TLP:CLEAR

MoonPeaking Into Kimsuky Operations: The DPRK Deck of Cards

Initial Version: September 23rd, 2024
Final Version: October 11th 2024

TLP:CLEAR

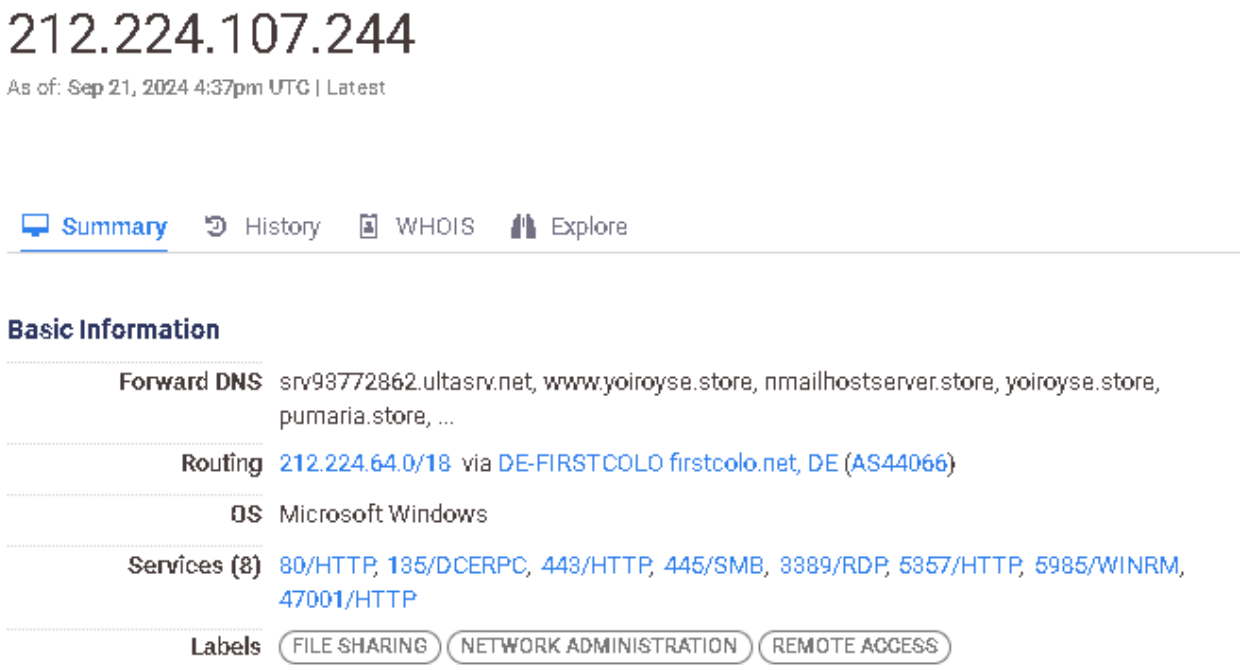
Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

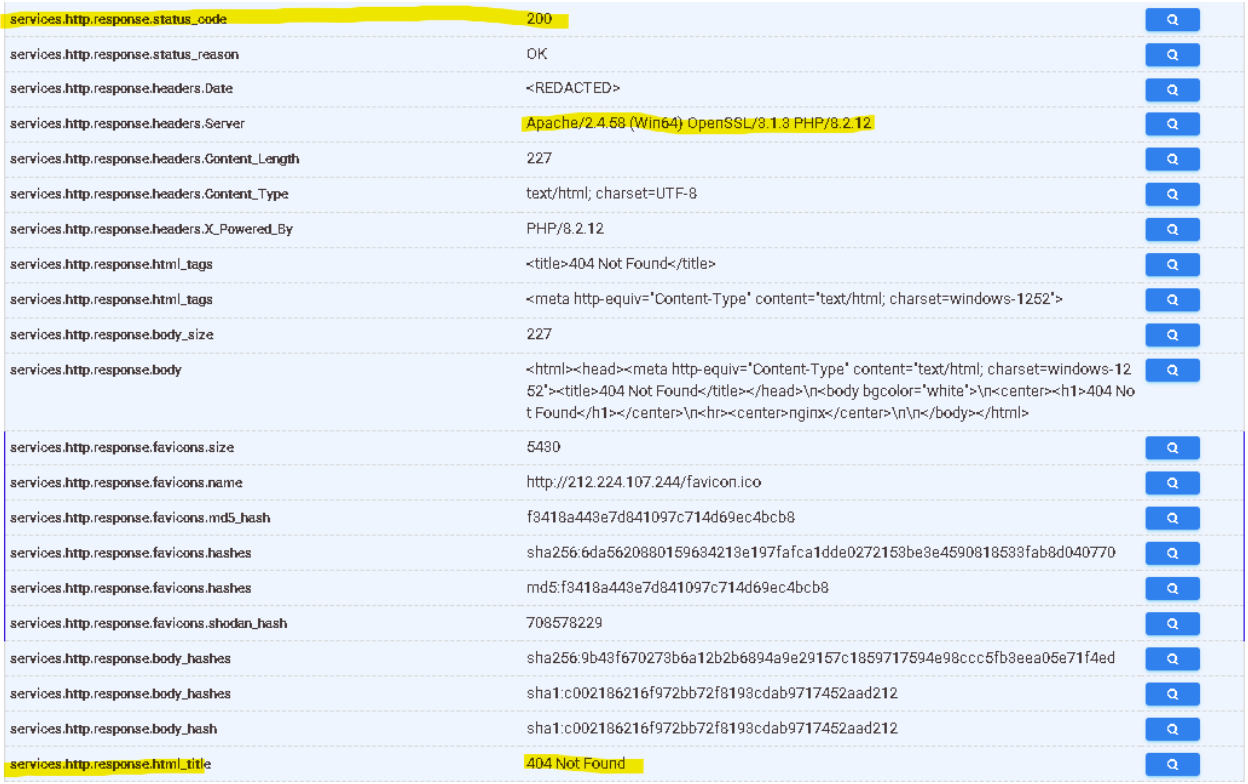
Mapping the Craters

Cisco Talos released a writeup on MoonPeak, a XenoRAT adaptation linked to UAT-5394/Kimsuky which can be found at https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/.
This serves to supplement their findings, alongside drawing links between Kimsuky and recent Lazarus Group/BlueNoroff campaigns.

Various domains listed in the IOCs section such as nmailhostserver[.]store and pumaria[.]store resolve to 212[.]224[.]107[.]244. It's important here to note that the tech stack (OpenSSL 3.1.3 + PHP 8.2.12 and Apache HTTPD 2.4.58) is one of the specific stacks used in this research to track recent Kimsuky hosts.



There are some interesting pivots available to us, but most notably there is a response hash that we can easily pivot from.



services.http.response.status_code	200
services.http.response.status_reason	OK
services.http.response.headers.Date	<REDACTED>
services.http.response.headers.Server	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
services.http.response.headers.Content_Length	227
services.http.response.headers.Content_Type	text/html; charset=UTF-8
services.http.response.headers.X_Powered_By	PHP/8.2.12
services.http.response.html_tags	<title>404 Not Found</title>
services.http.response.html_tags	<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
services.http.response.body_size	227
services.http.response.body	<html><head><meta http-equiv="Content-Type" content="text/html; charset=windows-1252"><title>404 Not Found</title></head>\n<body bgcolor="white">\n 404 Not Found \n<hr> nginx \n\n</body></html>
services.http.response.favicons.size	5430
services.http.response.favicons.name	http://212.224.107.244/favicon.ico
services.http.response.favicons.md5_hash	f3418a443e7d841097c714d69ec4bcb8
services.http.response.favicons.hashes	sha256:6da56208801596342l3e197fafca1dde0272153be3e4590818533fab8d040770
services.http.response.favicons.hashes	md5:f3418a443e7d841097c714d69ec4bcb8
services.http.response.favicons.shodan_hash	708578229
services.http.response.body_hashes	sha256:9b43f670273b6a12b2b6894a9e29157c1859717594e98ccc5fb3eea05e71f4ed
services.http.response.body_hashes	sha1:c002186216f972bb72f8193cdab9717452aad212
services.http.response.body_hash	sha1:c002186216f972bb72f8193cdab9717452aad212
services.http.response.html_title	404 Not Found

There is a commonly used discrepancy between response status code and the displayed page title, something which in normal cases matches up. Notable too is the charset set in the HTML tags compared to the charset set by the content type response header.

While those are all valuable, using the response hash is much more efficient and reliable in providing us with MoonPeak C2s.
services.http.response.body_hashes="sha256:9b43f670273b6a12b2b6894a9e29157c1859717594e98ccc5fb3eea05e71f4ed".

