What Wicked Webs We Un-weave

3/15/2022

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.

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 actor[4].

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

IIa: 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.
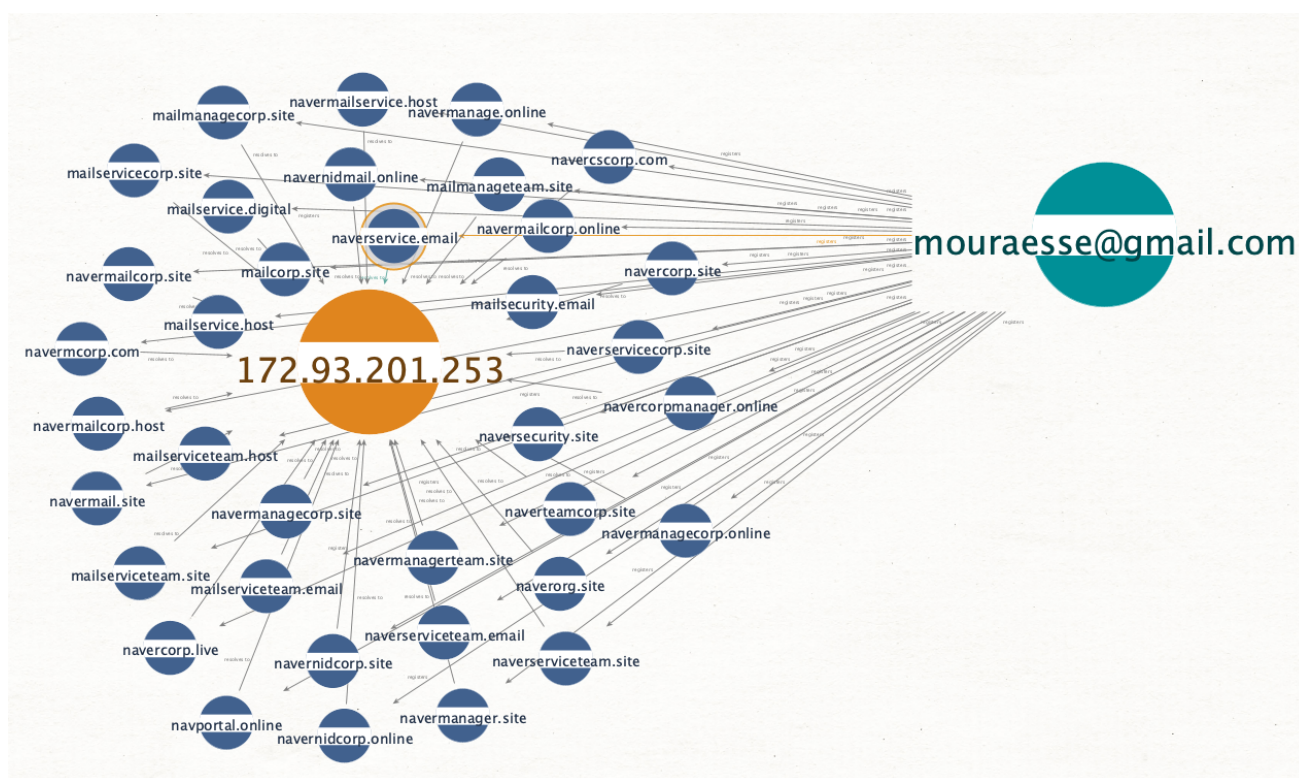
Image 1: Numerous domains registered by mouraesse@gmail[.]com resolved to 172.93.201[.]253

*note: PACT defines "critical nodes" as entities on a graphical link analysis chart that were instrumental in identifying connections between several, otherwise distinct, clusters of entities and activity.

This IP also provided the first glimpse of a recurring TTP (tactic, technique, or procedure) that PACT identified as an indicator to strengthen confidence in clustering this activity together: HTTP/302 redirects to spoofed Naver login pages on Hostinger's web hosting platform "000webhostapp[.]com", as seen below –

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.
