Kimsuky Phishing Operations Putting In Work

threatconnect.com/blog/kimsuky-phishing-operations-putting-in-work/

September 28, 2020

Executive Summary

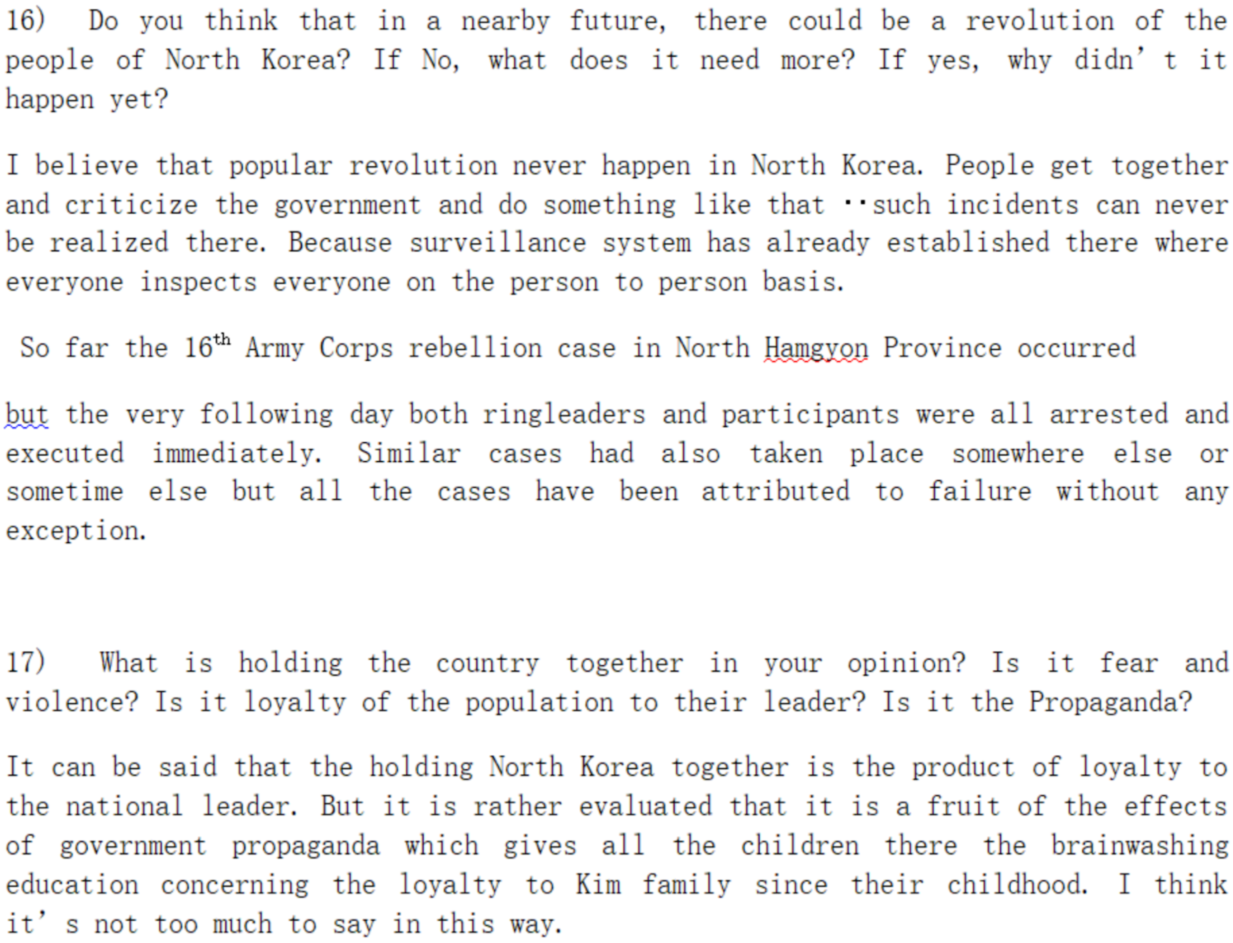
Recently, an international NGO that provides threat sharing and analysis support to frequently targeted communities reached out to ThreatConnect wanting to learn more about the origins of a targeted phishing attack they were researching. Researching both the attacker's infrastructure and tooling, we believe the nexus of the attack to be DPRK's Kimsuky group (aka Velvet Chollima). Kimsuky is notorious for their phishing efforts; researchers even dubbed this group the "King of Spear Phishing" in a 2019 VirusBulletin paper. They are also believed to be behind the attacks on Korea Hydro & Nuclear Power in 2014. The potential targets identified in this research range from journalism to civil society organizations. We suspect the activity discussed here to be part of Kimsuky's efforts to harvest credentials for espionage purposes though we can't rule out for certain that they aren't other objectives.