At the time of writing, there are 54 results for this query, a breakdown for IP prevalence is displayed here:

IP	Hosts	
158.247.202.152	8	14.29%

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857ae450597aa75d96efe6a359adf9c16

198.13.55.71	6	10.71%
212.224.107.244	6	10.71%
37.72.174.7	4	7.14%
84.246.85.175	3	5.36%
101.36.114.91	3	5.36%
141.164.37.141	3	5.36%
154.90.63.162	3	5.36%
154.90.63.209	3	5.36%
194.68.27.24	3	5.36%
92.38.160.131	2	3.57%
92.38.160.155	2	3.57%
156.244.19.155	2	3.57%
27.255.81.107	1	1.79%
50.114.5.159	1	1.79%

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

89.187.28.147	1	1.79%
104.194.152.251	1	1.79%
121.183.135.161	1	1.79%
156.244.19.95	1	1.79%
192.121.162.82	1	1.79%
210.92.18.162	1	1.79%

Scanning The Surface

Most of the domains in this listing are already known and documented, but without the added context of these being MoonPeak C2s.

For example: asanpolicy[.]lol at https://search.censys.io/hosts/101.36.114.91+www.asanpolicy.lol has been documented as a Kimsuky C2 based on byrne_emmy's post https://x.com/byrne_emmy12099/status/1832570100832153848, or member-apples[.]info from 0xmh1 at https://x.com/0xmh1/status/1835900052679872688. The vast majority of these IPs and domains are already listed in Maltrail but the historical links we can draw between these domains and prior campaigns are more interesting.

The IP continues to have new vhosts allocated, as evidenced by https://x.com/0xmh1/status/1839173077818814740 and the https://search.censys.io/hosts/101.36.114.91+rfatotal.one allocation later on the same day. It was noteworthy enough to check out the netblock, and upon reinspection, that's where the domains with opendirs related to https://x.com/asdasd13asbz/status/1783715045576421574 all hosted on 101[.]36[.]114[.]180.

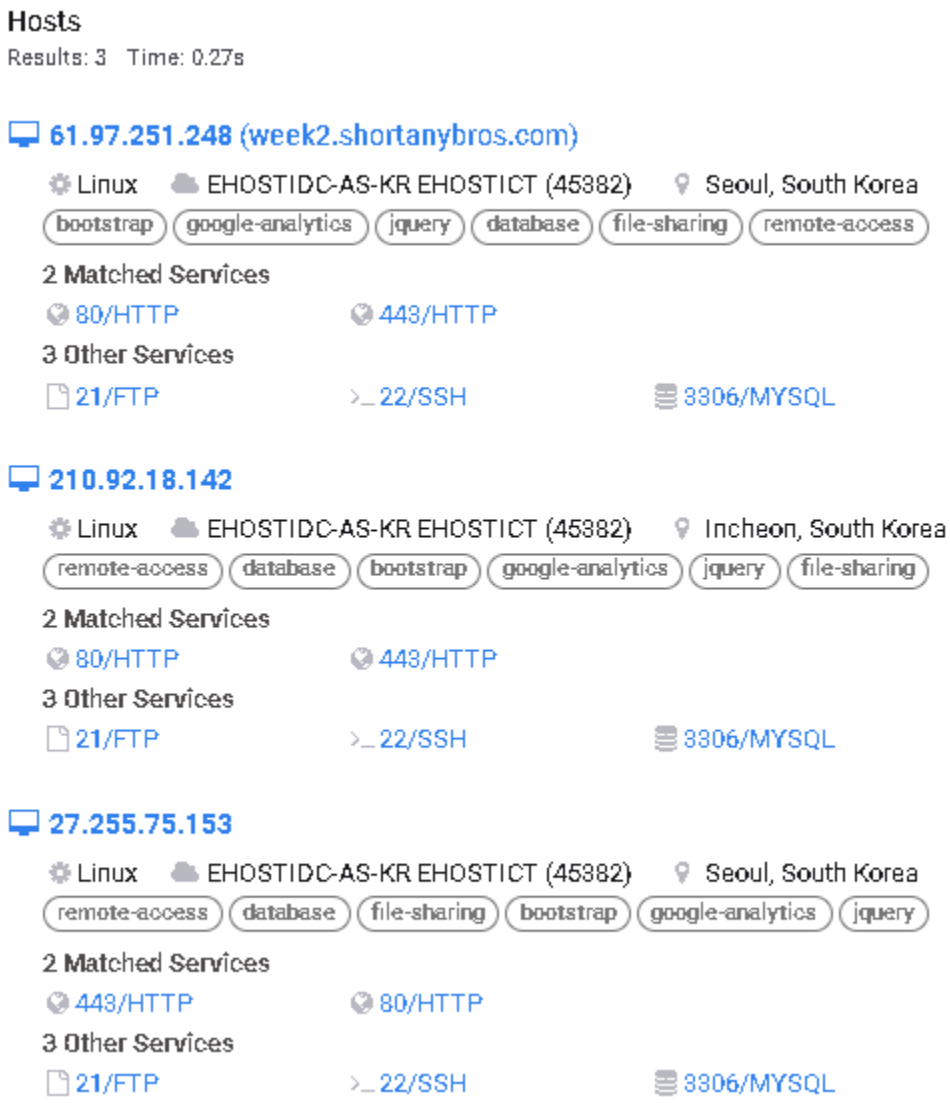
The first IP listed in the results is https://search.censys.io/hosts/27.255.81.107, one which already holds IOCs https://github.com/stamparm/maltrail/blob/1c3326742985b29a229a0de40eeb41c9d33f37bd/trails/static/malware/apt_kimsuky.txt#L7019. That domain smaths[.]lat is presented from a previous response hash IOC provided by Cyberteam008 at https://x.com/Cyberteam008/status/1765624539273183623. (The paste also links us to 27[.]255[.]75[.]158 which will be discussed later)

Cyberteam's tweet ranges back to early March 2024 and the Million OK campaign, which helps fit this into the broader timeline of implant development by the threat actors. Continuing on this trail, and following the hypothesis presented by myself at https://x.com/eastside_nci/status/1826907916135231985, we assume that the 27[.]255[.]81[.]0/24 block is operator controlled. We can prove this with simple historical indicators. 27[.]255[.]81[.]107 shows up from the MoonPeak body hash, with a domain linked back to Kimsuky operations in March. (27[.]255[.]81[.]69, 27[.]255[.]81[.]110, and 27[.]255[.]81[.]112 are listed on Validin having displayed the response hash) 27[.]255[.]81[.]118 is a MoonPeak IOC, which ShanHolo also mentioned as a XenoRat pivot in July at https://x.com/ShanHolo/status/1808906441077764574, further reinforcing the XenoRat → MoonPeak pipeline. Indicators for this block range back to September 2022 based on https://github.com/stamparm/maltrail/blob/caa3c7ac723b336cb2ad7ebc22248ca8db31548f/trails/static/malware/apt_kimsuky.txt#L1866C14-L1866C72.

The 210[.]92[.]18[.]169 is also mentioned in the same tweet as a pivot point, which was in a sequential block with 210[.]92[.]18[.]161 displaying NaverMail themed domains since June 29th. 210[.]92[.]18[.]162 is another IP that shows up in the body hash query, and also is a known Kimsuky IOC at https://github.com/stamparm/maltrail/blob/1be5e1af3b6360bb10fe659827739c8c6faeb65f/trails/static/malware/apt_kimsuky.txt#L9489. These, alongside other known indicators such as 210[.]92[.]18[.]142, 210[.]92[.]18[.]165, and 210[.]92[.]18[.]176, help fill in the 210[.]92[.]18[.]0/24 block mentioned at https://x.com/eastside_nci/status/1826907914918912293.

This links us to 61[.]97[.]251[.]248, and similarly, the 61[.]97[.]251[.]0/24 netblock with its entries at https://github.com/search?q=repo%3Astamparm%2Fmaltrail+%2F61%5C.97%5C.251%5C..%2B%2F&type=code. Shoutout Maltrail for realizing the netblock clustering and

doing their own pivoting based on it! A wide variety of IPs and domains from this block are already uploaded, but it is important to note a previous pivot that linked the IPs from the tweet. These all displayed a response body including: *services.http.response.html_tags="<meta content=\"https://www.facebook.com/mesinkasircomplete\" property=\"facebook:author\" />"*



While the .248 is down now, there is a new matching C2 on 61[.]97[.]251[.]251 at https://search.censys.io/hosts/61.97.251.251. Noting Perl in the tech stack tells us this is related to the malware family described at

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df155131591 7f05036db562857a
e450597aa75d96efe6a359adf9c16

https://x.com/asdasd13asbz/status/1791390914038149339, which is noted as **Operation Dream Job**.