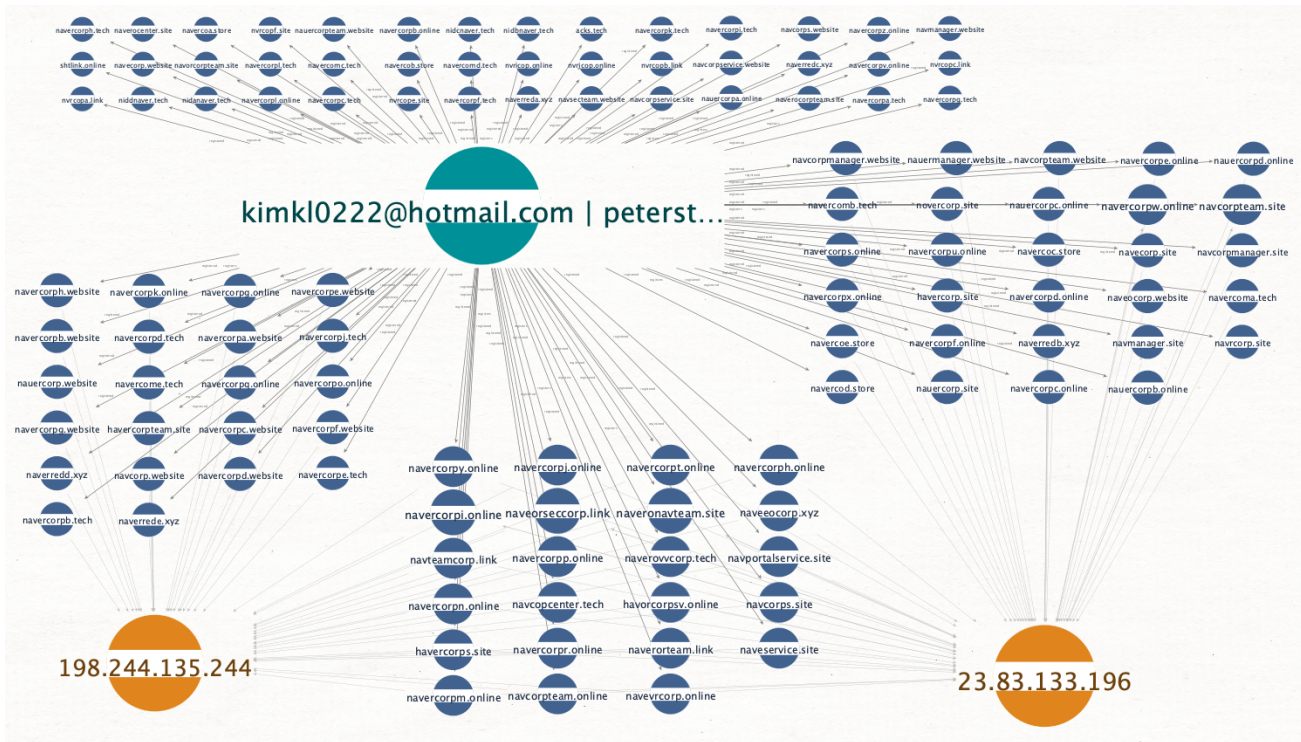
Image 3: Persona behind email addresses "peterstewart0326@gmail[.]com" and "kimkl0222@hotmail[.]com" shown along with Naver-themed domain registrations and the associated resolutions.

- IP addresses:
    - 23.83.133[.]196:
        - Part of ASN 19148 (LeaseWeb USA, Inc.), along with critical node 23.81.246[.]131
        - Linked via pDNS resolutions to many domains registered by the "kimkl0222@hotmail[.]com / peterstewart0326@gmail[.]com" actor
    - 198.244.135[.]244:
        - Part of ASN 16276 (OVH SAS), along with critical node "15.235.132[.]77", seen below
        - Linked via pDNS resolutions to many domains registered by the "kimkl0222@hotmail[.]com / peterstewart0326@gmail[.]com" actor
        - Displayed TTP overlap (IP seen serving HTTP/302 redirects to Naver phishing pages):

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

🔍 Lookup ▾ | ➜ Go To | ⟳ Rescan
💬 Add Verdict | ❶ Report

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 **navercorpd.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: ❶ Malicious for *navercorpd.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 "kimkl0222@hotmail[.]com / peterstewart0326@gmail[.]com" actor that allowed PACT to identify additional WHOIS domain registrant "gameproducters@outlook[.]com"
- 108.177.235[.]15
  - Part of ASN 395954 (Leaseweb USA, Inc.)
