

Tracking APT SideWinder Domains By Combining Regex Patterns, Whois Records and Domain Registrars

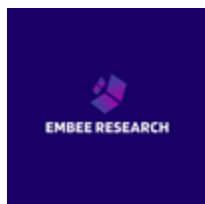
 embeerresearch.io/advanced-guide-to-infrastructure-analysis-tracking-apt-sidewinder-domains/

Matthew

May 23, 2024

Threat Intelligence Guides

Tracking APT SideWinder Domains With Regular Expressions, Whois Records and Domain Registrars



Matthew

May 23, 2024 - 16 min read

Threat Actors often leverage domain-based infrastructure to host and facilitate malicious operations. When actors deploy these new domains, they often leave patterns that can be used to signature the infrastructure and link it to past known activity.

Developing these signatures can be difficult, and there is little public documentation on how they can be performed. Today, we will look into a single domain indicator shared on X/Twitter and show you how to analyse it for patterns that lead to 36 additional domains.

Our final analysis will review these domains and link them with high confidence to public reports on APT SideWinder.

Overview

Before jumping in, here's a summary of what we'll cover in this blog.

- Obtaining initial intelligence (Domain) From Twitter/X
- Analysing the domain to find a pivot point
- Pivoting on regular expressions, dates and domain registrars
- Adjusting pivots to identify additional domains
- Parsing data output with CyberChef and JPATH
- Enriching output with WHOIS records
- Establishing patterns in subdomains
- Obtaining public intelligence reports to assist attribution
- Using public reports to link activity to APT SideWinder

Initial Intelligence

Our initial investigation begins with a single domain indicator shared by [DocGuard](#) in a recent post on X.

Note the domain's name of `docs.mofa-services-server[.]top` and consider that MOFA is an acronym for "Ministry of Foreign Affairs". This will become important later.



DOCGuard - Detect Maldocs in Seconds! 
@doc_guard

 Pakistan Prime Minister's Office Themed Phishing PDF File Evaded All the AV Solutions 

 VT Detection: 0 / 63

 Filename: Outstanding Payment of Tender upload fee - PPRA.pdf
 MD5: d4eb4cee8aeb6f2ea36afadeda9dbb23
 IOCs:
- http[:]//docs.mofa-services-server.top/
- (MD5) 38f96b882363cb659d4cabec49bf605c

Our initial indicator is a domain, so we can begin with domain-based analysis, such as a passive DNS lookup.

The aim here is to obtain historical records of IP addresses to which the domain has resolved. We want to use the IP addresses to find other domains associated with the same IP infrastructure.

Executing A Pivot On Our Initial Domain

Running a passive DNS lookup in [SilentPush](#), reveals that the domain currently resolves to an IP address of `188.114.97[.]3`. This IP is hosted by CloudFlare on [ASN 13335](#).

CloudFlare is a commercial and "legitimate" reverse proxy for network infrastructure. In the context of Threat investigations, Cloudflare effectively acts as a way of anonymising infrastructure as the attackers "real" server is hidden behind the CloudFlare proxy.

Since CloudFlare proxies are often shared between thousands of unrelated customers. This complicates the analysis process and hence it is regularly utilised by malicious actors.

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen
docs.mofa-services-server...	-	188.114.97.3	13335	2024-05-01 06:04:45	2024-05-01 06:04:45
docs.mofa-services-server...	-	188.114.96...	13335	2024-05-01 06:04:45	2024-05-01 06:04:45

We can try to find related domains by performing a passive DNS lookup for `188.114.97[.]3`, this will reveal any domains that have resolved to the same address.

Below is the passive DNS lookup for `188.114.97[.]3`, showing a large number of unrelated domains.

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	Type
7424ab97c0.sexypornycp.da...	-	188.114.97.3	13335	2023-11-30 19:44:29	2024-05-02 06:55:48	A
ok188kh.com	-	188.114.97.3	13335	2022-05-27 12:51:47	2024-05-02 06:55:47	A
interprime.online	-	188.114.97.3	13335	2023-09-08 11:03:12	2024-05-02 06:55:47	A
alishacortez.bellecams.co...	-	188.114.97.3	13335	2023-11-21 19:45:54	2024-05-02 06:55:47	A
johnathanmhcqvq.isblog.net	-	188.114.97.3	13335	2022-10-25 03:14:56	2024-05-02 06:55:47	A

Our screenshot above reveals that `801666666` domains have resolved to the same address.

As mentioned prior, this huge number of related domains is due to the usage of CloudFlare. We can narrow down the results by applying additional filters, but the number of results may still be in the 10's of thousands. Hence, we attempted a similar pivot on the parent domain to establish any easier patterns.

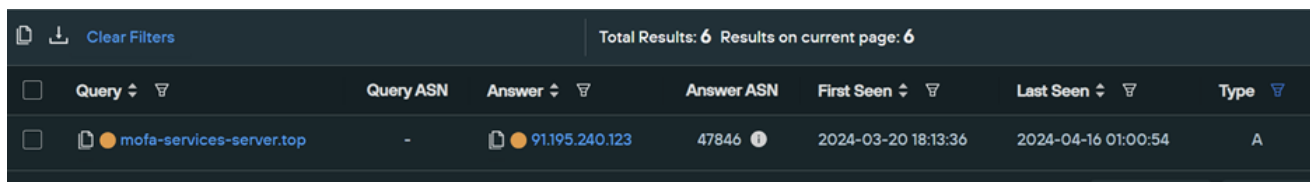
Since the parent domain is likely to be owned and controlled by the same actor, it can occasionally serve as a more accessible and more helpful pivot point.

Executing a Pivot On Our Parent Domain

Since pivoting on the initial `docs` subdomain had way too many results, we performed a similar lookup on the parent domain of `mofa-services-server[.]top`.

Parent domains aren't always given the same protection as subdomains, and since they are typically controlled by the same actor, they serve as a far more helpful pivot point.

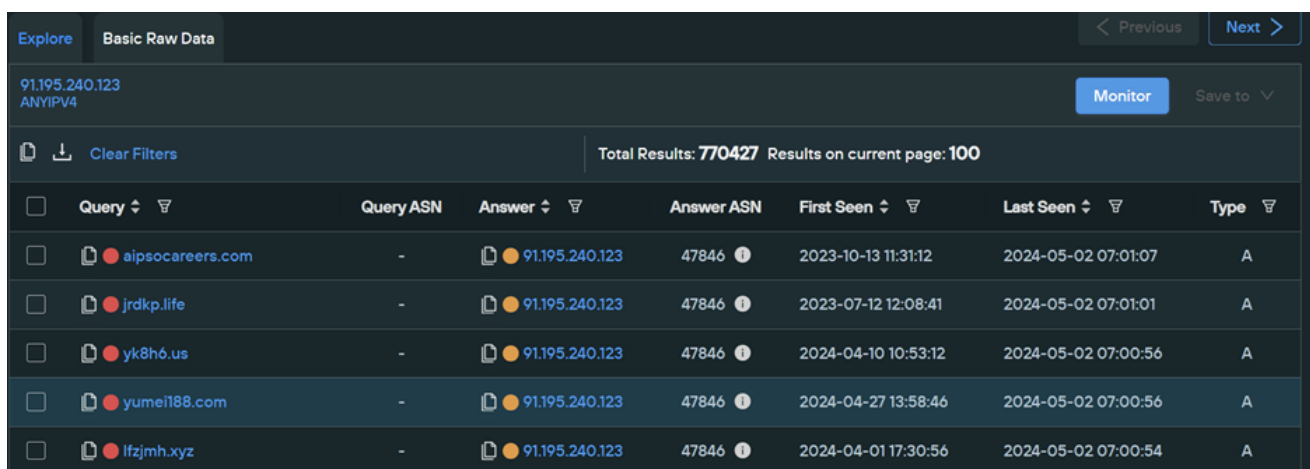
The parent domain of `mofa-services-server[.]top` has only one known IP of `91.195.240[.]123`, which is hosted on SEDO with ASN `47846`, and was first seen on `2024-03-20`.



Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	Type
<code>mofa-services-server.top</code>	-	<code>91.195.240.123</code>	<code>47846</code>	2024-03-20 18:13:36	2024-04-16 01:00:54	A

A passive DNS lookup on this new IP `91.195.240[.]123` will allow us to determine any domains that have shared the same address.

Performing this lookup identifies `770427` related domains. This is a huge number but significantly less than that of the original CloudFlare IP.



Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	Type
<code>aipsocareers.com</code>	-	<code>91.195.240.123</code>	<code>47846</code>	2023-10-13 11:31:12	2024-05-02 07:01:07	A
<code>jrdkp.life</code>	-	<code>91.195.240.123</code>	<code>47846</code>	2023-07-12 12:08:41	2024-05-02 07:01:01	A
<code>yk8h6.us</code>	-	<code>91.195.240.123</code>	<code>47846</code>	2024-04-10 10:53:12	2024-05-02 07:00:56	A
<code>yumei188.com</code>	-	<code>91.195.240.123</code>	<code>47846</code>	2024-04-27 13:58:46	2024-05-02 07:00:56	A
<code>lfzjmh.xyz</code>	-	<code>91.195.240.123</code>	<code>47846</code>	2024-04-01 17:30:56	2024-05-02 07:00:54	A

Since this is still a vast number, we can leverage regular expressions to apply additional filtering to narrow down our results. Performed correctly, this can significantly reduce the number of related domains to a manageable number.

(In this case, regular expressions will reduce the `770427` results down to only 6)

Building An Advanced Threat Intelligence Query

An advanced query allows us to apply specific filters that will significantly reduce the number of results. Before we can do this, we need to establish what exactly we will filter on.

Consider that we know the following information about `mofa-services-server[.]top`

- It's hosted on `91.195.240[.]123`
- It uses a `.top` Top Level Domain
- The domain name contains three words, separated by hyphens
- The domain was first observed on `2024-03-20`

An advanced query allows us to provide this information through date filters, network filters, and regular expressions. The below parameters are how they can be applied in SilentPush.

- `91.195.240[.]123` can be applied as a `qanswer` filter.
- TLD (`.top`) can be applied as `\.top$` to the end of a `domain_regex`
- Three words, separated by hyphens, can be applied as `^[a-z]{1,}\-[a-z]{1,}\-[a-z]{1,}` at the beginning of the `domain_regex`
- The first observed date can be applied as `first_seen_after=2024-03-18` and `first_seen_before=2024-03-22`, this allows for +/- 2 days of buffer on either side.

The complete regular expression used here is `^[a-z]{1,}\-[a-z]{1,}\-[a-z]{1,}\.top$` and if you are using `SilentPush`, the advanced query can be found in `Advanced Query Builder -> PADNS Queries -> Live Unsanctioned Assets Lookup`

Below we can see what this looks like with the filters applied.

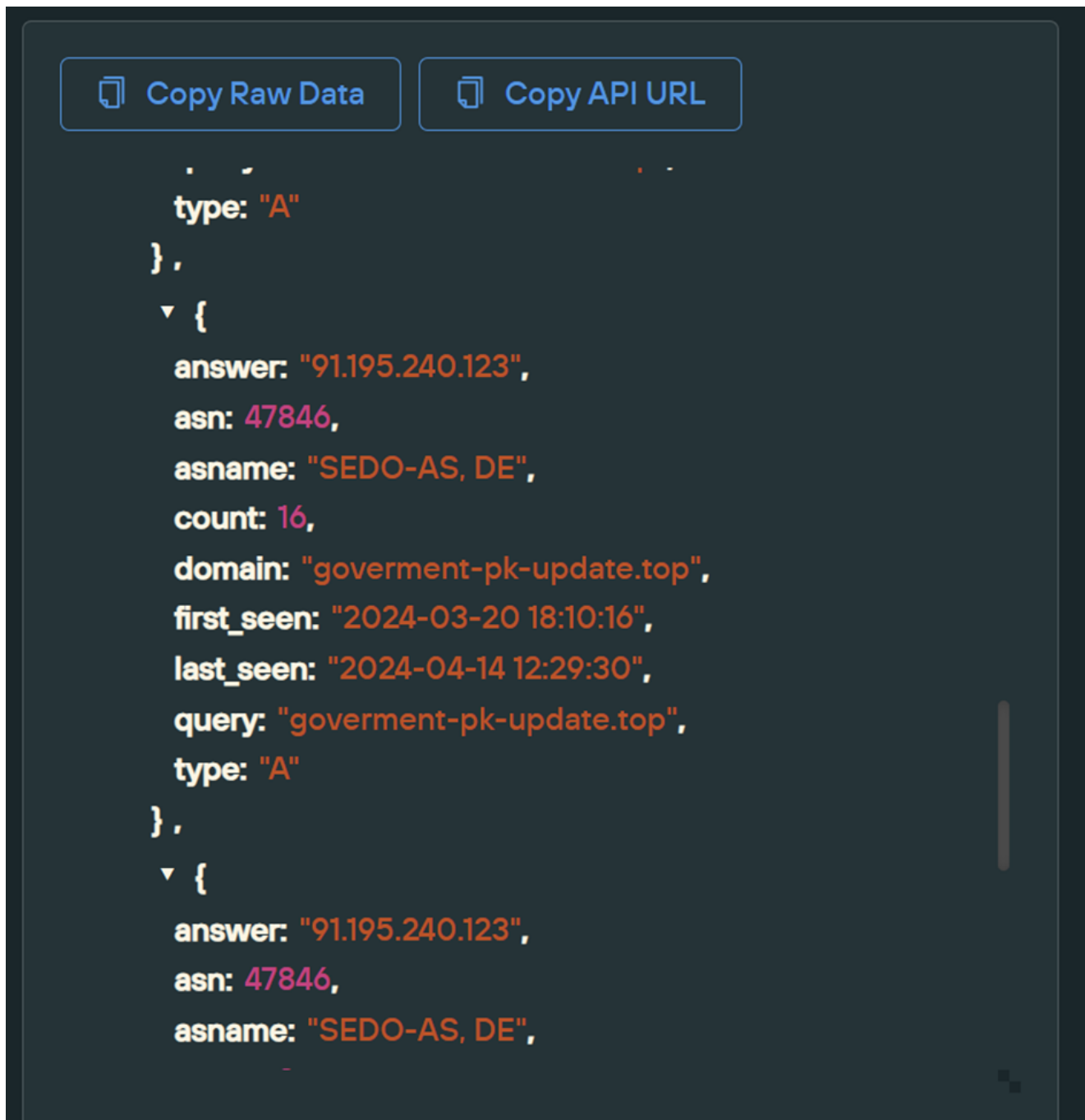
The screenshot shows the 'Advanced Query Builder' interface for 'Live Unsanctioned Assets Lookup'. The filters are organized into two columns:

- Left Column:**
 - `qtype*`: `A` and `AAAA`
 - `regex`: `^[a-z]{1,}\-[a-z]{1,}\-[a-z]{1,}\.top$`
 - `nsname`: (empty)
 - `with_metadata`:
 - `net`: `in` and `notin`
 - `asnum`: (empty)
 - `asname`: (empty)
 - `first_seen_before`: `2024-03-22`
 - `last_seen_before`: (empty)
- Right Column:**
 - `qname*`: `-`
 - `qanswer*`: `91.195.240.123`
 - `match`: `eq` and `neq`
 - `netmask`: (empty)
 - `network`: (empty)
 - `asn`: `in` and `notin`
 - `first_seen_after`: `2024-03-18`
 - `last_seen_after`: (empty)
 - `as_of`: (empty)

Applying these filters cuts the results down to only 7 domains. This is a great number and is significantly lower than the 770427 initially associated with the same IP 91.195.240[.]123. This means our filters were able to cut out 770420 results.

The 7 resulting domains contain recurring "PK" (Pakistan) themes and common acronyms for Government agencies.