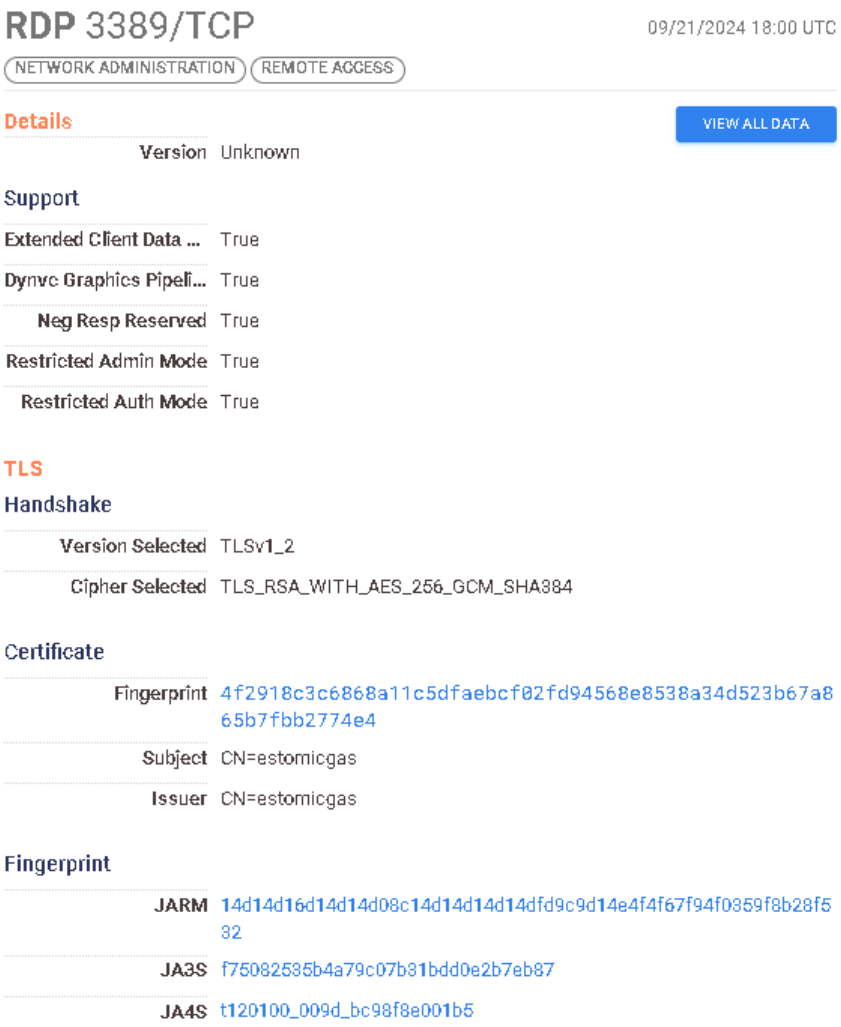
27[.]255[.]75[.]158 from the MoonPeak writeup suffers a similar fate, as it's in a historically used netblock, evidenced by https://github.com/search?q=repo%3Astamparm%2Fmaltrail%20%2F27%5C.255%5C.75%5C..%2B%2F&type=code. Interestingly, we see 27[.]255[.]75[.]142 referenced in TA505's repository with domains targeting Daum, a South Korean company not infrequently targeted with Kimsuky associated infrastructure. While this is likely a pure coincidence it is still an interesting bit tof information. The 27[.]255[.]75[.]0/24 netblock is included in a previously drawn conclusion of malicious block usage. The start of the thread included 27[.]255[.]75[.]153 as part of a MYSQL exposing subcluster of IPs. The 27[.]255[.]75[.]154, 27[.]255[.]75[.]156, and 27[.]255[.]75[.]158 are all known IOCs and further paint the picture of sequentially allocated infrastructure, similarly ranging back in age to the 27[.]255[.]81[.]0/24 cluster in Maltrail.

The Dark Side of the Moon

Making Threat Actors Suffer Together

Other important mentions for historical clustering are the hosts in AS29802/HVC-AS. 37[.]72[.]174[.]7 hosts two notable domain names with the body hash: mta-sts[.]resolveissue[.]org and www[.]resolveissue[.]org. Returning back to the Million OK cluster and Cyberwar's IOCs, there were 3 domains that matched this interesting pattern: mta-sts[.]docsuris[.]store, mta-sts[.]makeverify[.]store, mta-sts[.]usage[.]store. Additionally, the resolveissue[.]org domain is included in Maltrail's listings at https://github.com/stamparm/maltrail/blob/eb74d9eafdcd1a4cdec143bc4c1606b83af5662d/trails/static/malware/apt_kimsuky.txt#L11030.

This domain pattern continues to reappear upon continued MoonPeak body hash pivots. 192[.]121[.]162[.]82 and 194[.]68[.]27[.]24 display various Apple related pages. Similar to member-apples[.]info mentioned in the last section, we have applesec[.]info on https://search.censys.io/hosts/194.68.27.24+applesec.info and https://search.censys.io/hosts/192.121.162.82+applesec.info, as well as members-apple[.]com on https://search.censys.io/hosts/194.68.27.24+members-apple.com. Noteworthy here is an RDP certificate displayed.



This certificate's hash is 4f2918c3c6868a11c5dfaebcf02fd94568e8538a34d523b67a865b7fbb2774e4, and was issued on 2024-09-18T15:25:34 UTC, but only has this IP scanned displaying it. There exists an earlier certificate, from 1 day before, with hash *3b52bb66a72c3dfe7160e936cbce760b11fef041db2fb1c1a839314ea40fd2b7*, issued on 2024-09-17T11:50:57 UTC. This certificate isn't displayed on any Censys results.

192.121.162.0/24

Pivoting off the 192[.]121[.]162[.]0/24 block, there are even more hosts related via the mta-sts domain pattern included in a vhost dump. Based on the domains it is likely that these are all Kimsuky related as well.

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

applesec[.]info
automail-notifications[.]com
blog[.]iancaddis[.]com
democracycelebration[.]com
hostmail-server[.]com
iancaddis[.]com
mail[.]iancaddis[.]com
mta-sts[.]democracycelebration[.]com
mta-sts[.]iancaddis[.]com
np[.]chirumi[.]ru
vpn604306770[.]softether[.]net
webmail[.]iancaddis[.]com
www[.]democracycelebration[.]com
www[.]iancaddis[.]com
xpmediaweb[.]net

Specifically pointing out the host here at https://search.censys.io/hosts/192.121.162.235 hosting the chirumi domain here, as it doesn't display the tech stack known for Kimsuky, but presents a redirect to the Japenese media company NHK, which lines up with the history of DPRK targeting against Japan.

154.90.63.0/24

In similar fashion, 154[.]90[.]63.0/24 also is generally attacker controlled aside from some irrelevant IPs. Known indicators for Kimsuky range from 154[.]90[.]63.7 to 154[.]90[.]63.220, with an interesting note of 154[.]90[.]63.63 holding a Havoc C2. (https://github.com/search?q=repo%3Astamparm%2Fmaltrail%20%2F154%5C.90%5C.63%5C..%2B%2F&type=code)

Some fun indicators here are 154[.]90[.]63.6 which held domains such as ntshomes[.]online, ntsposting[.]site, ntskorea[.]site, and wetaxio[.]site. The *nts** domains, as one might guess, are already known indicators and heavily reused across campaigns. (see https://github.com/search?q=repo%3Astamparm%2Fmaltrail+AND+path%3A%2Ftrails%2Fstatic%2Fmalware%2F*_kimsuky.txt+%2Fnts%5Cw%2B%5C.%28site%7Conline%29%2F+&type=code)
The wetax domains also link us to 154[.]90[.]63[.]101 via https://github.com/stamparm/maltrail/blob/e9f6de6e9c74a1fb8b9eb73dbbffb67c554575

Authored by fopwn
0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

6d/trails/static/malware/apt_kimsuky.txt#L11312. Following the ASN's vhost listings, there exist various viagra related domains, as well as korean news-like sites.

korvi365.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
wix
80/HTTP

kr01.withpartner.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
80/HTTP

krconsnews.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
jquery
80/HTTP

krdambee.click (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
elementor jquery jquery-migrate wordpress
80/HTTP

krgeojegreennews.click (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
jquery site-kit wordpress
80/HTTP