The international NGO requested that we not share the contents of the phish or point out the organization they are working with. To protect their identity we will share our findings starting from the Kimsuky nexus, which emanates from research published by Korean security firm ESTSecurity on a malicious document. From there, we'll build out an understanding of additional, associated infrastructure and potential targets gleaned from those findings.

Kimsuky Nexus

ESTSecurity inspected a malicious lure document discussing North Korean defectors. This lure document contained a UPX packed binary that reached out to wave[.]posadadesantiago[.]com. Based upon their report we believe SHA256: 252d1b7a379f97fddd691880c1cf93eaeb2a5e5572e92a25240b75953c88736c, either is or is strikingly similar to the document discussed in their blog post based on these similarities:

Lure document text matches the screenshot



16) Do you think that in a nearby future, there could be a revolution of the people of North Korea? If No, what does it need more? If yes, why didn’ t it happen yet?

I believe that popular revolution never happen in North Korea. People get together and criticize the government and do something like that ··such incidents can never be realized there. Because surveillance system has already established there where everyone inspects everyone on the person to person basis.

So far the 16th Army Corps rebellion case in North Hamgyon Province occurred

but the very following day both ringleaders and participants were all arrested and executed immediately. Similar cases had also taken place somewhere else or sometime else but all the cases have been attributed to failure without any exception.

17) What is holding the country together in your opinion? Is it fear and violence? Is it loyalty of the population to their leader? Is it the Propaganda?

It can be said that the holding North Korea together is the product of loyalty to the national leader. But it is rather evaluated that it is a fruit of the effects of government propaganda which gives all the children there the brainwashing education concerning the loyalty to Kim family since their childhood. I think it’ s not too much to say in this way.

Figure 1: Screen Shot From 252d1b7a379f97fddd691880c1cf93eaeb2a5e5572e92a25240b75953c88736c

- The binary used the same string obfuscation technique
- C2 URL hxxp://wave[.]posadadesantiago[.]com/home/dwn.php?van=101
- Malicious document VBA code similarities with what’s shown in the screenshots
- Digital signature signer name EGIS CO., Ltd. in the dropped file

We’ll use this document as the launching point to discover additional infrastructure most likely associated with this attack.

Find All the Things

Before we get into our findings, we want to call out the infrastructure hunting techniques utilized below. Starting with a domain, we’ll look at the IP that hosts the domain and how many other domains are hosted there. In cases where very few and/or similar domains are hosted at the IP, we can assess with a reasonable level of confidence that the IP is dedicated to a single user.