  - Provided overlap with domains registered by the "kimkl0222@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):



```
// 80 / TCP                                          -146016816 | 2022-02-11T15:31:16.224664

Apache httpd 2.4.51

HTTP/1.1 302 Found
Date: Fri, 11 Feb 2022 15:31:15 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.11 PHP/7.4.25
X-Powered-By: PHP/7.4.25
Location: https://naverdmail.000webhostapp.com?ref=
Content-Length: 103
Content-Type: text/html; charset=UTF-8
```

```
// 443 / TCP                                         -146016816 | 2022-02-11T15:31:32.133850

Apache httpd 2.4.51

HTTP/1.1 302 Found
Date: Fri, 11 Feb 2022 15:31:31 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.11 PHP/7.4.25
X-Powered-By: PHP/7.4.25
Location: https://naverdmail.000webhostapp.com?ref=
Content-Length: 103
Content-Type: text/html; charset=UTF-8

SSL Certificate

Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            b5:c7:52:c9:87:81:b5:03
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=localhost
        Validity
            Not Before: Nov 10 23:48:47 2009 GMT
            Not After : Nov  8 23:48:47 2019 GMT
        Subject: CN=localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

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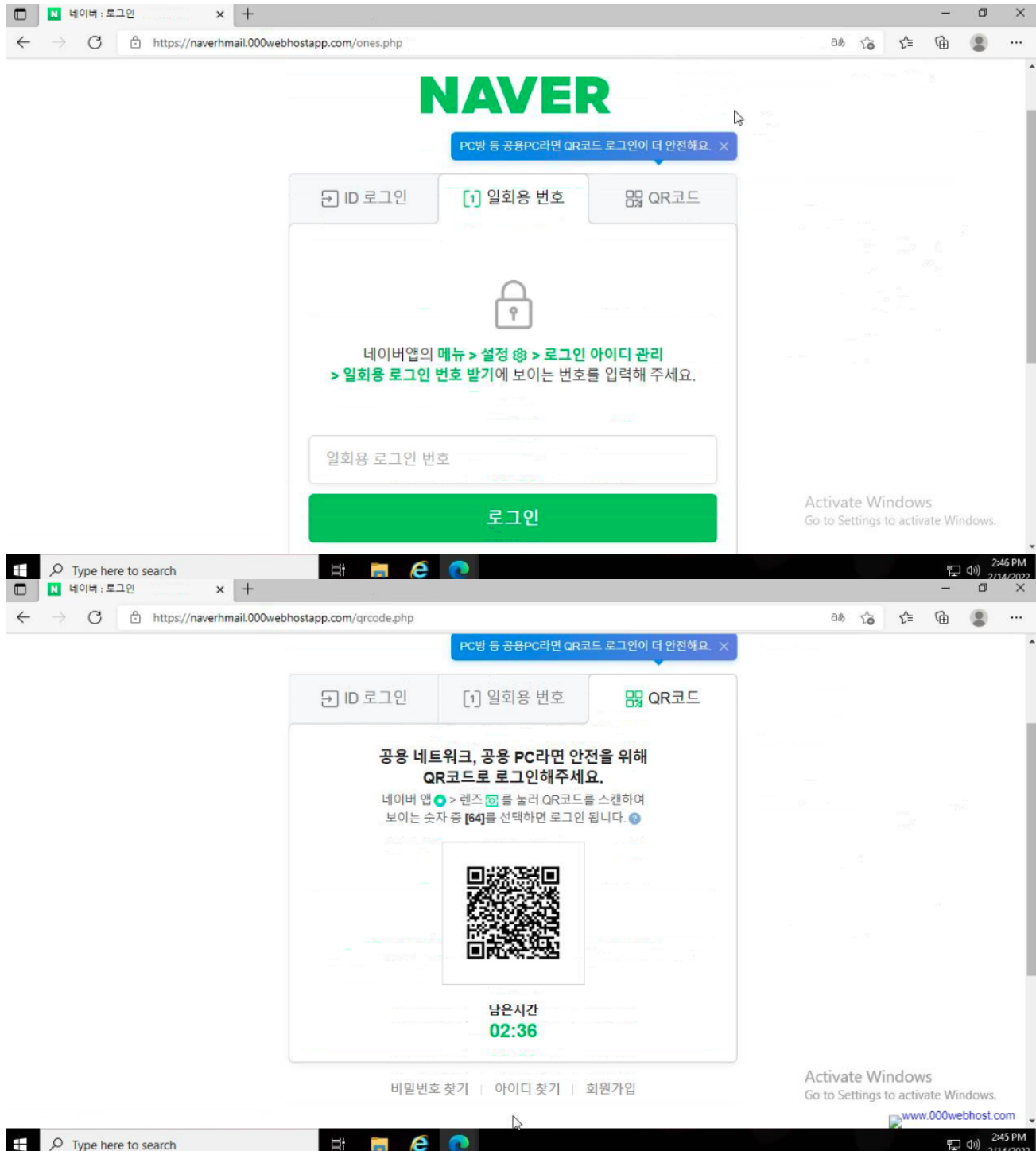
6 & 7: the Naver phishing pages PACT analyzed supported one-time-password and QR code functionality

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	0b4b1f2af5257c0aa79fda9b75accef9f4d6181b6d80eea5a1740460ab8514ae.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.
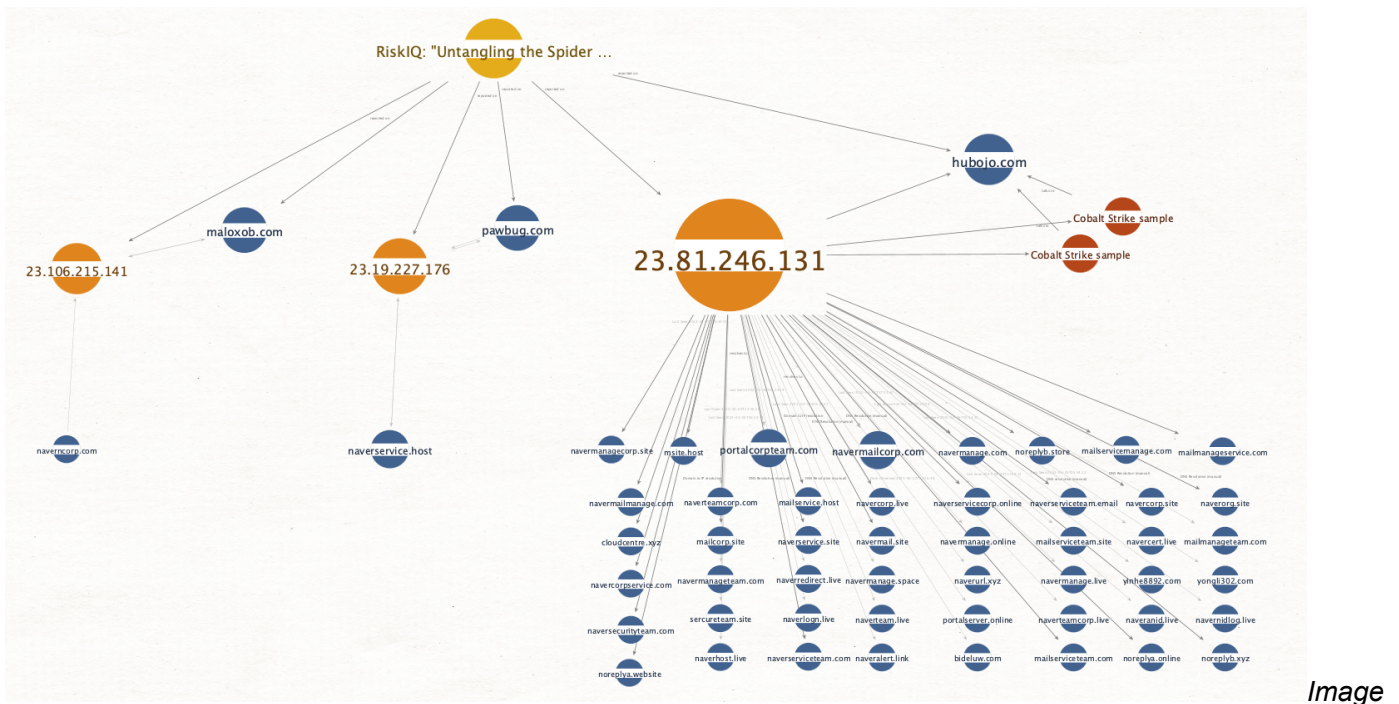
Image
9: Critical overlaps between RiskIQ's previous findings & the Naver-themed phishing activity.

