (such as mass phishing and credential gathering activity) is handled by affiliates or brokers who provide access to the ransomware operators, while post-compromise activities, ransomware development, and deployment/encryption are executed by yet other groups. This separation of duties is not uncommon within the Ransomware-as-a-Service (RaaS) criminal business model. Similar to what Microsoft and RiskIQ reported, PACT’s findings regarding the additional “uncertainty surrounding the nature of the shared qualities” of this infrastructure and the “significant variation in malicious activity” strengthen the hypotheses that both firms put forward: multiple entities could be utilizing the same third party providing “bulletproof hosting” services to conduct their operations. PACT was unable to refute this hypothesis, and so assesses with moderate confidence that an as-yet unreported criminal hosting service exists on this infrastructure. The only links that PACT was able to identify were hosting and DNS resolutions; no other operational mechanisms provided links to the reported WIZARD SPIDER activity (such as registrants, malicious samples, etc). Therefore, a novel and emerging “infrastructure as a service for cybercriminals” fits the available evidence.

A third hypothesis, which PACT finds unlikely, is that multiple operators are leveraging a third party’s compromised infrastructure to support their own discrete and unrelated campaigns. The relatively limited, publicly available information on the IP addresses that make up the core of the operational infrastructure seems to indicate an operator that adheres to strict operational security measures. Legitimate entities rarely have so little publicly available or accessible information on their available services on a given IP address. This fact, along with the historic overlaps in hosting combined with other observations, led PACT to find this final hypothesis improbable.

References:

Annex: Detection Opportunities & Indicators of Compromise

New Naver-themed phishing domains, identified with 30 Mar 2022 update:

navenidd[.]site	navercomg[.]link	naverbcom[.]link	naveracom[.]link
navreplyg[.]site	navreplyi[.]site	navercomh[.]link	navreplyb[.]live
navercomb[.]link	naverbnid[.]live	navernidc[.]link	navenidb[.]live
navernidd[.]online	navreplyk[.]site	navenidc[.]live	navernidb[.]link
navercome[.]link	navreplye[.]live	naverccom[.]link	navernidc[.]tech
nidnavera[.]online	navreplyf[.]site	nidnavere[.]online	navernidd[.]live
navreplyj[.]site	navernida[.]link	navercomc[.]link	navreplyd[.]live

naveranid[.]link	navercoma[.]link	navercomf[.]link	navercomd[.]link
navreplya[.]online	navreplyh[.]site	navercnid[.]link	
navreplya[.]live	navenida[.]live	navernida[.]tech	
acc-center.site	naveewteam.site	navermailservice.host	navportal.online
acks.tech	naveloga.online	navermailservice.online	navportalcenter.site
centersecurity.link	navelosa.host	navermailservice.site	navportalcorp.site
cloudalarm.online	naveoccorp.link	navermailteam.online	navportalsec.site
cloudalarm.site	naveoccorp.online	navermanage.com	navportalsecs.site
cloudalarm.space	naveocenter.link	navermanage.live	navportalservice.site
cloudalarm.tech	naveocop.link	navermanage.online	navrcenter.site
cloudalarm.website	naveocorp.link	navermanage.space	navrcorp.site
cloudalarm.xyz	naveocorp.online	navermanagecorp.online	navrcorp.tech
cloudcentre.online	naveocorp.site	navermanagecorp.site	navrcorp.xyz
cloudcentre.site	naveocorp.tech	navermanager.online	navrpcenter.site
cloudcentre.space	naveocorp.website	navermanager.site	navrrcorp.site
cloudcentre.store	naveocorps.link	navermanagerteam.site	navrrcorp.tech
cloudcentre.tech	naveoecorp.tech	navermanageteam.com	navsceteam.site
cloudcentre.website	naveogains.tech	navermcorp.com	navseccenter.site
cloudcentre.xyz	naveolink.online	navermgr.site	navseccorp.link
corpcenternav.site	naveologs.online	navermgr01.host	navseccorp.online
corpnavcenter.site	naveoocorp.online	navermgr01.site	navseccorp.site
corpnavsec.site	naveoocorp.link	navermgr02.site	navsecncenter.site
corprsecurity.tech	naveoocorp.online	naverncorp.com	navsecnet.online
corpseccenter.site	naveoocorp.site	navernidcorp.com	navsecorg.tech
corpsecnav.site	naveoocorp.xyz	navernidcorp.online	navsecportal.site
corpsecservice.site	naveoorcorp.link	navernidcorp.site	navsecportal.tech
havcorp.site	naveorcorp.host	navernidlog.live	navsecportals.tech
havecorp.link	naveorcorp.link	navernidmail.com	navsecsite.tech
havecorp.tech	naveorcorp.online	navernidmail.online	navsecteam.tech
havecorp.site	naveorcorp.site	naverocenter.site	navsecteam.website
haveorcorp.tech	naveorcorp.tech	naveroCorp.link	navsecuritycenter.site