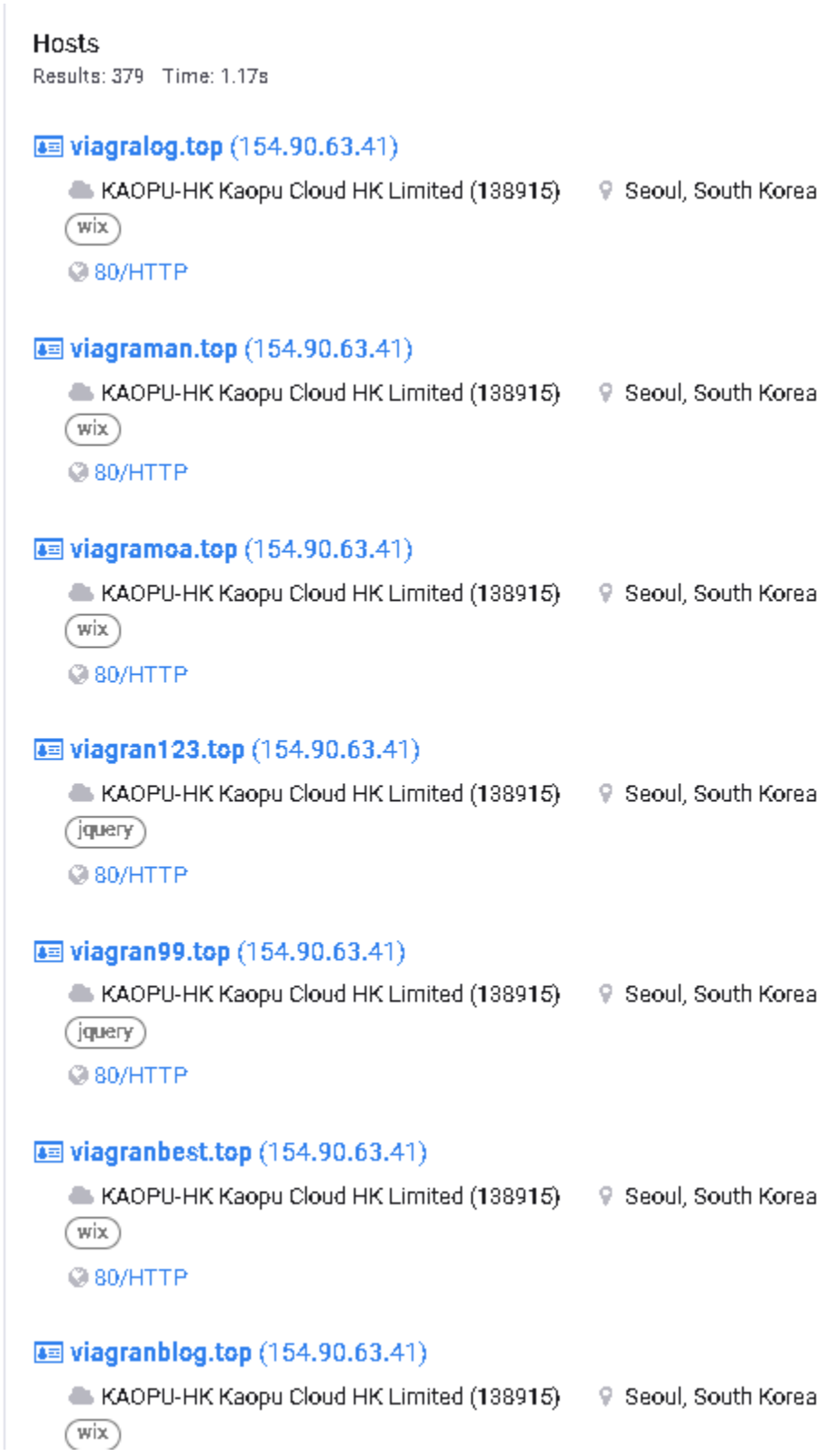
krsateconomy.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
jquery
80/HTTP

krthepopnews.click (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
elementor jquery jquery-migrate wordpress
80/HTTP

krtoworld21.click (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
elementor jquery jquery-migrate wordpress
80/HTTP

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16



Hosts
Results: 379 Time: 1.17s

viagralog.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
wix
80/HTTP

viagraman.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
wix
80/HTTP

viagramoa.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
wix
80/HTTP

viagran123.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
jquery
80/HTTP

viagran99.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
jquery
80/HTTP

viagranbest.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
wix
80/HTTP

viagranblog.top (154.90.63.41)
KAOPU-HK Kaopu Cloud HK Limited (138915) Seoul, South Korea
wix

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

These are all clustered around 154[.]90[.]63[.]41, which can be found at https://search.censys.io/hosts/154.90.63.41. While that IP alone only seems *weird* and not malicious, we move on to check its surroundings, where we find 154[.]90[.]63[.]47. This holds various suspicious domains, such as file[.]microsoftonline[.]msonazure[.]com, www[.]knstock[.]com, and www[.]shoo-oop[.]com. Interestingly, all of these domains had JS code that would call out to the WhatsApp API.

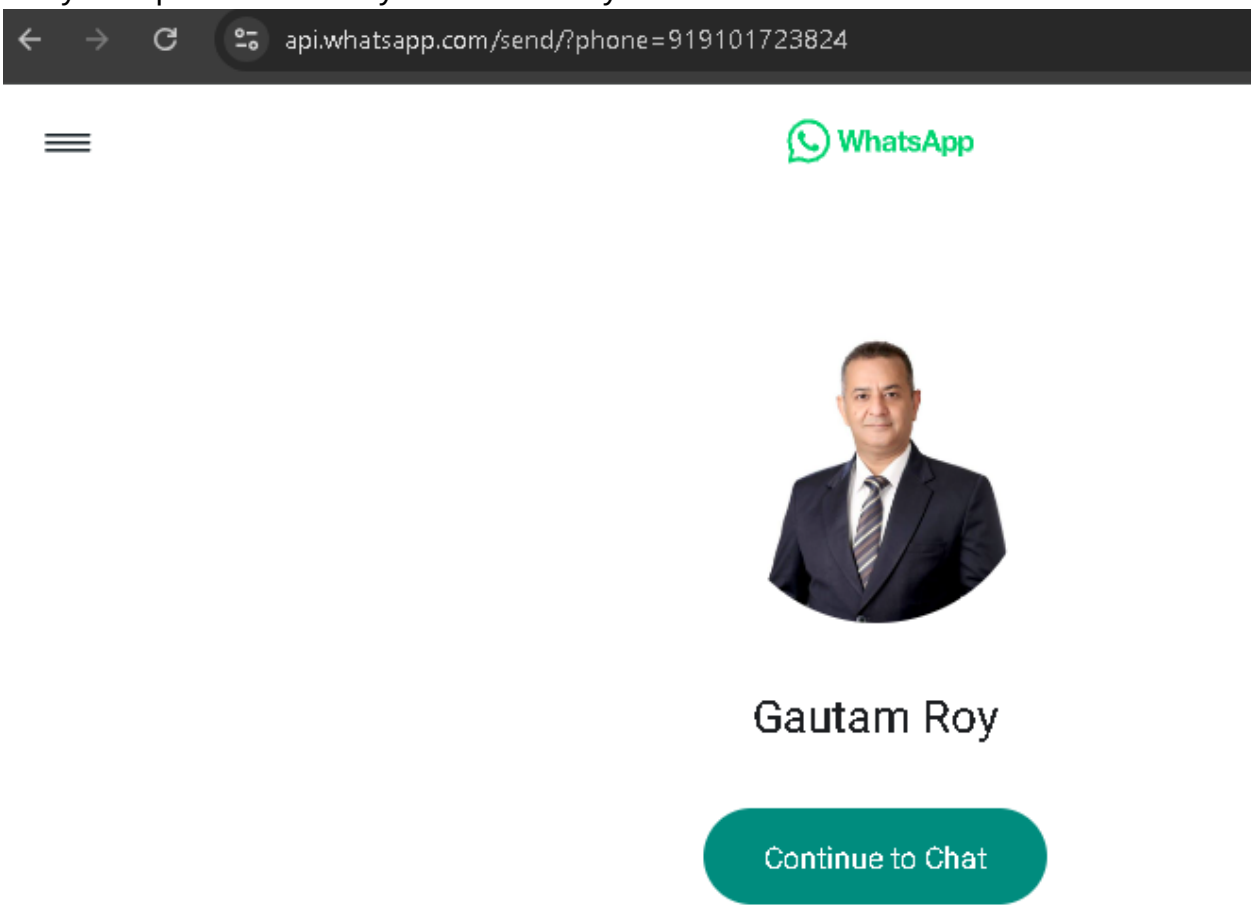
```
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=gbk">
<script language="javascript">
   function readcookie(name) {
       var cookievalue = "";
       var search = name + "=";
       if (document[.]cookie[.]length > 0) {
           offset = document[.]cookie[.]indexOf(search);
           if (offset != -1) {
               offset += search[.]length;
               end = document[.]cookie[.]indexOf(";", offset);
               if (end == -1) end = document[.]cookie[.]length;
               cookievalue =
unescape(document[.]cookie[.]substring(offset, end))
           }
       }
       return cookievalue;
   }
var HostArr = [
"hxxps[://]wa[.]me/919101723824?text=hello",

]

var HostIdx = Math[.]floor(Math[.]random() * (HostArr[.]length));
var HostVal = HostArr[HostIdx];
window[.]onload = function () {
document[.]location = HostVal;
}
</script></head>
<body>
</body>
```


Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

```
</html>
```

Searching for this specific response hash: **sha256:f74c0dc1748830fd51ea45a49e8b4ae248d178449f8e43d41c2d94e1e7e9626**, we only find domains on the aforementioned IP. The phone number links to a likely masqueraded identity of Gautam Roy.



Reverse image searching the picture leads us to an account named SanjayPawah: https://x.com/SanjayPawah.

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857ae450597aa75d96efe6a359adf9c16


The Sanjay Pawah
84 posts
Engineer YOUR sales success
Cultivating YOUR High-Performing Teams for up to 50% Surge in Sales and Market Share
Follow
The Sanjay Pawah
@SanjayPawah
Cultivating YOUR high-performance sales teams as India's first Talentpreneur Mentor | Business Coach | HR Business Partner | Sales Talent Acquisition Specialist
Professional Services
Faridabad,(Haryana)India
Joined May 2021
18 Following
16 Followers
Not followed by anyone you're following
Posts
Replies
Media
Pinned
The Sanjay Pawah @SanjayPawah · Jan 17
"From Depression's depths to India's 1st Talentpreneur Mentor"
At 19, I braved the entrepreneurial storm, faced 7 failures & overcame Despair.
The journey, from ICU to Influencer, led me to Mentorship, Success & a Legacy of Resilience.
A story of Hope, Defiance and Triumph.