Further overlaps were identified with two additional IP addresses that are likely to be shared resources**:

1. 184.168.221[.]39: ties together "mailhelp[.]online" (part of the cluster targeting Naver) with "jumpbill[.]com" and "raills[.]com" (reported as Cobalt Strike C2s by RiskIQ).
2. 195.186.208[.]193: ties together at least two of the domains seen in the Naver phishing activity ("navrcorp[.]site" & "navercorps[.]online") and dozens of the Cobalt Strike domains reported by RiskIQ

**Given the number of (apparently unrelated) resolutions recorded on these IPs, it is likely they are, or were, legitimate shared hosting or another pooled resource being abused by a small number of malicious actors. Nevertheless, the many links they formed helped increase PACT's confidence in assessing this activity as related; therefore, PACT included them in this report.

Part III: Closing Thoughts & Key Takeaways

IIIa. Analytic Gaps & Anomalous Findings

While analyzing and processing the information uncovered in this investigation, PACT identified a number of outliers and anomalies. They appear below in no particular order:

1. The majority of the domains identified within the Naver-phishing cluster of activity were registered *without privacy protection*; i.e., it was trivial for analysts to search for other domains registered with the same registrant information (e.g., email address). WHOIS Privacy and GDPR have made privacy a de facto standard during the domain registration process. It is uncommon to find a cluster of activity, especially one that is attributable to a named threat group like WIZARD SPIDER, wherein all the domain-based infrastructure is unobscured by privacy protection services.
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, navercorps[.]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

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	naveooccorp.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
havcorp.site
havecorp.link
havecorp.tech
haveecorp.site
haveorcorp.tech
havercorp.site
havercorp.tech
havercorps.site
havercorpteam.site
haverocorp.link
havoocorp.online
havoocorp.tech
havorcorp.link
havorcorp.online
havorcorp.site
havorcorp.tech
havorcorpsv.online
mailcontactteam.online
mailcorp.site
mailcorpcenter.online
mailcorpcenter.site
mailcustomerservice.site
mailhelp.online
mailmanagecorp.online
mailmanagecorp.site
mailmanageservice.com
mailmanageteam.com
mailmanageteam.site
mailmangecorp.us
mailportalcenter.online
mailportalcenter.site
mailscropcenter.site
mailsecurity.email
mailservice.digital
mailservice.host
mailservicecenter.site
mailservicecenters.site
mailservicecorp.online
mailservicecorp.site
mailservicemanage.com
mailserviceteam.com
mailserviceteam.email
mailserviceteam.host
mailserviceteam.online
mailserviceteam.site
mailteam.site
msite.host
naswsteam.site
nauercorp.site
nauercorp.website
nauercorpa.online

naveoorcorp.link
naveorcorp.host
naveorcorp.link
naveorcorp.online
naveorcorp.site
naveorcorp.tech
naveorrcorp.online
naveorrcorp.tech
naveorseccorp.link
naveorteam.site
naveoscorp.link
naveoteam.online
naveoteam.site
naver-accounts.com
naver-sec.net
naver-sec.org
naver-security.net
naver-security.org