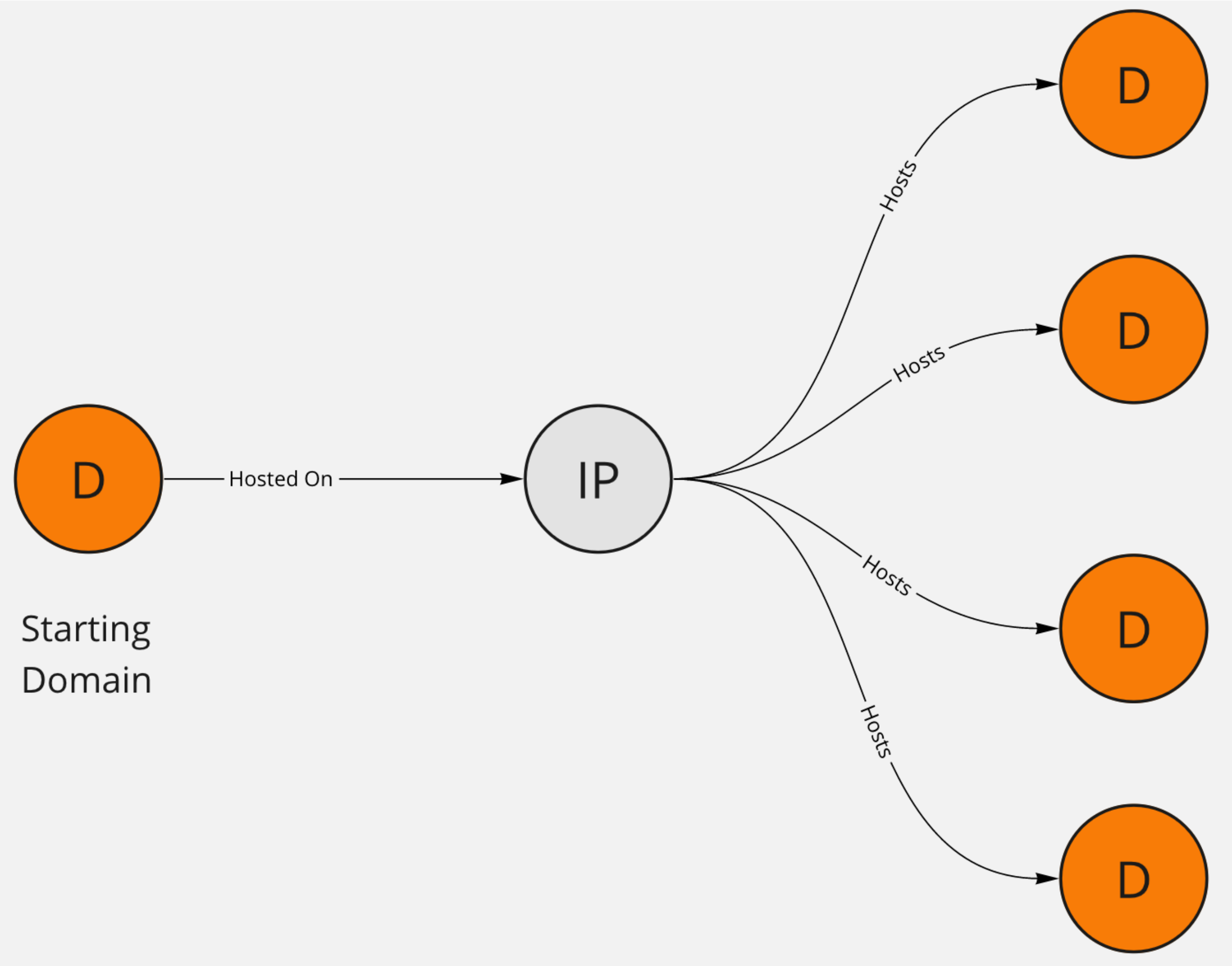


Figure 2: Domain to Hosted On IP to Hosts Domains

The second primary technique used is pivoting off of similar subdomain values which use reasonably unique strings. Think of this as searching on the beginning or middle of a multilevel domain name. Using login.un-phish.bad[.]com as a contrived example we'd search on login.un-phish.* to see what other domains this subdomain was used under. The trick here is not searching on a common string. Subdomain inspection can also hint at the activity behind the domain or even who might be targeted. For example, seeing a URL starting with login suggests that the URL is being used to harvest credentials. Finally, while infrastructure hunting may seem more like an art than a science; remember to always look for additional data points like registrar or hosting information to corroborate the results.

VirusTotal (VT) provides additional information on the malicious document. Here we are looking for any In The Wild (ITW) file origin URLs listed. These URLs sometimes show IPs or domains that served up the file. VT returns this ITW file origin URL:

hxxp://onedrive.sslport[.]work/share/file/interview%20with%20a%20north%20korean%20defector.doc (VT Link)

We now have a domain, let's start the pivots!