Other notable domains following these are found on 154[.]90[.]63[.]72, such as flyasian[.]online, korean-air[.]cloud, nts-mail[.]cloud, and many more. Most of the domain allocations are from this month, September, and mirror prior campaigns targeting the same user base. (https://search.censys.io/hosts/154.90.63.72/data/table and https://github.com/stamparm/maltrail/blob/e9f6de6e9c74a1fb8b9eb73dbbffb67c5545756d/trails/static/malware/apt_kimsuky.txt#L7758)
These domains are relatively standard within the Kimsuky arsenal, with the 200 OK response and 0 content length.

For an emerging IOC, 154[.]90[.]63[.]73 is currently hosting only a default Apache page with no SSL. Censys first detected port 80 allocation on September 23rd 2:37pm UTC.The domain, web[.]bluecash[.]tech, is most likely targeting American Express BlueCash members. 154[.]90[.]63[.]95 is hosting navor[.]online which is an IOC which used to be in the 210[.]92[.]18[.]0/24 cluster found in Maltrail. (https://github.com/stamparm/maltrail/blob/3c2b32e6356b059279a8cc077e41d1fc9e395548/trails/static/malware/apt_kimsuky.txt#L9808)

Any domains on 154[.]90[.]63[.]133 (*[.]purelyasia[.]com), 154[.]90[.]63[.]158 (vipgoogle[.]top), 154[.]90[.]63[.]162 (*[.]random[.]ntsapp[.]space), 154[.]90[.]63[.]164 (navcorp[.]site), 154[.]90[.]63[.]176 (krv[.]blue-stone[.]net),154[.]90[.]63[.]181 (api[.]toyota898[.]com), and 154[.]90[.]63[.]182 (mail[.]sbcgloball[.]store) are more than likely Kimsuky associated based on their domain name patterns. The entire block's domains are included at the end of the report in the IOC section.

27.255.80.0/24

Interestingly, there is not much data in Maltrail for the 27[.]255[.]80[.]0/24 block. The 27[.]255[.]80[.]162 is included as an IOC in the Talos writeup, so let's take a look at the block to see if this might be Kimsuky operated. One suspicious IP is 27[.]255[.]80[.]194 at https://search.censys.io/hosts/27.255.80.194, with mta-sts domain names, which starts off a chain of these domains, all through 27[.]255[.]80[.]199.

telcourse[.]com
thegallerybistro[.]com
theparodyshow[.]com
thevanderveldes[.]com

Authored by fopwn
0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857ae450597aa75d96efe6a359adf9c16

thewrayslIc[.]com
Pocketpills[.]me

Peaking into Lazarus

It's notable that various MoonPeak IPs from the Talos writeup haven't shown up in any of the analyses yet. This is due to the fact that their usage and indicators are outside of my accessible range on Censys, but Validin helps us out in that regard. As Validin only uses SHA1 hashes for body responses, we need to use ***sha1:c002186216f972bb72f8193cdab9717452aad212***. These hosts can be found via https://app.validin.com/detail?find=c002186216f972bb72f8193cdab9717452aad212&type=hash&ref_id=ca4b70e8eda#tab=host_pairs_v2

91[.]194[.]161[.]109, 104[.]194[.]152[.]251, and 167[.]88[.]173[.]173 are present in the results.

95[.]164[.]86[.]148, and 210[.]92[.]18[.]169 were standard XenoRat.

During the time of writing this up, a new MoonPeak C2 was allocated at https://search.censys.io/hosts/91.194.160.13 which is hosted in STARK's Tokyo data center. Thanks to Aidan from Censys for the reminder to diff the domains that day, and the analysis is covered in https://x.com/eastside_nci/status/1838687289750208568.

The 104[.]194[.]152[.]251 IP coincidentally is also relatively close to a cluster of Lazarus attributed domains at 104[.]194[.]153[.]133. These relate to the domains from Elastic's DPRK Code of Conduct writeup: https://www.elastic.co/security-labs/dprk-code-of-conduct. The domains for that campaign, such as akamaitechnologies[.]online, held the Kimsuky tech stack, including indicators such as 0 content length and 200/302 response codes. Based on this, and pivots from Maltrail (https://github.com/stamparm/maltrail/blob/3c2b32e6356b059279a8cc077e41d1fc9e395548/trails/static/malware/apt_lazarus.txt#L3454), the follow on action was to check the ASN for matching IPs/hosts. The list is included in the IOCs section under "ROUTERHOSTING Lazarus".

Further confirmation that this is more likely Lazarus is the gdrivemail[.]site domain, alongside updatecheck[.]v6[.]rocks and the meeting/meet domains. The gdrive aspect of the domain name is found in Lazarus and BlueNoroff lists: https://github.com/stamparm/maltrail/blob/3c2b32e6356b059279a8cc077e41d1fc9e395548/trails/static/malware/apt_lazarus.txt#L853 and

https://github.com/stamparm/maltrail/blob/3c2b32e6356b059279a8cc077e41d1fc9e395548/trails/static/malware/apt_bluenoroff.txt#L7

The updatecheck[.]v6[.]rocks at https://search.censys.io/hosts/45.61.151.17 domain links thematically to two Lazarus/BlueNoroff domains, versionupdate[.]dns[.]army at https://search.censys.io/hosts/45.61.140.26 , which is tagged, and updatecheck[.]dns[.]navy at https://search.censys.io/hosts/45.61.150.15.

The meeting domains, such as meeting[.]sellinicapital[.]com, were reported on by myself at https://x.com/eastside_nci/status/1836605224020033548, in relation to domains at 45[.]61[.]135[.]105. Looking at https://search.censys.io/hosts/45.61.135.105, recent domains added include online[.]zoom-client[.]com and www[.]frameworks[.]ventures. This complicates some attribution aspects as zoom-client seems more related to Kimsuky attributed domains found at https://github.com/stamparm/maltrail/blob/3c2b32e6356b059279a8cc077e41d1fc9e395548/trails/static/malware/apt_kimsuky.txt#L10875. This IP was also reported on by myself in https://x.com/eastside_nci/status/1836494627987443806.

Following these trends, and checking for hosts matching the below query, we find a cluster within AS-CHOOPA.

(same_service(services.http.response.headers: (key: `Server` and value.headers: "Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.?.??") and services.http.response.status_code:302 and services.http.response.body_size:0 and services.http.response.headers.location:"google.com")) and autonomous_system.name=`AS-CHOOPA`

As it turns out, these are the current vhost locations for the domains found in the ROUTERHOSTING cluster. The current IP is 141[.]164[.]44[.]25 over at https://search.censys.io/hosts/141.164.44.25 holds the certificate for gdrivemail[.]site, while also seeing domain name allocation since September 6th through September 23rd.

allowservice[.]store
blockaccess[.]store
confirnuser[.]store
denyaccess[.]site
gplayall[.]store
repairservice[.]store
requestrecover[.]store
rnailservice[.]store
serveicecheck[.]store
servicegroup[.]store
www[.]blockaccess[.]store

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

www[.]confirnuser[.]store
www[.]gplayall[.]store
www[.]repairservice[.]store
www[.]requestrecover[.]store

This once again muddies the attribution space, as repairservice[.]store is attributed to Kimsuky according to Maltrail https://github.com/stamparm/maltrail/blob/eb74d9eafdcd1a4cdec143bc4c1606b83af5662d/trails/static/malware/apt_kimsuky.txt#L8898.
Additionally, 158[.]247[.]216[.]107 at https://search.censys.io/hosts/158.247.216.107 seems to be another related IP, as they both overlap on the service domains. These have been allocated since the 24th of September.

Conclusions

A table of netblocks historically operated by Kimsuky is listed below:

27.255.75.0/24
27.255.80.0/24
27.255.81.0/24
61.97.251.0/24
154.90.63.0/24
167.88.172.0/24*
192.121.162.0/24
210.92.18.0/24

*Potentially BlueNoroff

Thanks to some help from @0xmh1, we can find some history in more esoteric areas of the internet as well. The domain my[.]view-hwp[.]kro[.]kr popped up in some broad ranging searches on the tech stack with 302 redirects to Google. These were hosted on 202[.]131[.]233[.]167 at https://search.censys.io/hosts/202.131.233.167. The hwp based domain names are also historically relevant, linking back to a 2023 campaign reported on by SentinelOne here https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/. Beyond this, the IP has included domain names targeting the Japanese Ministry of Foreign Affairs, which is a likely target for any DPRK foreign espionage operations.

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

Image credit goes to https://x.com/0xmh1

In retrospect, it is much more difficult than anticipated to categorize DPRK activity neatly into their own little brackets. Each respective government organization, and therefore the APTs we use to represent their cyber capabilities, works towards the goals of Kim-Jong Un. Overlap in targeting and capabilities is more than likely to occur, as we explicitly saw between Kimsuky's MoonPeak and Lazarus' VMConnect campaign.