Government themes were observed in our initial mofa-services-server[.]top indicator through mofa (Ministry of Foreign Affairs).



The screenshot shows a dark-themed interface with two buttons at the top: "Copy Raw Data" and "Copy API URL". Below the buttons is a JSON array of two objects. Each object contains the following fields: "type": "A", "answer": "91.195.240.123", "asn": 47846, "asname": "SEDO-AS, DE", "count": 16, "domain": "government-pk-update.top", "first_seen": "2024-03-20 18:10:16", "last_seen": "2024-04-14 12:29:30", and "query": "government-pk-update.top".

```
type: "A",
},
{
  answer: "91.195.240.123",
  asn: 47846,
  asname: "SEDO-AS, DE",
  count: 16,
  domain: "government-pk-update.top",
  first_seen: "2024-03-20 18:10:16",
  last_seen: "2024-04-14 12:29:30",
  query: "government-pk-update.top",
  type: "A"
},
{
  answer: "91.195.240.123",
  asn: 47846,
  asname: "SEDO-AS, DE",
```

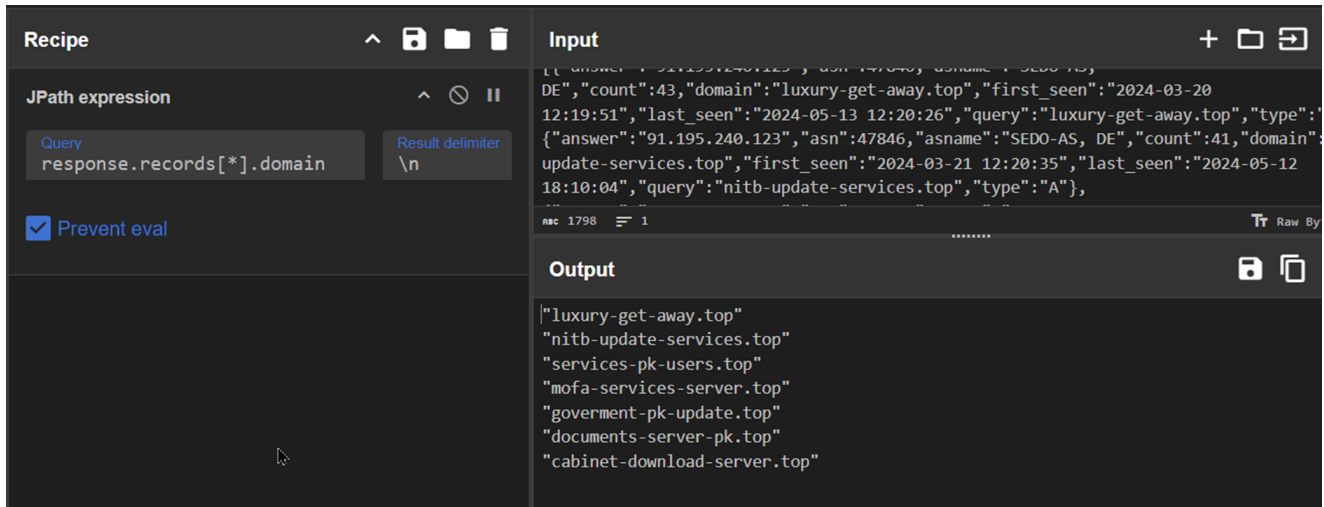
Parsing JSON Data With CyberChef and JPATH

The results are returned in JSON format and contain a huge amount of information. We only need the resulting domains (for now), so we can use Python or CyberChef to extract the domain field.

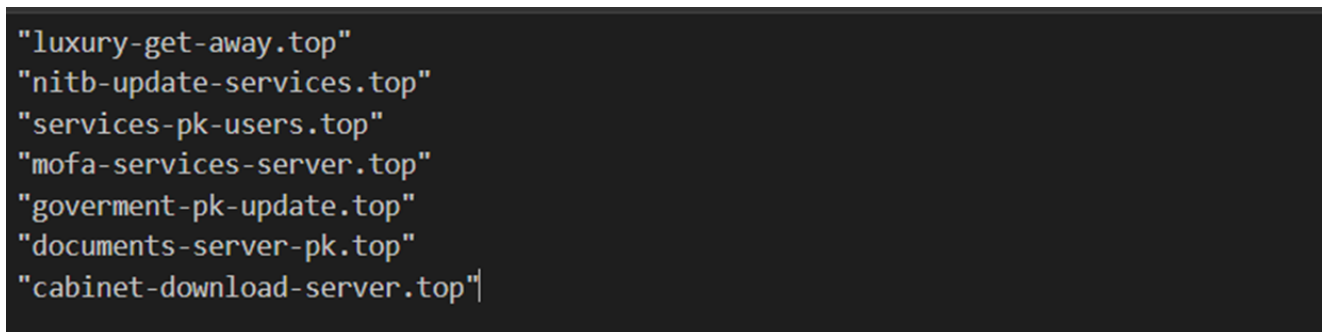
For the sake of simplicity, we leveraged CyberChef and a JPath expression to filter the JSON output to return the 7 resulting domains.

We achieved this with a JPath expression of `response.records[*].query`

| (If you're unfamiliar with JPath, [here](#) is an excellent tutorial for understanding it)



The 7 resulting domains can be seen clearly below.



The 7 domains have a recurring theme of Pakistan and Government agencies. We can also observe a recurring theme of IT Support services through mentions of updates, server, download and services.

(Later we'll see how these are TTPs of APT SideWinder)

- PK - Shortening of Pakistan
- NITB - National Information Technology Board
- MOFA - Ministry of Foreign Affairs
- Government - Misspelling of Government
- Cabinet - Decision-making arm of the Government

These similarities indicate that the domains are related and that we're onto something, especially given they share the same IP address and have close registration dates (as required by our filters)

So far, the domains share the same IP infrastructure, same naming schemes and similar registration dates. We can build on this and establish further commonalities, such as domain registrars, subdomains and associated files.

Enriching Domains With WHOIS Records

One method we can use to establish further commonalities is to perform WHOIS lookups on the domains. A WHOIS lookup will provide information about who registered the domains and which domain registrar they were registered with.

If the same domain registrar and registration information can be seen across multiple domains, this can be an indication that the domains are related.

Many services (such as WHOIS) can perform these lookups but are limited to individual searches. We will leverage SilentPush for our lookups, as it supports bulk searches and significantly speeds up our process.

If you are using SilentPush, bulk lookups can be performed with Advanced Query Builder -> Enrichment Queries -> Domain Bulk

The screenshot shows a web interface with a dark theme. At the top left, there is a 'Documentation' link. Below it are tabs for 'Simple Query' and 'Advanced Query', and a 'Save Query' button. There are also 'Search' and 'Reset Form' buttons. The main content area is divided into two columns. The left column has two sections: 'domains' and 'scan_data'. The 'domains' section has a dropdown menu with the following items: 'luxury-get-away.top', 'nitb-update-services.top', 'services-pk-users.top', 'mofa-services-server.top', 'government-pk-update.top', and 'documents-server-pk.top'. The 'scan_data' section has a checked checkbox. The right column has an 'explain' section with a checked checkbox. To the right of the 'explain' section is a large JSON response box with two buttons: 'Copy Raw Data' and 'Copy API URL'. The JSON response is as follows:

```
{
  "status_code": 200,
  "error": null,
  "response": [
    {
      "host_flags": [
        {
          "domain": "services-pk-users.to",
          "host_has_expired_certificate": false,
          "host_has_open_directory": false,
          "host_has_open_s3_bucket": false
        }
      ]
    }
  ],
  "domain_urls": {
    "results_summary": [

```

After exporting the resulting JSON and parsing it with CyberChef, we can see that 6/7 of the domains were registered with [NameSilo](#) on [2024-03-19](#) with exact registration times within minutes of each other.