naver-services.com
naveradmin.online
naveradmin00.tech
naveradmin01.link
naveradmin01.site
naveradmin02.site
naveradmin03.site
naveradmin04.tech
naveradmin05.site
naveradmin06.online
naveradmin07.site
naveradmina.tech
naveralert.link
naveranid.live
naverccorp.com
navercert.live
navercert.online
navercoa.store
navercob.store
navercoc.store
navercod.store
navercoe.store
navercoma.tech
navercomb.tech
navercomc.tech
navercomd.tech
navercome.tech
navercop.link
navercop.online
navercorp.email
navercorp.live
navercorp.site
navercorpa.tech
navercorpa.website

navernidcorp.site
navernidlog.live
navernidmail.com
navernidmail.online
naverocenter.site
naverocorp.link
naverocorp.online
naverocorp.site
naverocorp.tech
naverocorpteam.site
naveronavteam.site
naveroocorp.link
naveroocorp.site
naverooteam.site
naverooteam.tech
naverorcorp.tech
naverorg.site
naverorteam.link
naverorteam.online
naveroscope.tech
naveroteam.online
naveroteam.tech
naverovocorp.site
naverovvcorp.tech
naverrcorp.site
naverreda.xyz
naverredb.xyz
naverredc.xyz
naverredd.xyz
naverrede.xyz
naverredirect.live
naverrteam.site
naversec.site
naversecurity.site
naversecurityservice.online
naversecurityteam.com
naverservice.email
naverservice.host
naverservice.link
naverservice.online
naverservice.site
naverservicecorp.com
naverservicecorp.online
naverservicecorp.site
naverserviceteam.com
naverserviceteam.email
naverserviceteam.site
navertcorp.com
naverteam.live
naverteam.site
naverteam01.site
naverteamcorp.com

navsecportal.tech
navsecportals.tech
navsecsite.tech
navsecteam.tech
navsecteam.website
navsecuritycenter.site
navsecuritycenter.tech
navsecuritycorp.link
navsecuritycorp.site
navsecurityportal.online
navsecurityteam.tech
navsecvcorp.online
navsecvteam.site
navserveportal.site
navservicecenter.site
navservicescenter.online
navserviceteam.com
navserviceteam.site
navserviceucenter.site
navservicevcenter.site
navsite.online
navsvcorp.tech
navsvportal.tech
navteam.online
navteamcorp.link
navvccenter.online
navvcorp.host
navvcorp.link
navvcorp.online
navvcorp.site
navvctr.link
navvctr.site
navvctr.tech
navvctvr.site
navveoocorp.online
navvocorp.online
navvocorp.site
navvrcorp.site
navvsecurity.site
navvtr.site
navvtrr.site
navvtrs.site
navvtrw.site
nevercorp.online
nevercorp.site
nevercorp.tech
neverrcorp.tech
nidanaver.tech
nidbnaver.tech
nidcnaver.com
nidcnaver.tech
niddnaver.tech

nauercorpb.online
nauercorpc.online
nauercorpd.online
nauercorpteam.website
nauermanager.website
navaccountcenter.online
navadmin.site
navadmin01.site
navcen.site
navcenter.xyz
navcenterportal.site
navcopcenter.tech
navcorp.host
navcorp.link
navcorp.space
navcorp.website
navcorpacenter.site
navcorpcenter.site
navcorpctr.online
navcorpctr.site
navcorpmanage.site
navcorpmanager.site
navcorpmanager.website
navcorpportal.xyz
navcorps.site
navcorps.website
navcorpscenter.site
navcorpsecurity.site
navcorpserver.site
navcorpservice.site
navcorpservice.website
navcorpsite.online
navcorpssec.tech
navcorpsuppot.site
navcorpteam.online
navcorpteam.site
navcorpteam.website
navcpcenter.site
navcrtr.online
navctrv.site
navcvcorp.online
naveacorp.tech
naveccorp.link
navecorp.host
navecorp.online
navecorp.site
navecorp.website
naveeccorp.tech