IP Pivot

Taking this domain, sslport[.]work, pivot off the IP hosting the domain to uncover a number of domains hosted on the same IP.

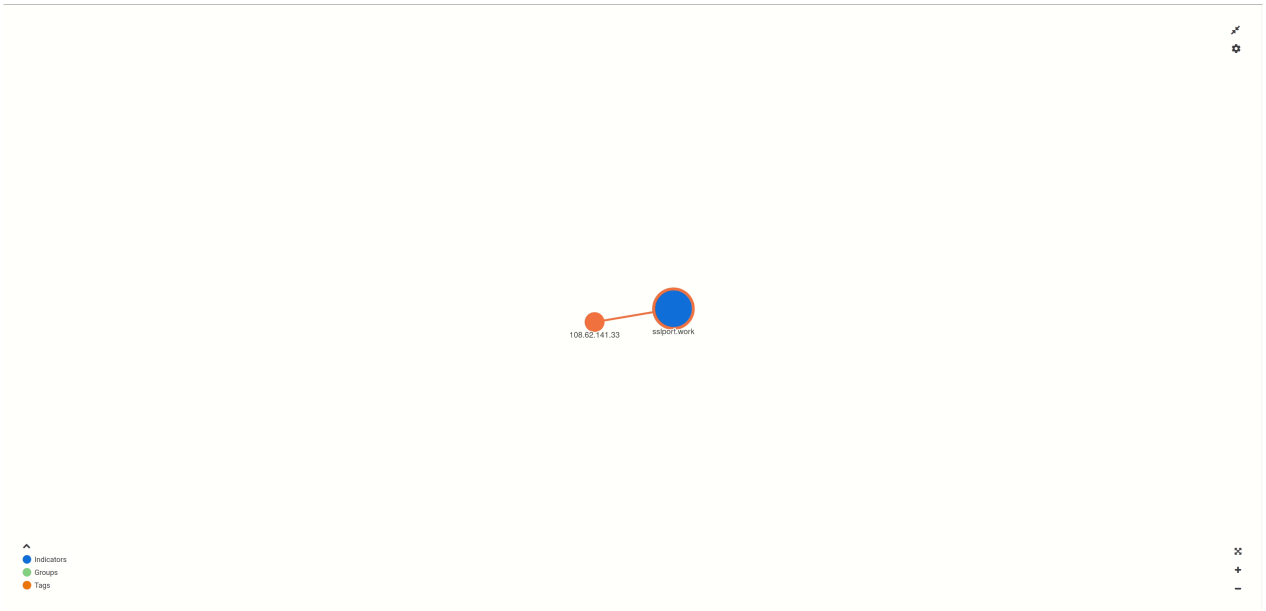


Figure 3: sslport[.]work to IP to Domains to IP to Domains

IP: 108.62.141.33

- com-download[.]work
- com-option[.]work
- com-sslnet[.]work
- com-ssl[.]work
- com-vps[.]work
- desk-top[.]work