One of the resulting domains [luxury-get-away\[.\]top](#) features a different naming theme and registration time. For the purposes of this blog, we will ignore this domain for the remainder of this analysis.

```
Output
"domain": "services-pk-users.top"
"whois_created_date": "2024-03-19 04:09:59"
"registrar": "NameSilo, LLC"

"domain": "luxury-get-away.top"
"whois_created_date": "2024-03-19 17:20:15"
"registrar": "NameSilo, LLC"

"domain": "mofa-services-server.top"
"whois_created_date": "2024-03-19 04:10:08"
"registrar": "NameSilo, LLC"

.....
"domain": "cabinet-download-server.top"
"whois_created_date": "2024-03-19 04:09:58"
"registrar": "NameSilo, LLC"

"domain": "documents-server-pk.top"
"whois_created_date": "2024-03-19 04:10:08"
"registrar": "NameSilo, LLC"

"domain": "nitb-update-services.top"
"whois_created_date": "2024-03-19 04:09:57"
"registrar": "NameSilo, LLC"

"domain": "government-pk-update.top"
"whois_created_date": "2024-03-19 04:09:56"
"registrar": "NameSilo, LLC"
```

We now had 6 related domains, 5 of which were new and discovered through pivoting.

Consider that our analysis established these commonalities between the 6 domains.

1. Same theme of Government Entities and Pakistan
2. Same naming pattern (3 words separated by hyphens)
3. Same Top Level Domain of `.top`
4. Same registration provider of `NameSilo`
5. Same IP address `91.195.240[.]123` (and hence, the same ASN `47846`)
6. Same registration date `2024-03-19` and registration times between `04:09` and `04:11`

Pivoting To Additional Domains

With 6 domains and 6 commonalities between them, we had a strong base to begin performing additional pivots.

We expanded our search by making the following adjustments to our query.

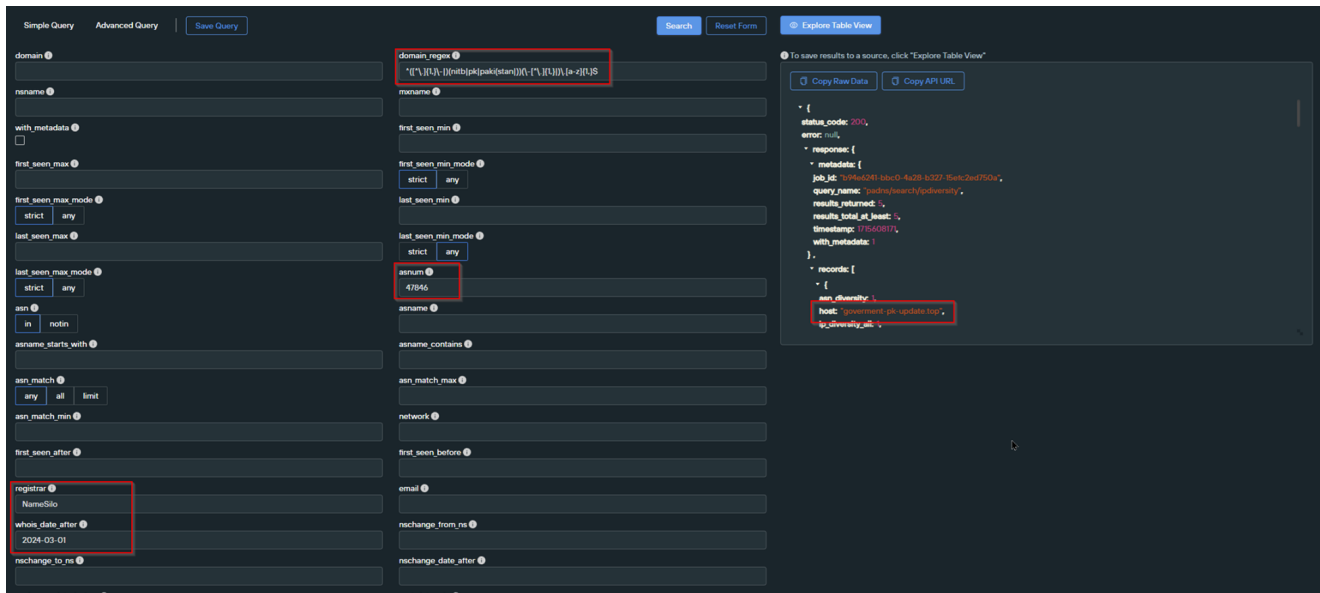
- Relaxing the IP requirement to allow for any IP hosted on [SED0/47846](#),
- Requiring NITB, PK or Pakistan keywords in our regex
- Relaxing the date requirements to any time after [2024-03-01](#).
- Adding a registrar requirement of [NameSilo](#)
- Relaxing the TLD requirements (Any TLD, not just [.top](#))

Applied as an advanced search in SilentPush, this translated to

- Pakistan keywords, `domain_regex=^([\.\-]{1,}\-|)(nitb|pk|paki(stan|))([\.\-]{1,}|)\.[a-z]{1,}$`
- Registered with NameSilo `registrar=NameSilo`
- Registered after March 2024 `whois_date_after=2024-03-01`
- Hosted on [SED0/47846](#), `asnum=47846`
- Hosted on any Top Level Domain `\.[a-z]{1,}$` (located at the end of our `domain_regex`)

In SilentPush, this is an advanced domain search which can be found under Advanced Query Builder -> Domain Queries -> Search.

Also, we'd like to extend a special thanks to the SilentPush research team who helped with this section.



After running the search and filtering the JSON output, we obtained five results.

Two of these results were not present in our initial search. This meant that we now had a total of 8 domains related to our initial indicator.

```
government-pk-update.top
govt-pk.com
moma-gov-pk.org
nitb-update-services.top
services-pk-users.top
```

The two new domains were largely thanks to our relaxation of the Top-Level-Domain requirements.

The new domains correspond to

- Govt-pk[.]com
- Moma-gov-pk[.]org

We now had three additional keywords that we could use to expand our search again. These keywords correspond to gov, govt and moma (Ministry of Maritime Affairs)

We then executed another advanced domain search, identical to before but now with a new regular expression.

- *Government* Themes in domain name, `domain_regex=^([^\.]{1,}\-|) (gov(t|erment)|moma)(-[^\.]{1,}|)\.[a-z]{1,}$`
- Registered with NameSilo `registrar=NameSilo`
- Registered after March 2024 `whois_date_after=2024-03-01`
- Hosted on SED0/47846, `asnum=47846`
- Hosted on any Top Level Domain `\.[a-z]{1,}$`

Search Reset Form Explore Table View

domain_regex **^([\d]{1}-){0}(gov(t(erment)))?(moma)(-[\d]{1})\[a-z]{1}\$**

mxname

first_seen_min

first_seen_min_mode **strict** any

last_seen_min

last_seen_min_mode **strict** any

asnum 47846

asname

asname_contains

asn_match_max

network

To save results to a source, click "Explore Table View"

Copy Raw Data Copy API URL

```

{
  "asn_diversity": 1,
  "host": "mohre-gov.info",
  "ip_diversity_all": 1,
  "ip_diversity_groups": 1,
  "timeline": [
    {
      "asn": 47846,
      "asname": "SEDO-AS, DE",
      "first_seen": "2024-03-21 11:34:57",
      "ip": "91.195.240.123",
      "last_seen": "2024-05-11 11:35:19"
    }
  ]
},
{
  "asn_diversity": 2,
  "host": "moma-gov-pk.org"
}

```

Updating the previous query to this regex returned 11 results. These results continued the theme of government entities, with references to

- NCSC (Possibly National Centre for Cyber Security)
- MOHRE (Ministry of Human Rights)
- IRS (Internal Revenue Service)
- PPY (possibly Pakistan Patriotic Youth)

```

amazonas-gov.co
cnsa-gov.com
gov-letsgethail.com
government-pk-update.top
govt-pk.com
irs-gov.net
justice-gov.info
mohre-gov.info
moma-gov-pk.org
my-gov-confirm.org
ncsc-gov.com
optimaxsi-gov.com
ppy-gov.pics
tax-service-gov.com
taxservice-gov.com

```

The results demonstrated a new recurring naming theme of `govpk` and `gov-pk`, so we again modified the regular expression to target these domain themes.