naveecorp.link
naveecorp.online
naveecorp.site
naveecorp.tech

navercorpb.online
navercorpb.tech
navercorpb.website
navercorpc.online
navercorpc.tech
navercorpc.website
navercorpd.online
navercorpd.tech
navercorpd.website
navercorpe.online
navercorpe.tech
navercorpe.website
navercorpf.online
navercorpf.tech
navercorpf.website
navercorpg.online
navercorpg.tech
navercorpg.website
navercorph.online
navercorph.tech
navercorph.website
navercorpi.online
navercorpi.tech
navercorpj.online
navercorpj.tech
navercorpk.online
navercorpk.tech
navercorpl.online
navercorpl.tech
navercorpm.online
navercorpmanager.online
navercorpn.online
navercorpo.online
navercorpp.online
navercorpq.online
navercorpr.online
navercorps.online
navercorpservice.com
navercorpt.online
navercorpteam.com
navercorpteam.online
navercorpu.online
navercorpv.online
navercorpw.online
navercorpx.online
navercorpy.online
navercorpz.online
navercscorp.com
naverdoc.site
naverhost.live
naverkr.online
naverlogn.live

naverteamcorp.live
naverteamcorp.site
navertecha.host
navertechb.site
navertechc.email
navertechd.net
naverteche.link
navertechf.host
navertechg.site
navertechh.online
navertechi.link
navertechj.host
navertechk.site
navertechl.online
navertechm.link
navertechn.host
navertecho.site
navertechp.online
navertechq.link
navertechr.host
navertechs.site
navertecht.online
navertechu.link
naverurl.xyz
navervteam.site
naveservice.site
navevcorp.link
navevcorp.online
navevcorp.site
navevrcorp.online
navhelp.online
navmailcenter.site
navmailcorp.site
navmailserver.site
navmanage.online
navmanager.site
navmanager.website
navocorp.link
navocorp.site
navocorp.tech
navoercorp.host
navoercorp.link
navoercorp.site
navoocorp.link
navoocorp.online
navoocorp.site
navoorcorp.link
navoorcorp.online
navoorcorp.site
navorcop.site
navorcorp.link
navorcorp.online

nidinaver.com
nidnavcenter.link
nidnavcenter.online
nidnavcenter.site
nidnavportal.site
nidnavscenter.xyz
nidnavsecurity.tech
nidpavsec.digital
nidportalnav.online
nidseccenter.host
nidseccenter.site
nidsecuritycenter.online
nidsecuritycorp.tech
noreplya.online
noreplya.site
noreplya.space
noreplya.tech
noreplya.website
noreplya.xyz
noreplyb.online
noreplyb.site
noreplyb.space
noreplyb.store
noreplyb.tech
noreplyb.website
noreplyb.xyz
novercorp.site
nvrcopa.link
nvrcopb.link
nvrcopc.link
nvrcope.site
nvrcopf.site
nvricop.online
nvrjcop.online
nvscetr.site
portalcorpsec.site
portalcorpteam.com
portalseccorps.site
portalserver.online
scientisttest.digital
seccenter.link
seccenter.online
seccorp.link
secmanageteam.site
secnavportal.digital
secportal.digital
secportal.link
secportalnav.site
secportals.digital
secportalsnav.site
securityccenter.site
securitycenter.link

naveecorp.xyz
naveeecorp.site
naveeocorp.xyz
naveeoocorp.link
naveeorcorp.tech
naveeoteam.site
naveercorp.online

navermail.site
navermailcorp.com
navermailcorp.host
navermailcorp.online
navermailcorp.site
navermailmanage.com
navermailservice.com

navorcorp.xyz
navorcorpteam.site
navovcorp.online
navovcorp.site
navovcorp.tech
navpcenter.online
navpcenter.site

securitycenter.space
securitynavcenter.site
securitynavcenter.tech
securityvcenter.site
sercureteam.site
setcenter.store
shtlink.online