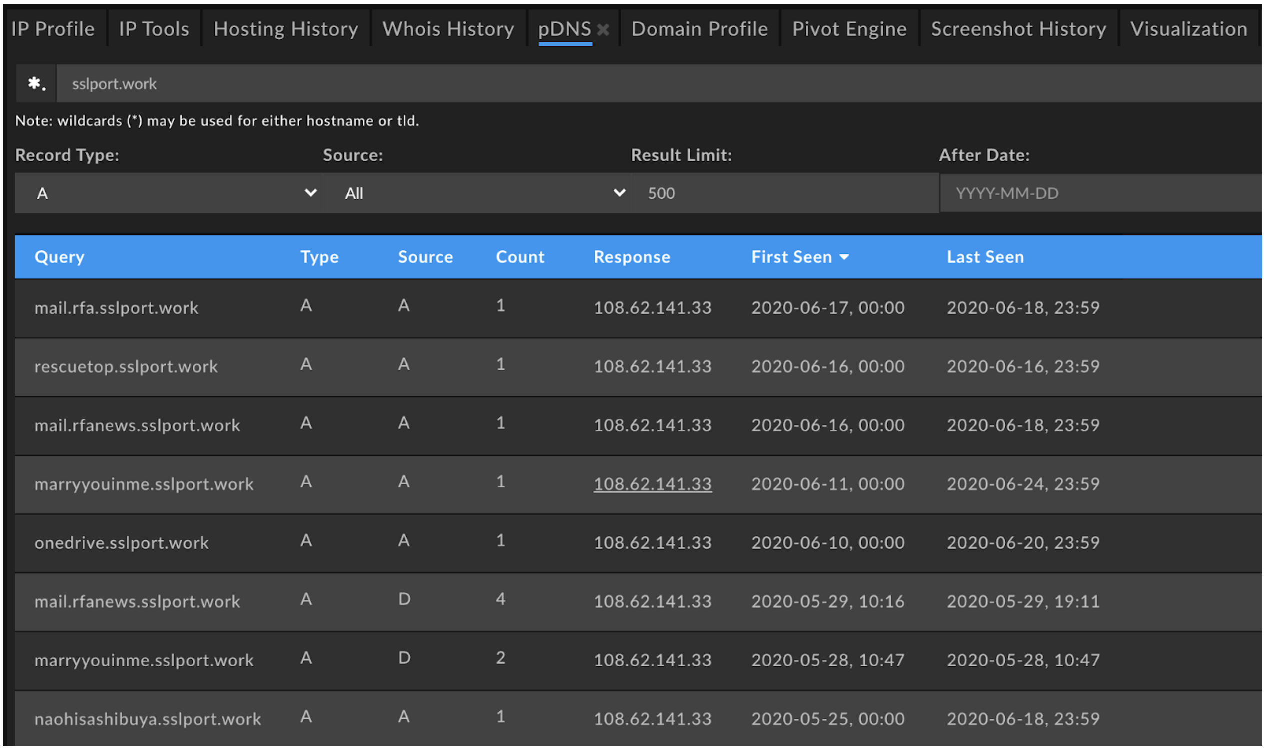
- intemet[.]work
- jp-ssl[.]work
- org-vip[.]work
- sslport[.]work
- sslserver[.]work
- ssltop[.]work
- taplist[.]work
- vpstop[.]work
- webmain[.]work

The domain com-download[.]work stands out as it was referenced in an article linked from the ESTSecurity article above. The article describes a phishing attempt against the Korean Studies Institute at George Washington University.

Next, let’s look into subdomains used.

Enumerating Subdomains

Focusing on sslport[.]work again, we see some interesting subdomains under the pDNS tab in DomainTools Iris:



*. sslport.work

Note: wildcards (*) may be used for either hostname or tld.

Record Type: A

Source: All

Result Limit: 500

After Date: YYYY-MM-DD

Query	Type	Source	Count	Response	First Seen	Last Seen
mail.rfa.sslport.work	A	A	1	108.62.141.33	2020-06-17, 00:00	2020-06-18, 23:59
rescuetop.sslport.work	A	A	1	108.62.141.33	2020-06-16, 00:00	2020-06-16, 23:59
mail.rfanews.sslport.work	A	A	1	108.62.141.33	2020-06-16, 00:00	2020-06-18, 23:59
marryyouinme.sslport.work	A	A	1	108.62.141.33	2020-06-11, 00:00	2020-06-24, 23:59
onedrive.sslport.work	A	A	1	108.62.141.33	2020-06-10, 00:00	2020-06-20, 23:59
mail.rfanews.sslport.work	A	D	4	108.62.141.33	2020-05-29, 10:16	2020-05-29, 19:11
marryyouinme.sslport.work	A	D	2	108.62.141.33	2020-05-28, 10:47	2020-05-28, 10:47
naohisashibuya.sslport.work	A	A	1	108.62.141.33	2020-05-25, 00:00	2020-06-18, 23:59