My own distinctions between actors lies in their tech stack versions, alongside where they host, and how they write their domains. As was mentioned with ROUTERHOSTING, one of the MoonPeak IPs was in close proximity to an IP IOC from the Elastic writeup, which would re-emerge upon using a Kimsuky-inspired query. The query used to separate these for now is ***(same_service(services.http.response.headers: (key: `Server` and value.headers: "Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.?.??") and***

services.http.response.status_code:302 and services.http.response.body_size:0 and services.http.response.headers.Location:"https://google.com"))

It seems like there is some form of intermediary between Kimsuky and Lazarus Group who uses a similar set of shared tactics. This actor doesn't appear to be Talos' UAT-5394 based on hosting distributions. This could potentially be the current iteration of what has been tracked as BlueNoroff. Being a sub-group of Lazarus, we expect there to be overlaps but also deviations from their known crypto related targeting. Notably, the updatecheck[.]v6[.]rocks domain, linked to the BlueNoroff tagged IP, alongside the specific usage of gdrivemail[.]site, all link this to historical BN campaigns. The subgroup specifically has a history of using the gdrive prefix with the .site TLD.
https://github.com/stamparm/maltrail/blob/3c2b32e6356b059279a8cc077e41d1fc9e395548/trails/static/malware/apt_bluenoroff.txt#L382 provides an entry for a good overview on this.

If we take this at face-value and say BlueNoroff is a group connecting Kimsuky and Lazarus operations, we can reasonably assume that even more server tech overlaps may exist. The distinguishing indicator being the *primary* usage of ROUTERHOSTING, allows us to find some more domains that could well be related to DPRK operations. We have seen (again at face-value) BN hosting at 167[.]88[.]172[.]115 with the Gdrive domain, and as it turns out 167[.]88[.]172[.]218 hosts a Binance themed phishing domain, supporto-reddito-binance[.]com at https://search.censys.io/hosts/167.88.172.218+supporto-reddito-binance.com. This presents the established tech stack, but also allows us to find an interesting pivot into related crypto-phishing operations. Based on the response's HTML tags from the image, we are able to deduce a usable query to find more related domains.

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

services.http.response.html_tags	<title data-shuvi-head="true">Accedi | Binance</title>
services.http.response.html_tags	<meta charset="utf-8">
services.http.response.html_tags	<meta name="og:type" content="website">
services.http.response.html_tags	<meta property="og:title" content="Bitcoin Exchange | Cryptocurrency Exchange | Binance">
services.http.response.html_tags	<meta property="og:description" content="Binance cryptocurrency exchange - We operate the worlds biggest bitcoin exchange and altcoin crypto exchange in the world by volume">
services.http.response.html_tags	<meta name="keywords" content="Blockchain Crypto Exchange, Cryptocurrency Exchange, Bitcoin Trading, Ethereum price trend, BNB, CZ, BTC price, ETH wallet registration, LTC price, Binance, Poloniex, Bittrex" data-shuvi-head="true">
services.http.response.html_tags	<meta property="og:title" content="Accedi | Binance" data-shuvi-head="true">
services.http.response.html_tags	<meta property="og:site_name" content="Binance" data-shuvi-head="true">
services.http.response.html_tags	<meta property="twitter:title" content="Accedi | Binance" data-shuvi-head="true">
services.http.response.html_tags	<meta property="twitter:card" content="summary_large_image" data-shuvi-head="true">
services.http.response.html_tags	<meta name="description" content="login-description" data-shuvi-head="true">
services.http.response.html_tags	<meta property="og:description" content="login-description" data-shuvi-head="true">
services.http.response.html_tags	<meta property="twitter:description" content="login-description" data-shuvi-head="true">
services.http.response.html_tags	<meta http-equiv="etag" content="e9b75200e32e25f3ba29637ff7cddc76225b4180">
services.http.response.html_tags	<meta name="viewport" content="width=device-width,initial-scale=1.0,maximum-scale=1.0,minimum-scale=1.0,user-scalable=no">
services.http.response.html_tags	<meta name="format-detection" content="telephone=no">
services.http.response.html_tags	<meta name="360-site-verification" content="e362348efd31ed6e77bcf0ba4963a6de">
services.http.response.html_tags	<meta name="sogou_site_verification" content="tKz9Rld4qH">
services.http.response.html_tags	<meta name="robots" content="index" data-shuvi-head="true">
services.http.response.html_tags	<meta name="referrer" content="no-referrer">
services.http.response.body_size	38310
services.http.response.body	<!DOCTYPE html><html lang="en" dir="ltr"><head><meta charset="utf-8"><meta name="og:type" content="website"><meta property="og:title" content="Bitcoin Exchange | Cryptocu

services.http.response.html_tags="<meta name=\"keywords\" content=\"Blockchain Crypto Exchange, Cryptocurrency Exchange, Bitcoin Trading, Ethereum price trend, BNB, CZ, BTC price, ETH wallet registration, LTC price, Binance, Poloniex, Bittrex\" data-shuvi-head=\"true\">"

A list of domains showing this pattern is included in the IOCs section under Crypto IOCs.

To close this out, it was quite interesting that both of those domains were hosted in 167[.]88[.]172[.]0/24. Important for attribution here are 167[.]88[.]172[.]52 at https://search.censys.io/hosts/167.88.172.52. With domain names such as naver[.]downallfiles[.]store, the down/download lure seems to be more used across BlueNoroff campaigns. Another malicious indicator is unorg[.]store which resolved to 167[.]88[.]172[.]83 on August 16th. Following the sequential allocation patterns, 167[.]88[.]172[.]84 hosted usavoip[.]il[.]3cx[.]us, blatantly targeting 3CX, who has notoriously been affected by DPRK attacks. Further down the line, we see some more Apple/iCloud related domains, namely *[.]setting-icloud[.]info at 167[.]88[.]172[.]131 as of September 15th, but now taken down. With these in mind, unless you have specific reasons to access IPs in that range, with moderate confidence we can say that the 167[.]88[.]172[.]0/24 is an operating ground for BlueNoroff.

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

Further Investigations

This last bit aims to correlate various information shared after limited disclosure of this threat brief. TLP_R3D also posted the query publicly at https://x.com/TLP_R3D/status/1844803543267471606 which expedited this writeup. Recent days have seen continued allocations of MoonPeak C2s targeting various broader sectors. My tweet at https://x.com/eastside_nci/status/1843741402775404590 covers the ongoing use of Apple related domains for deploying MoonPeak, alongside some Microsoft related domains via login[.]microsoft365[.]com[.]ng. Additionally, 0xMH1 described some more domains also popping up in the MoonPeak hash query: https://x.com/0xmh1/status/1844650735746810362. (poseides[.]store, sellura[.]store, and apporigin[.]store)

Recently, Mikhail from Maltrail and myself looked at https://search.censys.io/hosts/63.250.44.85, specifically, scs[.]visa[.]mofa[.]gov[.]sa[.]dnss[.]world. This seems to be targeting the Saudi Arabian Ministry of Foreign Affairs, which is completely new for Kimsuky, at least to my knowledge. While there has been history of the DPRK regime supporting anti-KSA groups, such as the Houthis, this supports seems to mostly be limited to providing kinetic support (https://www.brookings.edu/articles/expect-to-see-more-north-korean-weapons-reach-nonstate-armed-actors-in-2024/) rather than involvement in the cybersphere. Our reasoning and support for this attribution is the banner hash used on the domain: **services.banner_hashes="sha256:14309ae76fa5485d6498b8cda9c17e4f9e0e0a58a4fe98c47656b80bc5e6bc09"**.

This hash specifically links back to other Kimsuky attributed domains that were found and reported on, specifically the cluster including targeting of the Wilson Center. These domains and my initial thoughts on them can be found at https://x.com/eastside_nci/status/1829413692372586570.

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

kemop.cj7778.top (23.27.202.204)

EVOXTENTERPRISE-AS-AP Evoxt Enterprise (149440) New York, United States

1 Matched Service

80/HTTP

1 Other Service

443/HTTP

zy5.tuling168.cfd (23.27.202.204)

EVOXTENTERPRISE-AS-AP Evoxt Enterprise (149440) New York, United States

2 Matched Services

80/HTTP 443/HTTP

scs.visa.mofa.gov.sa.dnss.world (63.250.44.85)

NAMECHEAP-NET (22612) Arizona, United States

1 Matched Service

443/HTTP

nid-naver.ddnsking.com (183.111.125.44)

KIXS-AS-KR Korea Telecom (4766) Incheon, South Korea

2 Matched Services

80/HTTP 443/HTTP

drive.wilsoncenter.port0.org (185.203.119.14)

BELCLOUD (44901) Sofia-Capital, Bulgaria

2 Matched Services

443/HTTP 80/HTTP

mydrive.home.kg (185.203.119.14)

BELCLOUD (44901) Sofia-Capital, Bulgaria

2 Matched Services

80/HTTP 443/HTTP

naververify.p-e.kr (185.203.119.14)

BELCLOUD (44901) Sofia-Capital, Bulgaria

1 Matched Service

443/HTTP

uidlogin.o-r.kr (185.203.119.14)

BELCLOUD (44901) Sofia-Capital, Bulgaria

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df155131591 7f05036db562857a
e450597aa75d96efe6a359adf9c16

The domains all point to historical targeting patterns of Kimsuky, alongside the tech stack used in certain Operation Dream Job campaigns (https://x.com/asdasd13asbz/status/1791390914038149339). Based on these indicators, these have been added to Maltrail as Kimsuky domains (https://github.com/stamparm/maltrail/commit/2820d8ca8ec09f23d00ee03843ae89f77dfd2134). It is almost predeicatable to see an influx of Saudi targeting, especially due to their recent commitment to a defense partnership with the ROK (https://www.reuters.com/world/south-korea-saudi-arabia-sign-agreement-defence-cooperation-2024-02-05/), alongside their continued decrease of trade with North Korea (https://oec.world/en/profile/bilateral-country/sau/partner/prk). It also would not be a surprise if this operation could be aligned with gaining intelligence on ROK-KSA contracts, weapons details, and most likely individuals seeking visas. Several high level ROK officials have been officially stated to be "exchanged" to Saudi Arabia over the past years, such as "Minister of Trade, Industry and Energy, Dukgeun Ahn" in April 2024. (https://www.mofa.go.kr/eng/nation/m_4902/view.do?seq=193) The Korean MOFA states there are 2400 Koreans living in the KSA, which would allow DPRK actors a very niche look into the lives of likely successful Korean business people now operating abroad. Additionally, the MOFA has information related to future diplomatic exchanges, which could be used for pre-creation of new spearphishing lures.