havercorp.site	naveorrcorp.online	naverocorp.online	navsecuritycenter.tech
havercorp.tech	naveorrcorp.tech	naverocorp.site	navsecuritycorp.link
havercorps.site	naveorseccorp.link	naverocorp.tech	navsecuritycorp.site
havercorpteam.site	naveorteam.site	naverocorpteam.site	navsecurityportal.online
haveroCorp.link	naveoscorp.link	naveronavteam.site	navsecurityteam.tech
havooCorp.online	naveoteam.online	naveroocorp.link	navsecvcorp.online
havooCorp.tech	naveoteam.site	naveroocorp.site	navsecvteam.site
havorcorp.link	naver-accounts.com	naverooteam.site	navserveportal.site
havorcorp.online	naver-sec.net	naverooteam.tech	navservicecenter.site
havorcorp.site	naver-sec.org	naverorcorp.tech	navservicescenter.online
havorcorp.tech	naver-security.net	naverorg.site	navserviceteam.com
havorcorpsv.online	naver-security.org	naverorteam.link	navserviceteam.site
mailcontactteam.online	naver-services.com	naverorteam.online	navserviceucenter.site
mailcorp.site	naveradmin.online	naveroscope.tech	navservicevcenter.site
mailcorpcenter.online	naveradmin00.tech	naveroteam.online	navsite.online
mailcorpcenter.site	naveradmin01.link	naveroteam.tech	navsvcorp.tech
mailcustomerservice.site	naveradmin01.site	naverovocorp.site	navsvportal.tech
mailhelp.online	naveradmin02.site	naverovvcorp.tech	navteam.online
mailmanagecorp.online	naveradmin03.site	naverrcorp.site	navteamcorp.link
mailmanagecorp.site	naveradmin04.tech	naverredda.xyz	navvcenter.online
mailmanageservice.com	naveradmin05.site	naverreddb.xyz	navvcorp.host
mailmanageteam.com	naveradmin06.online	naverreddc.xyz	navvcorp.link
mailmanageteam.site	naveradmin07.site	naverreddd.xyz	navvcorp.online
mailmangecorp.us	naveradmina.tech	naverrede.xyz	navvcorp.site
mailportalcenter.online	naveralert.link	naverredirect.live	navvctr.link
mailportalcenter.site	naveranid.live	naverrteam.site	navvctr.site
mailscropcenter.site	naverccorp.com	naversec.site	navvctr.tech
mailsecurity.email	navercert.live	naversecurity.site	navvctvr.site
mailservice.digital	navercert.online	naversecurityservice.online	navveoocorp.online
mailservice.host	navercoa.store	naversecurityteam.com	navvocorp.online
mailservicecenter.site	navercob.store	naverservice.email	navvocorp.site

mailservicecenters.site	navercoc.store	naverservice.host	navvrcorp.site
mailservicecorp.online	navercod.store	naverservice.link	navvsecurity.site
mailservicecorp.site	navercoc.store	naverservice.online	navvtr.site
mailservicemanage.com	navercoma.tech	naverservice.site	navvtrr.site
mailserviceteam.com	navercomb.tech	naverservicecorp.com	navvtrs.site
mailserviceteam.email	navercomc.tech	naverservicecorp.online	navvtrw.site
mailserviceteam.host	navercomd.tech	naverservicecorp.site	nevercorp.online
mailserviceteam.online	navercome.tech	naverserviceteam.com	nevercorp.site
mailserviceteam.site	navercop.link	naverserviceteam.email	nevercorp.tech
mailteam.site	navercop.online	naverserviceteam.site	neverrcorp.tech
msite.host	navercorp.email	navertcorp.com	nidanaver.tech
naswsteam.site	navercorp.live	naverteam.live	nidbnaver.tech
nauercorp.site	navercorp.site	naverteam.site	nidcnaver.com
nauercorp.website	navercorpa.tech	naverteam01.site	nidcnaver.tech
nauercorpa.online	navercorpa.website	naverteamcorp.com	niddnaver.tech
nauercorpb.online	navercorpb.online	naverteamcorp.live	nidinaver.com
nauercorpc.online	navercorpb.tech	naverteamcorp.site	nidnavcenter.link
nauercorpd.online	navercorpb.website	navertecha.host	nidnavcenter.online
nauercorpteam.website	navercorpc.online	navertechb.site	nidnavcenter.site
nauermanager.website	navercorpc.tech	navertechc.email	nidnavportal.site
navaccountcenter.online	navercorpc.website	navertechd.net	nidnavscenter.xyz
navadmin.site	navercorpd.online	naverteche.link	nidnavsecurity.tech
navadmin01.site	navercorpd.tech	navertechf.host	nidpavsec.digital
navcen.site	navercorpd.website	navertechg.site	nidportalnav.online
navcenter.xyz	navercorpe.online	navertechh.online	nidseccenter.host
navcenterportal.site	navercorpe.tech	navertechi.link	nidseccenter.site
navcopcenter.tech	navercorpe.website	navertechj.host	nidsecuritycenter.online
navcorp.host	navercorpf.online	navertechk.site	nidsecuritycorp.tech
navcorp.link	navercorpf.tech	navertechl.online	noreplya.online
navcorp.space	navercorpf.website	navertechm.link	noreplya.site
navcorp.website	navercorpg.online	navertechn.host	noreplya.space