- *Gov/Gov-pk keywords* in the domain name, `domain_regex=^([\.\-]{1,}\-|)(gov\-pk|govpk)(-[\.\-]{1,}|)\.[a-z]{1,}$`
- Registered with NameSilo `registrar=NameSilo`
- Registered after March 2024 `whois_date_after=2024-03-01`
- Hosted on `SED0/47846`, `asnum=47846`
- Hosted on any Top Level Domain `\.[a-z]{1,}$` (end of `domain_regex`)

The screenshot shows a search interface with a query editor on the left and a results pane on the right. The query editor has a red box around the `domain_regex` field containing the regular expression: `^([\.\-]{1,}\-|)(gov\-pk|govpk)(-[\.\-]{1,}|)\.[a-z]{1,}$`. The results pane shows a JSON object with the following fields: `ip: "91.195.240.123"`, `last_seen: "2024-05-05 12:07:11"`, `asn_diversity: 1`, `host: "paknavy-govpk.com"` (highlighted with a red box), `ip_diversity_all: 1`, `ip_diversity_groups: 1`, and a `timeline` array containing one entry with `asn: 47846`, `asname: "SED0-AS, DE"`, `first_seen: "2024-05-10 13:07:11"`, `ip: "91.195.240.123"`, and `last_seen: "2024-05-12 11:22:41"`.

Executing this new query returned 3 results, two of them are new and feature government entities listed below.

- Paknavy (Pakistan Navy)
- DGPS (Directorate General Ports and Shipping)

The screenshot shows a list of search results in a dark-themed interface. The results are: `dgps-govpk.com`, `moma-gov-pk.org`, and `paknavy-govpk.com`.

So far, all of our searches have required the domain to be associated with an ASN number of `SED0/47846`.

One method we used to identify additional domains was to relax the ASN requirement whilst maintaining the other parameters.

We repeated this for all of our searches, with one in particular bringing in new results.

- Any domain name containing gov ,gov-pk or govpk and hyphens `domain_regex = ^([\.\-]{1,}|)(gov\-\pk|govpk)(-[\.\-]{1,}|)\.[a-z]{1,}$`
- Hosted on *any* Top Level Domain (The final `\.[a-z]{1,}$` in our regex)
- Hosted on *any* Autonomous System (removal of the `asnum` parameter)
- Registered with `NameSilo`
- Registered after `2024-03-01`

The screenshot shows a search interface with a dark theme. At the top, there are buttons for 'Simple Query', 'Advanced Query', 'Save Query', 'Search', 'Reset Form', and 'Explore Table View'. The 'domain_regex' field is highlighted with a red box and contains the regex: `^([\.\-]{1,}|)(gov\-\pk|govpk)(-[\.\-]{1,}|)\.[a-z]{1,}$`. Other fields include 'domain', 'nsname', 'mxname', 'with_metadata', 'first_seen_max', 'first_seen_max_mode', 'last_seen_max', 'last_seen_max_mode', 'asn', 'asname_starts_with', and 'asn_match'. On the right, a JSON result is displayed, with the 'host' field highlighted in red: `host: "pta-govpk.com"`. The JSON also shows `asn: 47846`, `asname: "SEDO-AS, DE"`, `first_seen: "2024-03-22 13:14:16"`, `ip: "91.195.240.12"`, and `last_seen: "2024-04-25 03:23:45"`.

Executing the search with new parameters provided 9 domains, multiple of which were new and continued the theme of impersonating Pakistan Government entities.

- EP - Express Mail Track & Trace System
- NADRA - National Database and Registration Authority
- PTA - Pakistan Telecommunication Authority

```
dgps-govpk.co
dgps-govpk.com
ep-gov-pk.icu ←
gov-govpk.info
mail-govpk.com
moma-gov-pk.org
nadra-govpk.com ←
paknavy-govpk.com
pta-govpk.com| ←
```

We can continue to use the same concept of relaxing and adjusting parameters to identify additional domains. However, to keep this post from getting too long (there are infinite possible pivots), we've decided to leave the pivoting section here and continue with our currently identified domains.

Results from our additional pivots will be included in the final IOC section of this post

Establishing Patterns in Subdomains

Recall that the initial domain shared by DocGuard had the primary malicious activity under the `docs` subdomain of `docs.mofa-services-server[.]top`

We wanted to see if our new domains had any such subdomains which could establish a further pattern linking the activity to the initial domain.

Recall the `docs.mofa-services-server[.]top` domain shared by DocGuard. The `docs` subdomain was first seen on `2024-05-01`, approximately 6 weeks after the parent domain was first registered.

If you are using SilentPush, this search can be found under Advanced Query Builder -> PADNS Queries -> Subdomain Records

Search Reset Form

domain* ⓘ
mofa-services-server.top

first_seen_before ⓘ
[Empty]

limit ⓘ
100

with_metadata ⓘ

Copy Raw Data Copy API URL

```
metadata: {  
  job_id: "59c04042-23c0-4230-b804-f6dc4629fb5c",  
  query_name: "padns/lookup/subdomains",  
  results_returned: 1,  
  results_total_at_least: 1,  
  timestamp: 1715610048,  
  with_metadata: "1"  
},  
records: [  
  {  
    first_seen: "2024-05-01 06:04:45",  
    last_seen: "2024-05-08 19:02:22",  
    subdomain: "docs.mofa-services-server.top",  
    type: "A"  
  }  
]
```

We ran an identical search for our `documents-server-pk[.]top` domain, which revealed a similar pattern where a `pmo` subdomain was created approximately 6 weeks after the parent domain first appeared.

One theory is that the Threat Actor is “sitting” on parent domains and then performing malicious activity via subdomains at a later date. This may be to avoid domain-based filtering that blocks or alerts on recently registered infrastructure (<30 days old) .

Search Reset Form

domain* ⓘ
documents-server-pk.top

first_seen_before ⓘ
[Empty]

limit ⓘ
100

with_metadata ⓘ

Copy Raw Data Copy API URL

```
metadata: {  
  job_id: "551c0ff1-2d8e-4d61-af15-0712433d6de9",  
  query_name: "padns/lookup/subdomains",  
  results_returned: 1,  
  results_total_at_least: 1,  
  timestamp: 1715610082,  
  with_metadata: "1"  
},  
records: [  
  {  
    first_seen: "2024-05-01 06:40:40",  
    last_seen: "2024-05-07 14:58:40",  
    subdomain: "pmo.documents-server-pk.top",  
    type: "A"  
  }  
]
```

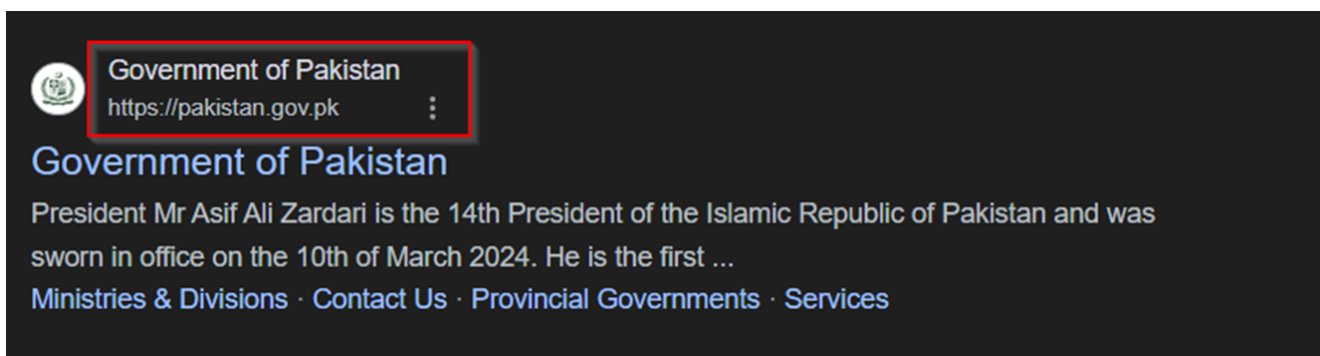
Repeating the subdomain searches returned a total of 15 subdomains featuring Government themes and new government entities of

- MOD (Ministry of Defense)
- ECP (Election Commission of Pakistan)
- CTD (Counter Terrorism Department)
- LGCD (Local Government and Community Development)
- PUBAD (Ministry of Public Administration, Home Affairs and Provincial Councils).