Disclaimer: At the time of writing, some of the information is incomplete or outdated. The vast majority of these domains should still be accessible via non-enterprise versions of Censys, but if not Validin will have the historical domains indexed.

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

Netblock IOCs

154.90.63.0/24

154[.]90[.]63[.]6: line601[.]top, ntshomes[.]online, ntskorea[.]site, ntsposting[.]site, wetaxio[.]site, www[.]ntshomes[.]online, ywhg3[.]yw520[.]org, zhy6699[.]top
154[.]90[.]63[.]26: casugdksald[.]top, fivoyoiofax[.]top, www[.]tmallchain[.]vip, yoivisaeiov[.]top
154[.]90[.]63[.]27: inspectt[.]xyz, kld-kokoa[.]online, www[.]inspectt[.]xyz
154[.]90[.]63[.]33: htijertyul[.]top, qwifjlkgdjg[.]top
154[.]90[.]63[.]36: 5234[.]degine[.]asia
154[.]90[.]63[.]37: hg5[.]yw520[.]org
154[.]90[.]63[.]38: composite[.]oam007[.]icu, h5[.]cott[.]top
154[.]90[.]63[.]40: seo1889tx[.]com, wk55151[.]top, www[.]wk55151[.]top, yl2[.]xlk668801[.]top
154[.]90[.]63[.]41: 059879e5-b2e8-4f58-aa46-95f69d92aa34[.]random[.]dyunews[.]click, 059879e5-b2e8-4f58-aa46-95f69d92aa34[.]random[.]koreavi58[.]click, 059879e5-b2e8-4f58-aa46-95f69d92aa34[.]random[.]koreavi79[.]click, 059879e5-b2e8-4f58-aa46-95f69d92aa34[.]random[.]krsateconomy[.]top, 059879e5-b2e8-4f58-aa46-95f69d92aa34[.]random[.]ytongsin[.]click, 123yaggug[.]top, 24parmacy[.]koreavia365[.]top, 24pharmacy[.]top, 24yaggug[.]top, 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]365yaggug[.]top, 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]dyunews[.]click, 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]krtoworld21[.]click, 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]viagraclub[.]top, 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]viagrandata[.]top, 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]viasky[.]top, 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]viaya[.]top, 365yaggug[.]top, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]kvia1004[.]top, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]kvia365[.]top, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]viagrajo[.]top, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]viagraman[.]top, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]viagratoo[.]top, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]viayy[.]top, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]yjilbo[.]click, bgptools-wildcard-confirmed[.]kvia123[.]top, bgptools-wildcard-confirmed[.]viagraclub[.]top, bgptools-wildcard-confirmed[.]ytongsin[.]click, dyunews[.]click, hanayak[.]krvia58[.]top, hanayak[.]vnaa[.]top, kdonggukin[.]top, koreapenvill[.]click, koreavi58[.]click, koreavi79[.]click, koreavi99[.]click, koreavia070[.]top, koreavia24[.]top, koreavia365[.]top, korvi010[.]top, korvi123[.]top, korvi365[.]top, kr01[.]withpartner[.]top, krconsnews[.]top, krdambee[.]click, krgeojegreennews[.]click, krsateconomy[.]top, krthepopnews[.]click, krtoworld21[.]click, krvia58[.]top, krvia79[.]top, krviagi[.]top, krviakong[.]top, krviasky[.]top, krwoman25[.]click, kukey[.]click, kvia1004[.]top, kvia123[.]top, kvia365[.]top, nmeftdaejinyutong[.]koreavi99[.]click, qldkrmfk123[.]top,

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

qldkrmfk24[.]top, qldkrmfk365[.]top, qldkrmfkdirrnr[.]top, qldkrmfkgnrl[.]top, thegoyang[.]click, tldkffltmgnrl[.]top, vabb[.]top, via-mall[.]top, via070[.]top, viadd[.]top, viaee[.]top, viagra[.]krvia58[.]top, viagraapp[.]top, viagraclub[.]top, viagrajo[.]top
154[.]90[.]63[.]41: viagralog[.]top, viagraman[.]top, viagramoa[.]top, viagran123[.]top, viagran99[.]top, viagranbest[.]top, viagranblog[.]top, viagrandata[.]top, viagrandoumi[.]top, viagrannews[.]top, viagratab[.]top, viagratoo[.]top, viamoa[.]top, viasky[.]top, viatt[.]top, viawhat[.]top, viaya[.]top, viayy[.]top, vndd[.]top, vnee[.]top, vnff[.]top, www[.]krdambee[.]click, www[.]krthepopnews[.]click, www[.]krtoworld21[.]click, www[.]krvia58[.]top, www[.]vabb[.]top, www[.]viagran123[.]top, www[.]viagranbest[.]top, yjilbo[.]click, yondo[.]click, ytongsin[.]click
154[.]90[.]63[.]43: kr-sl-01[.]serverintoshell[.]com
154[.]90[.]63[.]44: gadaxbedvd[.]top, hadfecderf[.]top, uionersto[.]top
154[.]90[.]63[.]47: abaofen[.]com, file[.]microsoftonline[.]msonazure[.]com, knstock[.]com, login[.]microsoftonline[.]msonazure[.]com, shoo-oop[.]com, sytegdj[.]com, www[.]abaofen[.]com, www[.]knstock[.]com, www[.]microsoftonline[.]msonazure[.]com, www[.]shoo-oop[.]com
154[.]90[.]63[.]51: sioumsacd[.]top
154[.]90[.]63[.]53: hoduaosuba[.]top, kjhgfdsazx[.]top, savxiouter[.]top
154[.]90[.]63[.]72: 2c8b3f19-0325-4acc-a3dd-31a918e4dbf5[.]random[.]wetax[.]online, flyasian[.]online, korean-air[.]cloud, nts-app[.]cloud, nts-mail[.]cloud, ntshomes[.]info, ntshomes[.]online, ntsinf[.]cloud, ntsxapp[.]site, wetaxio[.]site, www[.]ntshomes[.]online, www[.]ntsinf[.]cloud
154[.]90[.]63[.]73: web[.]bluecash[.]tech
154[.]90[.]63[.]74: exchangemail[.]c[.]discoverogun[.]net, siuobgnfbs[.]top
154[.]90[.]63[.]77: bdiasuouer[.]top
154[.]90[.]63[.]80: kbcofficialsite[.]com, proto-win[.]com, sunbirdshobbies[.]com, www[.]kbcofficialsite[.]com, www[.]proto-win[.]com, www[.]sunbirdshobbies[.]com
154[.]90[.]63[.]83: picklsoboc[.]top, siuerotfns[.]top
154[.]90[.]63[.]84: pl999[.]yw520[.]org
154[.]90[.]63[.]95: www[.]navor[.]online
154[.]90[.]63[.]99: buuhdsoah[.]top
154[.]90[.]63[.]103: www[.]wpresto[.]xyz
154[.]90[.]63[.]114: haninsight[.]com
154[.]90[.]63[.]115: alphabet633[.]top, b01[.]tiktok132[.]com, oiulduckbac[.]top
154[.]90[.]63[.]119: clh123[.]com, markw4[.]bb139[.]com, w1[.]147dh[.]com, w1[.]258dh[.]com, w4[.]bb139[.]com, www[.]clh123[.]com
154[.]90[.]63[.]123: gdadgaedgft[.]top
154[.]90[.]63[.]125: hasuihdfasa[.]top
154[.]90[.]63[.]133: admin[.]purelyasia[.]com, callbacks-direct[.]purelyasia[.]com, callbacks[.]purelyasia[.]com, docs[.]purelyasia[.]com, git[.]purelyasia[.]com, gocallbacks-direct[.]purelyasia[.]com, kibana[.]purelyasia[.]com
154[.]90[.]63[.]141: duiashidoui[.]top, huderfgeg[.]top, roiuknbaszc[.]top, uityersto[.]top
154[.]90[.]63[.]141: utgdutrdh[.]top
154[.]90[.]63[.]143: fndhuviocs[.]top
154[.]90[.]63[.]144: 2znl[.]yw520[.]org, fashofuodasu[.]vip, kr2[.]pg360[.]xyz, picsaoutgf[.]top