navcorpcenter.site	navercorpg.tech	navertecho.site	noreplya.tech
navcorpcenter.site	navercorpg.website	navertechp.online	noreplya.website
navcorpctr.online	navercorph.online	navertechq.link	noreplya.xyz
navcorpctr.site	navercorph.tech	navertechr.host	noreplyb.online
navcorpmanage.site	navercorph.website	navertechs.site	noreplyb.site
navcorpmanager.site	navercorpi.online	navertecht.online	noreplyb.space
navcorpmanager.website	navercorpi.tech	navertechu.link	noreplyb.store
navcorpportal.xyz	navercorpj.online	naverurl.xyz	noreplyb.tech
navcorps.site	navercorpj.tech	navervteam.site	noreplyb.website
navcorps.website	navercorpk.online	naveservice.site	noreplyb.xyz
navcorpscenter.site	navercorpk.tech	navevcorp.link	novercorp.site
navcorpsecurity.site	navercorpl.online	navevcorp.online	nvrcoipa.link
navcorpserver.site	navercorpl.tech	navevcorp.site	nvrcoipb.link
navcorpsservice.site	navercorpm.online	navevrcorp.online	nvrcoipc.link
navcorpsservice.website	navercorpmanager.online	navhelp.online	nvrcope.site
navcorpssite.online	navercorpn.online	navmailcenter.site	nvrcoipf.site
navcorpsssec.tech	navercorpo.online	navmailcorp.site	nvrcoiponline
navcorpssupport.site	navercorpp.online	navmailserver.site	nvrjcop.online
navcorpsteam.online	navercorpq.online	navmanage.online	nvsctr.site
navcorpsteam.site	navercorpr.online	navmanager.site	portalcorpsec.site
navcorpsteam.website	navcorps.online	navmanager.website	portalcorpsteam.com
navcpcenter.site	navercorpsservice.com	navocorp.link	portalseccorps.site
navctr.online	navercorpt.online	navocorp.site	portalserver.online
navctrv.site	navercorpsteam.com	navocorp.tech	scientisttest.digital
navcvcorp.online	navercorpsteam.online	navoercorp.host	seccenter.link
naveacorp.tech	navercorpu.online	navoercorp.link	seccenter.online
naveccorp.link	navercorpv.online	navoercorp.site	seccorp.link
navecorp.host	navercorpw.online	navoocorp.link	secmanageteam.site
navecorp.online	navercorpx.online	navoocorp.online	secnavportal.digital
navecorp.site	navercorpy.online	navoocorp.site	secportal.digital
navecorp.website	navercorz.online	navoorcorp.link	secportal.link

naveecorp.tech	navercscorp.com	navoorcorp.online	secportalnav.site
naveecorp.link	naverdoc.site	navoorcorp.site	secportals.digital
naveecorp.online	naverhost.live	navorcorp.site	secportalsnav.site
naveecorp.site	naverkr.online	navorcorp.link	securitycenter.site
naveecorp.tech	naverlogn.live	navorcorp.online	securitycenter.link
naveecorp.xyz	navermail.site	navorcorp.xyz	securitycenter.space
naveecorp.site	navermailcorp.com	navorcorpteam.site	securitynavcenter.site
naveecorp.xyz	navermailcorp.host	navovcorp.online	securitynavcenter.tech
naveeocorp.link	navermailcorp.online	navovcorp.site	securityvcenter.site
naveeorcorp.tech	navermailcorp.site	navovcorp.tech	sercureteam.site
naveeoteam.site	navermailmanage.com	navpcenter.online	setcenter.store
naveercorp.online	navermailservice.com	navpcenter.site	shtlink.online