We can see these themes in the screenshot below.

```
ctd.govt-pk.com
docs.mofa-services-server.top
ecp.govt-pk.com
embajadadenepal.es.govt-pk.com
investinnepal.gov.np.govt-pk.com
lgcd.punjab.gov.pk.govt-pk.com
mindef.gov.pk.govt-pk.com
mod.gov.bd.govt-pk.com
mod.gov.np.govt-pk.com
mofa.gov.bd.govt-pk.com
mofa.gov.np.govt-pk.com
pmo.documents-server-pk.top
prisons.punjab.govt-pk.com
pubad.gov.lk.govt-pk.com
sparrso.gov.bd.govt-pk.com
```

Of additional interest here is that we see domains targeting Sri Lanka (lk) and Nepal, and that the majority of subdomains exist under `gov-pk[.]com`, which is an impersonation of the legitimate domain `gov[.]pk`



We can also observe that `pubad.gov.lk.govt-pk[.]com` is an impersonation of the legitimate Sri Lankan domain `pubad.gov[.]lk`



Ministry of Public Administration, Home Affairs

<https://www.pubad.gov.lk>



Ministry of Public Administration, Home Affairs, Provincial ...

Sri Lanka Administrative Service

Circular Manager - Document Search - Establishments Code

Most of the identified parent domains did not have an associated subdomain. We believe this is likely due to the “waiting” that the actor is using after the parent domain is first created.

At the time of this writing, it had only been 6 days since the first malicious subdomains were observed. Hence, we believe that the remaining subdomains had not yet been created.

Linking Domains to APT SideWinder

At the time of this writing, we could not find any publicly available reports on our 37 newly identified domains.

However, we found two extremely interesting reports by [BlackBerry](#) and [Group-IB](#) that detail 2023 activity of the Indian Advanced Persistent Threat (APT) known as SideWinder. This Threat Actor is known for targeting Pakistan, Nepal and Sri Lanka. (All in line with the activity we observed so far)

Both reports provide the following details and TTP's regarding the SideWinder group.

- Primary targeting of South Asian countries bordering India
- Heavy usage of domains impersonating Government Entities
- Heavy targeting of Military and Government Entities
- Heavy usage of Initial Access via Weaponized Documents with Government Themes

Domain Similarity, Government Entities and Primary Targeting of South Asian Countries

The [BlackBerry](#) report contains a list of known SideWinder domains targeting South Asian countries.

The following domains were extracted from the BlackBerry report and show remarkable similarities to those identified during our analysis. Note the heavy usage of...

- Hyphens in domain names
- Recurring themes of Government entities
- Recurring themes of Pakistan and Sri Lanka

- Heavy usage of Subdomains

Although we have grouped this under one heading, this screenshot represents 4 unique commonalities between the domains we identified and known activity from APT SideWinder.



The second report from [Group-IB](#) shows similar domains with remarkable similarities to those identified in our analysis.

daraz-pk.com
defpak.org
fia-gov.com
helpdesk-gov.info
mfagov.org
mofs-gov.org
ntc-pk.com
ntc-pk.org
paf-govt.info
paf-govt.net
pak-gov.info
pak-govt.net
pak-news.info
paknavy-gov-pk.downld.net
pk.downld.net
ptcl-govp.org
sbp-pk.org
sindhpolice-govpk.org
telemart-pk.com

Subset of SideWinder domains
shared by Group-IB

Public Reports of Initial Access Via Weaponized Documents

Both the [Group-IB](#) and [BlackBerry](#) reports detail SideWinder activity where initial access is achieved via weaponised documents with Government Entity themes.

Additionally, both reports detail a malicious document titled [GUIDELINES FOR BEACON JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE \(PNWC\).doc](#)

The reports detail that this document leveraged a remote template injection vulnerability [CVE-2017-0199](#) to download a remote file named [file.rtf](#) that contained obfuscated Javascript code.

A visual overview of the document (Taken from BlackBerry and Group-IB) can be seen below.

GUIDELINES FOR BEACON JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC)

Pakistan Navy War College (PNWC) invites manuscripts for its journal (Beacon-23). The journal is accredited with HEC in 'Y' category. Research articles shall be accepted in areas related to International Relations, Strategic Studies, International and Regional Security, South Asian Studies, Maritime Security, Indian and Pacific Ocean studies and Hybrid Warfare.

Submission Deadlines: Research scholars who wish to contribute original, unpublished articles to the journal may submit these by first week of January, 2023. The articles may be written individually or co-authored.

Article word limit: The manuscripts should normally be 5000 (+_ 10%) words excluding abstract, author's Introduction, footnotes and bibliography.

Format: All article submissions must include an abstract of about 200-250 words with 5-7 keywords and footnotes. The first page of the manuscript should contain the title of the paper, the name(s) of author(s), abstract and footnote giving introduction and current affiliation of the author(s). A 'Disclaimer' must be made at (footnote 2) and when applicable.

Plagiarism: Similarity index (Turnitin Report) must not exceed 18%.

The BlackBerry article details another SideWinder document featuring Pakistan Government themes and an overall well-made and professional-looking email.



United States of America
Amendment 1 to Letter of Offer and Acceptance
PK-P-GAA

Based on Embassy of Pakistan, Letter of Request (LOR), Ref: (continued on page 2)

Mail To: Government of Pakistan, Embassy of Pakistan, Attache Defense Procurement 3517 International Court, N.W. Washington, DC 20008.

Pursuant to the Arms Export Control Act, the Government of the United States (USG) offers to amend the Letter of Offer and Acceptance (LOA) identified above for the purchase of defense articles, defense services, or both. Other provisions, terms, and conditions of the original LOA remain unchanged.

This Amendment provides additional support by increasing the (continued on page 2)

Basic LOA accepted: 03 Jul 2019.

Estimated Cost: \$5,000,000

Due with Amendment Acceptance: \$1,774,239

Terms of Sale:

Cash Prior to Delivery

Dependable Undertaking

This offer expires on 17 February 2023. Unless a request for extension is made by the Purchaser and granted by the USG, the offer will terminate on the expiration date.

This Amendment consists of page 1 through page 7.

The undersigned are duly authorized representatives of their Governments and hereby respectively offer and accept this Amendment:

GAISER, ALFRED, Signature
 OTTO, 1031333840 Doc ID

26 Oct 2022

U.S. Signature

Date

Purchaser Signature

Date

 Typed Name and Title

Weaponized Documents In Our Newly Identified Domains

Reviewing one of our discovered domains [paknavy-govpk\[.\]info](http://paknavy-govpk[.]info) on VirusTotal, we can see an associated [.docx](#) file named [MoITT_federaIemp\[.\]docx](#) from [2024-04-29](#)