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

154[.]90[.]63[.]149: hengbyudfegc[.]top, hengdyuenfh[.]top, odliasb[.]com, znl11[.]yw520[.]org
154[.]90[.]63[.]150: kr03[.]letsvpn[.]cloud
154[.]90[.]63[.]155: gengdededr[.]top, hresthsdgfgd[.]top, roiuytasdsk[.]top, ruioytesam[.]top
154[.]90[.]63[.]157: bhednfhrde[.]top, gugiakhfoiaa[.]top
154[.]90[.]63[.]158: dacadanca[.]top, herangtherd[.]top, hrngaengae[.]top, uagsasghtr[.]top, utbeoutedburt[.]top, vipgoogle[.]top
154[.]90[.]63[.]162: 059879e5-b2e8-4f58-aa46-95f69d92aa34[.]random[.]nicecreclit[.]site, 059879e5-b2e8-4f58-aa46-95f69d92aa34[.]random[.]ntsapp[.]space, 952cd7f5-55c2-472f-bc9d-08487ef75661[.]random[.]ntsapp[.]site, assembly-kr[.]site, basescan[.]website, bgptools-wildcard-confirmed[.]checkpermission[.]cloud, bgptools-wildcard-confirmed[.]epeople-kr[.]site, cdn-0[.]ntsnews[.]online, checkpermission[.]cloud, checkpermission[.]site, cpanel[.]ntsnews[.]online, cpcalendars[.]ntsnews[.]online, cpcontacts[.]ntsnews[.]online, doh[.]checkpermission[.]site, emv1[.]nicecreclit[.]site, epeople-kr[.]site, goocgles[.]site, kr-gov24[.]site, mail[.]ntsnews[.]online, main-alarm[.]space, mois-gov[.]site, nice-creclit[.]website, nicecreclit[.]site, nts-doc[.]site, ntsapp[.]site, ntsapp[.]space, ntsapp[.]store, ntsnews[.]online, open-ai[.]website, qooqlesec[.]site, webdisk[.]ntsnews[.]online, webmail[.]ntsnews[.]online, wetaxalimi[.]icu, wetaxalimi[.]space, www[.]dongwon-mil[.]site, www[.]epeople-kr[.]site, www[.]ntsapp[.]space, www[.]ntsnews[.]online, www[.]wetaxalimi[.]icu
154[.]90[.]63[.]164: navcorp[.]site, www[.]navcorp[.]site
154[.]90[.]63[.]166: a[.]aimayou[.]xyz
154[.]90[.]63[.]174: fouriyesruwe[.]top
154[.]90[.]63[.]176: krv[.]blue-stone[.]net
154[.]90[.]63[.]181: api[.]toyota898[.]com, app[.]mitsubishi1870[.]com, app[.]mitsubishi18700[.]com, ke[.]mitsubishi18700[.]com, kf[.]mitsubishi1870[.]com, kf[.]mitsubishi18700[.]com, kf[.]mitsubishisea[.]com, kf[.]toyota868[.]com, kf[.]toyota898[.]com, mitsubishi1870[.]com, mitsubishiasi[.]com, mitsubishisea[.]com, toyota898[.]com, www[.]mitsubishi1870[.]com, www[.]mitsubishi18700[.]com, www[.]mitsubishiasi[.]com, www[.]mitsubishisea[.]com, www[.]toyota898[.]com
154[.]90[.]63[.]182: mail[.]sbcgloball[.]store
154[.]90[.]63[.]187: bduiaghidkha[.]top, gafvaagdv[.]top, hafaabhcaf[.]top
154[.]90[.]63[.]198: jhgfdsaoiuy[.]top, jiuyotrewas[.]top, kopsansad[.]top
154[.]90[.]63[.]203: umami[.]jqmu[.]xyz
154[.]90[.]63[.]205: ap-north-homura[.]spool[.]tetr[.]io
154[.]90[.]63[.]207: gajfbafgada[.]top, youjdjhdsfh[.]top
154[.]90[.]63[.]209: bdasugiofahf[.]top, iyhuy[.]uufogame[.]com, member-apples[.]info
154[.]90[.]63[.]211: 971nb[.]com
154[.]90[.]63[.]211: kr91[.]oportal[.]cc, vasdvausdgasi[.]top, vip-dinsov[.]top, www[.]971nb[.]com
154[.]90[.]63[.]225: cnaishfkaskao[.]top
154[.]90[.]63[.]227: 1314[.]degine[.]asia
154[.]90[.]63[.]229: abb[.]xteam[.]buzz
154[.]90[.]63[.]234: 154[.]90[.]63[.]234[.]sslip[.]io, dshth[.]uufogame[.]com
154[.]90[.]63[.]245: hoksadwer[.]top
154[.]90[.]63[.]247: hanguo11[.]sdkkk[.]top, hanguo22[.]sdkkk[.]top

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

154[.]90[.]63[.]248: tgdegrfbhebg[.]top
154[.]90[.]63[.]250: sdbnasbnf[.]top
154[.]90[.]63[.]251: huyiwesxa[.]top
154[.]90[.]63[.]253: seoul[.]fotrosna[.]ir

ROUTERHOSTING Lazarus

104[.]194[.]153[.]133: accessservice[.]store
104[.]194[.]153[.]133: activemail[.]store
104[.]194[.]153[.]133: allowservice[.]store
104[.]194[.]153[.]133: clothe10[.]onlinenet[.]store
104[.]194[.]153[.]133: clothe2[.]onlinenet[.]store
104[.]194[.]153[.]133: clothe3[.]onlinenet[.]store
104[.]194[.]153[.]133: clothe4[.]onlinenet[.]store
104[.]194[.]153[.]133: clothe5[.]onlinenet[.]store
104[.]194[.]153[.]133: clothe6[.]onlinenet[.]store
104[.]194[.]153[.]133: everyconnect[.]store
104[.]194[.]153[.]133: gdrivemail[.]site
104[.]194[.]153[.]133: helpsend[.]online
104[.]194[.]153[.]133: onlinenet[.]store
104[.]194[.]153[.]133: receivemail[.]store
104[.]194[.]153[.]133: rnailservice[.]store
104[.]194[.]153[.]133: serveicecheck[.]store
104[.]194[.]153[.]133: servicegroup[.]store
104[.]194[.]153[.]133: supportcentre[.]store
104[.]194[.]153[.]133: www[.]onlinenet[.]store
167[.]88[.]166[.]218: www[.]jiamingho[.]com
167[.]88[.]167[.]162: jovtje[.]online
167[.]88[.]167[.]162: www[.]jovtje[.]online
167[.]88[.]172[.]115: allowservice[.]store
167[.]88[.]172[.]115: confirnuser[.]store
167[.]88[.]172[.]115: denyaccess[.]site
167[.]88[.]172[.]115: repairservice[.]store
172[.]86[.]70[.]114: 172[.]86[.]70[.]114[.]sslip[.]io
45[.]61[.]128[.]122: cardiagnostic[.]net
45[.]61[.]128[.]122: meet[.]caladangroup[.]xyz
45[.]61[.]128[.]122: meet[.]selinicapital[.]online
45[.]61[.]128[.]122: meet[.]selinicapital[.]xyz
45[.]61[.]128[.]122: meeting[.]sellinicapital[.]com
45[.]61[.]128[.]122: shh5[.]baranftw[.]xyz
45[.]61[.]151[.]17: updatecheck[.]v6[.]rocks

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16

TLP:CLEAR

Crypto IOCs

binance-conferme[.]com
d2e0atddryggqg[.]cloudfront[.]net
sfarb[.]top
trsutex-io[.]top
trusts-ex[.]life
trusts-ex[.]org
www[.]trsutex-io[.]top
arbth[.]top
autoconfig[.]dko02[.]vas-server[.]cz
autodiscover[.]dko02[.]vas-server[.]cz
bian[.]cntestsystem[.]com
binancegiveaway[.]getqk[.]com
binanceinfosecurities[.]com
binanceinfosecurity[.]com
chanecoin[.]com
claimclaim[.]pages[.]dev
coinapitaltrust[.]sbs
cointrustapital[.]one
contrusts[.]life
contrusts[.]top
d1jou383zqkjsz[.]cloudfront[.]net
d1p88e31y95sgc[.]cloudfront[.]net
d35c9gbuyjkccx[.]cloudfront[.]net
dichiarazione-redditi-account[.]com
dko02[.]vas-server[.]cz
ec2-52-59-37-184[.]eu-central-1[.]compute[.]amazonaws[.]com
ercth[.]top
help-blnance[.]com
mail[.]dko02[.]vas-server[.]cz
sfeth[.]top
sgcpro[.]cc
supporto-reddito-binance[.]com
tiger24geb[.]life
trusts-ex[.]buzz
trusts-ex[.]cc
trxusha[.]top
wisecryptoinvestor[.]com
www[.]binance-heipers[.]com
www[.]chanecoin[.]com
www[.]sgcpro[.]cc
www[.]wisecryptoinvestor[.]com

TLP:CLEAR

Authored by fopwn

0594f9a6f6e9a8fe5ad05afff1d03f74fade370330ebc3cef1693df69690b93dd99285a2df1551315917f05036db562857a
e450597aa75d96efe6a359adf9c16