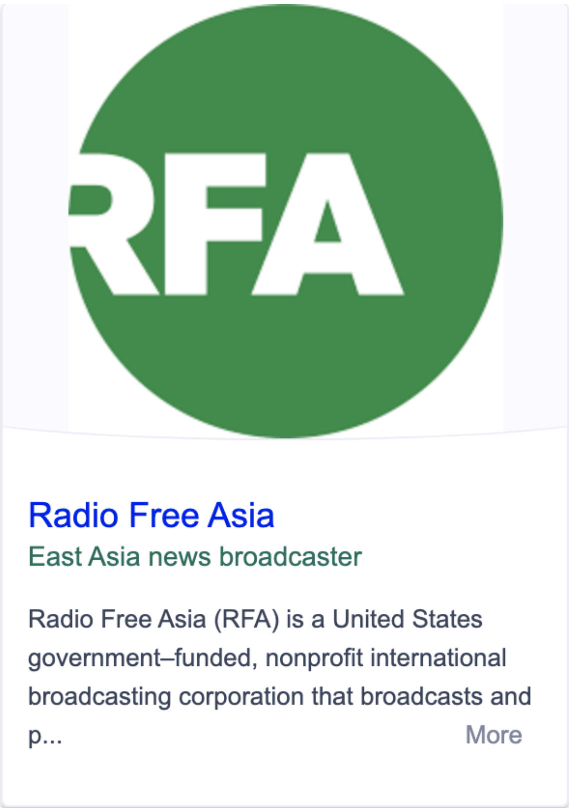
Figure 4: sslport[.]work pDNS

These two entries:

- mail.rfanews.sslport[.]work
- mail.rfa.sslport[.]work

lead to a potential target — Radio Free Asia, a broadcast organization that consistently reports on North Korea. The usage of RFA in the subdomain is suspicious but we can't say for certain they were a target as their likeness may have been used in attacks against other organizations.

Pulling on another thread from the same IP, we find another potential target. These three entries appear when looking at the pDNS data in DomainTools for the IP 108.62.141[.]33.