Search: paknavy-govpk.info

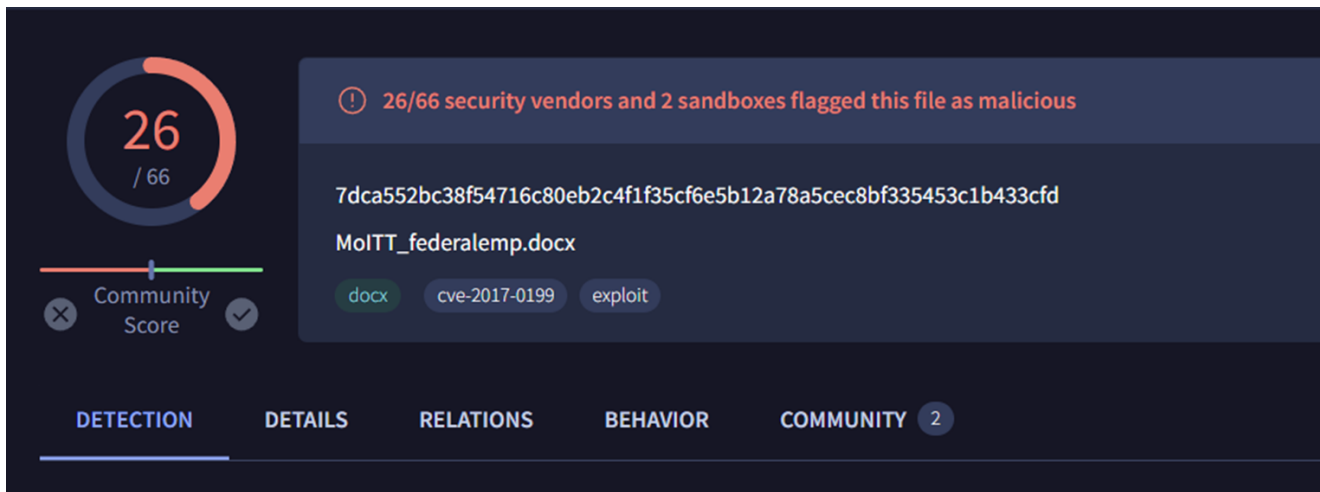
Communicating Files (1)

Scanned	Detections	Type	Name
2024-04-29	26 / 66	Office Open XML Document	MoITT_federaIemp.docx

Historical Whois Lookups (2)

Last Updated	Registrar
+ 2024-03-30	NameSilo, LLC
+ 2024-03-22	NameSilo, LLC

This file, which is linked to our new domains, features the same [CVE-2017-0199](#) exploit as detailed by BlackBerry and Group-IB

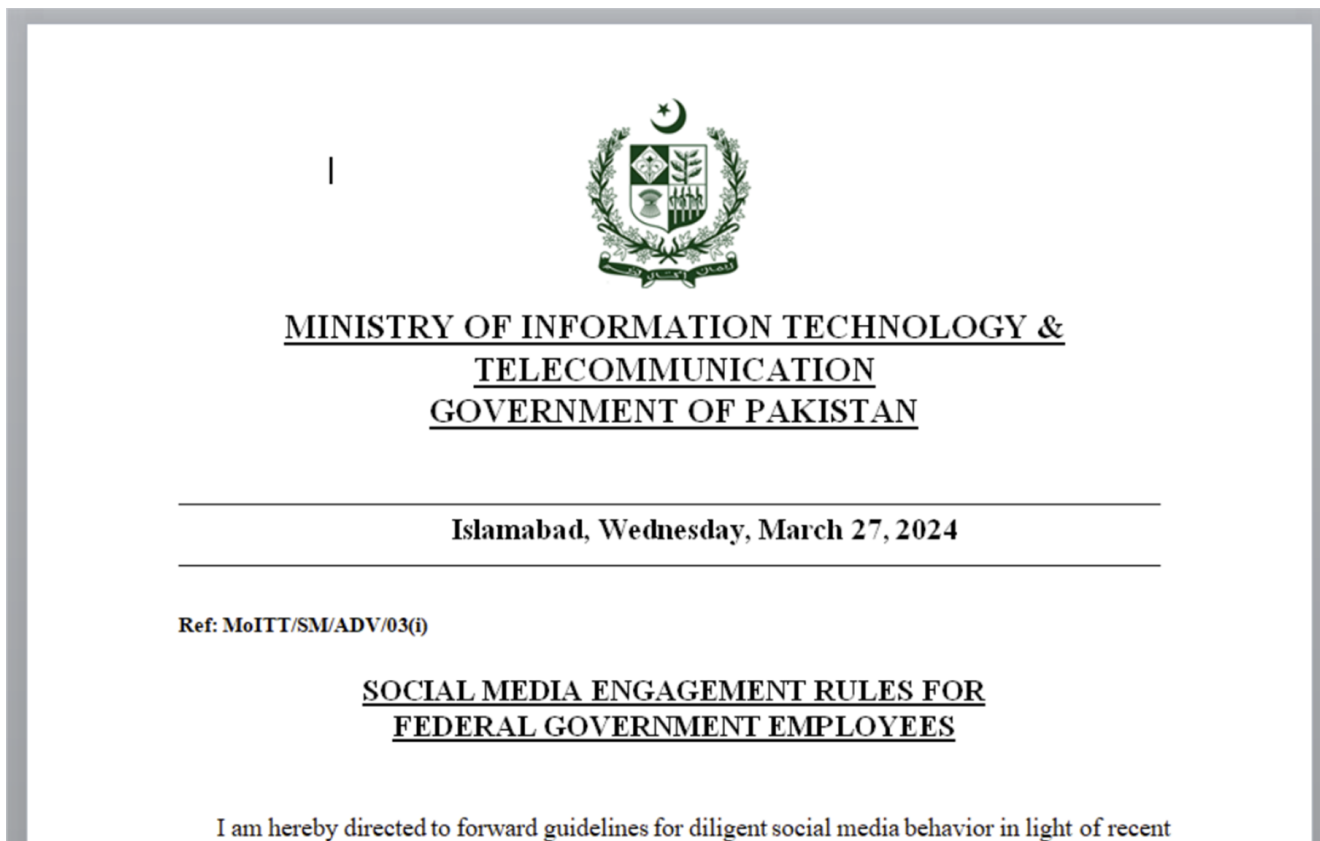


The screenshot shows a security analysis interface. On the left, there is a circular gauge with the number '26' and '/ 66' below it, and a 'Community Score' indicator with a green checkmark. On the right, a dark blue box contains a warning icon and the text '26/66 security vendors and 2 sandboxes flagged this file as malicious'. Below this, the file hash '7dca552bc38f54716c80eb2c4f1f35cf6e5b12a78a5cec8bf335453c1b433cfd' and the file name 'MoITT_federalempl.docx' are displayed. Three tags are shown: 'docx', 'cve-2017-0199', and 'exploit'. At the bottom, there is a navigation bar with tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY' (which has a '2' next to it).

By searching the file hash

[7dca552bc38f54716c80eb2c4f1f35cf6e5b12a78a5cec8bf335453c1b433cfd](#) on [Hybrid-Analysis](#), we noticed that the document contained Pakistan government themes and an overall similar structure to the publicly reported documents.

Below is the document associated with our domain [paknavy-govpk\[.\]info](#)



The screenshot shows the header of a document. At the top center is the national emblem of Pakistan. Below it, the text reads: 'MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION' and 'GOVERNMENT OF PAKISTAN'. A horizontal line follows, with the date 'Islamabad, Wednesday, March 27, 2024' centered below it. Another horizontal line follows, with the reference number 'Ref: MoITT/SM/ADV/03(i)' on the left. Below this, the title 'SOCIAL MEDIA ENGAGEMENT RULES FOR FEDERAL GOVERNMENT EMPLOYEES' is centered and underlined. At the bottom, the text 'I am hereby directed to forward guidelines for diligent social media behavior in light of recent' is visible.

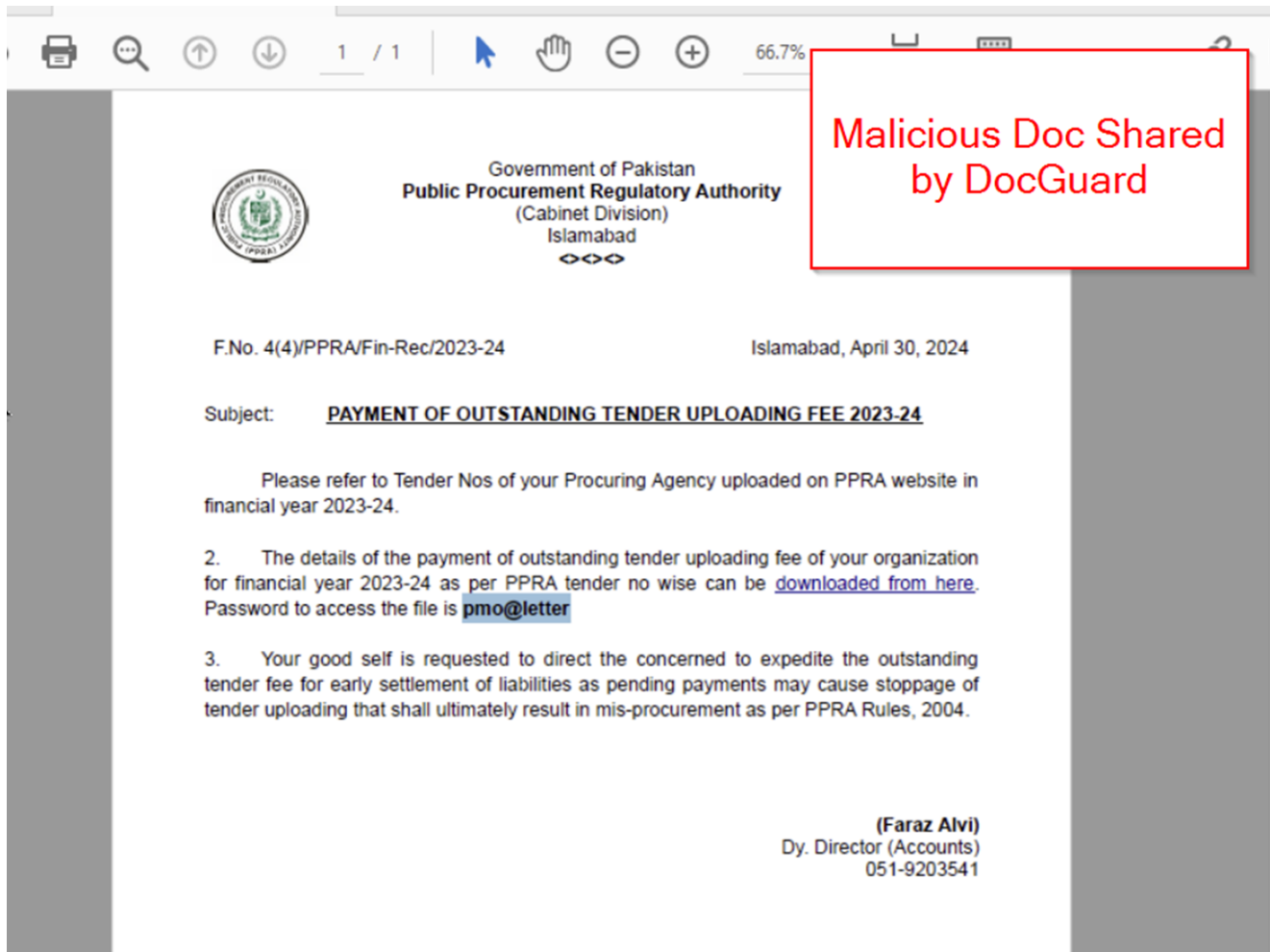
The usage of Pakistan government themes, weaponized documents and the same exploit [CVE-2017-0199](#) is a strong indication that this activity is linked to the public SideWinder reports.

Modification of Weaponized Documents

We could not find any additional presence of weaponised documents leveraging [CVE-2017-0199](#) in our remaining domains. Although, we did observe a change to PDFs linking to password-protected .zip files.

This represented a change in specific tactics, but continuing the overall tactic of weaponized documents.

The initial domain [docs.mofa-services-server\[.\]top](#) is related to the following document (shared by DocGuard in their initial post), which features a password-protected .zip with a password of [pmo@letter](#)



One of our identified subdomains [pmo.documents-server-pk\[.\]top](#) is related to a similar PDF file linking to a .zip.

pmo.documents-server-pk.top

Communicating Files (1)

Scanned	Detections	Type	Name
2024-04-30	0 / 62	PDF	62032f85-3d61-43c6-a2d3-d8e7e3adf39b.pdf

By taking the hash from VirusTotal and searching it on [Hybrid-Analysis](#), we see a similar theme of Government entity-themed phishing with password-protected .zip files.

The end of the document featured a prompt to download a password-protected file.



The presence of password-protected .zip files (likely containing malware) instead of CVE-2017-0199 represents both a strong link (via weaponized docs) and a slight change in SideWinder activity and techniques.

The overall tactic of weaponized documents is continued, but the specific tactic of CVE-2017-0199 has changed to a password-protected zip file.

SideWinder Usage of NameSilo

A subset of the older SideWinder domains shared by BlackBerry and Group-IB feature NameSilo as the domain registrar.

Many shared domains did not feature NameSilo, but this shows that SideWinder is familiar with NameSilo and uses it for a subset of their domain infrastructure.

Since all of the domains we featured today utilised NameSilo, this indicates a weaker but still useful connection between the new domains and those already publicly attributed to SideWinder.

```
"query": "sindhpolice-govpk.org"
"whois_created_date": "2022-11-22 07:35:53"
"registrar": "Namesilo, LLC"

"query": "sbp-pk.org"
"whois_created_date": "2022-11-22 07:35:18"
"registrar": "Namesilo, LLC"

"query": "fia-gov.com"
"whois_created_date": "2022-07-08 10:04:28"
"registrar": "Namesilo, LLC"

"query": "helpdesk-gov.info"
"whois_created_date": "2022-11-22 07:34:05"
"registrar": "Namesilo, LLC"

"query": "paknavy-gov-pkp.downld.net"
"whois_created_date": "2021-04-07 20:20:00"
"registrar": "Namesilo, LLC"

"query": "paknavy-gov-pk.downld.net"
"whois_created_date": "2021-04-07 20:20:00"
"registrar": "Namesilo, LLC"

"query": "pk.downld.net"
"whois_created_date": "2021-04-07 20:20:00"
"registrar": "Namesilo, LLC"
```

Subset of Domains From Group-IB and BlackBerry showing NameSilo usage.

Conclusion

We have now analysed a single domain indicator with threat intelligence tooling and identified 37 new domains with strong relations to known SideWinder activity. We analysed historical records around IP addresses, domain registrars, registration dates, associated files, and subdomains.

The tool used in this analysis was [SilentPush](#), If you'd like to follow along, consider signing up for the Community Edition.

Domain Indicators

nitb-update-services[.]top
services-pk-users[.]top
mofa-services-server[.]top
goverment-pk-update[.]top
documents-server-pk[.]top
Cabinet-download-server[.]top
amazonas-gov[.]co
cnsa-gov[.]com
dgps-govpk[.]co
dgps-govpk[.]com
ep-gov-pk[.]christmas
ep-gov-pk[.]icu
gov-govpk[.]info
Govt-pk[.]com
justice-gov[.]info
mohre-gov[.]info
moma-gov-pk[.]org
my-gov-confirm[.]org
ncsc-gov[.]com
paknavy-govpk[.]info
Update-govpk[.]co
paknavy-govpk[.]com
ctd[.]govt-pk[.]com
docs[.]mofa-services-server[.]top
ecp[.]govt-pk[.]com
embajadadenepal[.]es[.]govt-pk[.]com
investinnepal[.]gov[.]np[.]govt-pk[.]com
lgcd[.]punjab[.]gov[.]pk[.]govt-pk[.]com
mindef[.]gov[.]pk[.]govt-pk[.]com
mod[.]gov[.]bd[.]govt-pk[.]com
mod[.]gov[.]np[.]govt-pk[.]com
mofa[.]gov[.]bd[.]govt-pk[.]com
mofa[.]gov[.]np[.]govt-pk[.]com
pmo[.]documents-server-pk[.]top
prisons[.]punjab[.]govt-pk[.]com
pubad[.]gov[.]lk[.]govt-pk[.]com
sparrso[.]gov[.]bd[.]govt-pk[.]com
mail-govpk[.]com
nadra-govpk[.]com
pta-govpk[.]com
newmofa[.]org
update-govpk[.]co
mod-gov-pk[.]live
pakistan-mofa[.]cloud
s3-network-pakistan[.]online