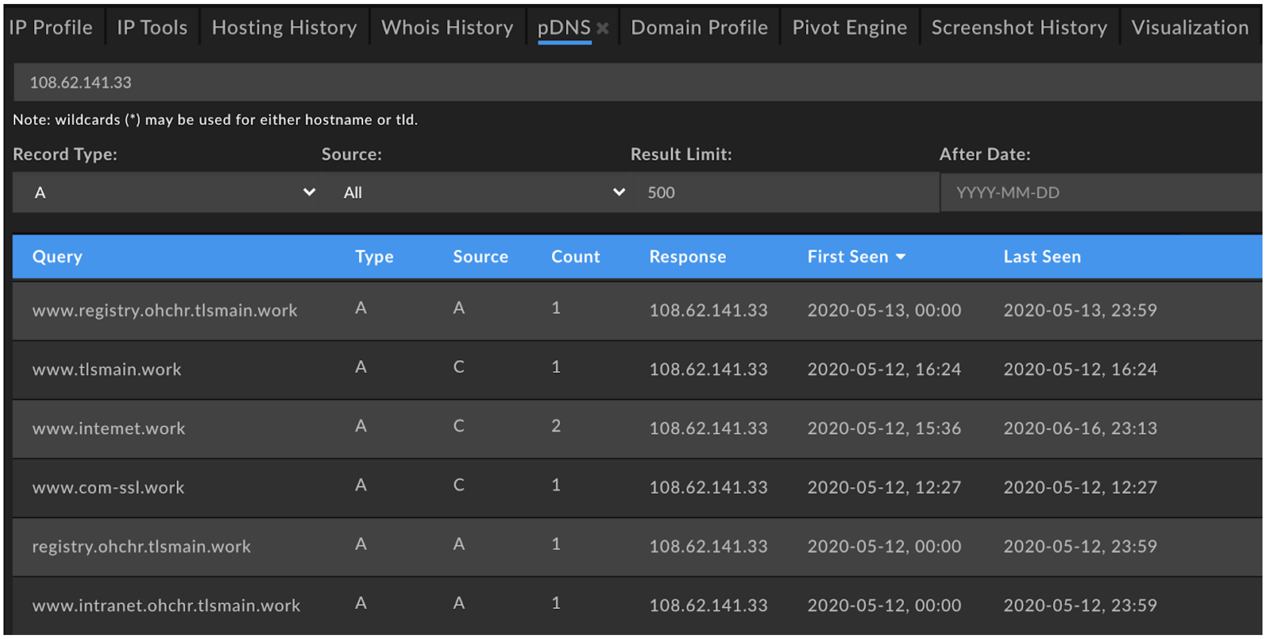


Radio Free Asia

East Asia news broadcaster

Radio Free Asia (RFA) is a United States government–funded, nonprofit international broadcasting corporation that broadcasts and p... More

Figure 5: Radio Free Asia



108.62.141.33

Note: wildcards (*) may be used for either hostname or tld.

Record Type: A
Source: All
Result Limit: 500
After Date: YYYY-MM-DD

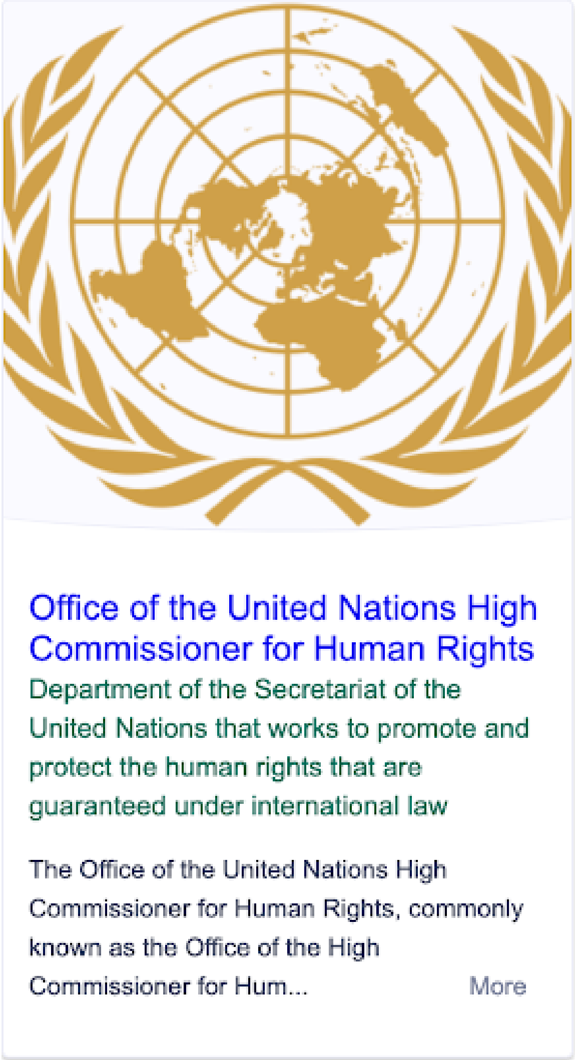
Query	Type	Source	Count	Response	First Seen	Last Seen
www.registry.ohchr.tlsmain.work	A	A	1	108.62.141.33	2020-05-13, 00:00	2020-05-13, 23:59
www.tlsmain.work	A	C	1	108.62.141.33	2020-05-12, 16:24	2020-05-12, 16:24
www.intemet.work	A	C	2	108.62.141.33	2020-05-12, 15:36	2020-06-16, 23:13
www.com-ssl.work	A	C	1	108.62.141.33	2020-05-12, 12:27	2020-05-12, 12:27
registry.ohchr.tlsmain.work	A	A	1	108.62.141.33	2020-05-12, 00:00	2020-05-12, 23:59
www.intranet.ohchr.tlsmain.work	A	A	1	108.62.141.33	2020-05-12, 00:00	2020-05-12, 23:59

Figure 6: 108.62.141[.]33 pDNS

- registry.ohchr.tlsmain[.]work
- www[.]registry[.]ohchr[.]tlsmain[.]work
- www[.]intranet[.]ohchr[.]tlsmain[.]work

Immediately ohchr jumps out as it may spoof the "Office of the United Nations High Commissioner for Human Rights".

But wait! The trail does not stop here.

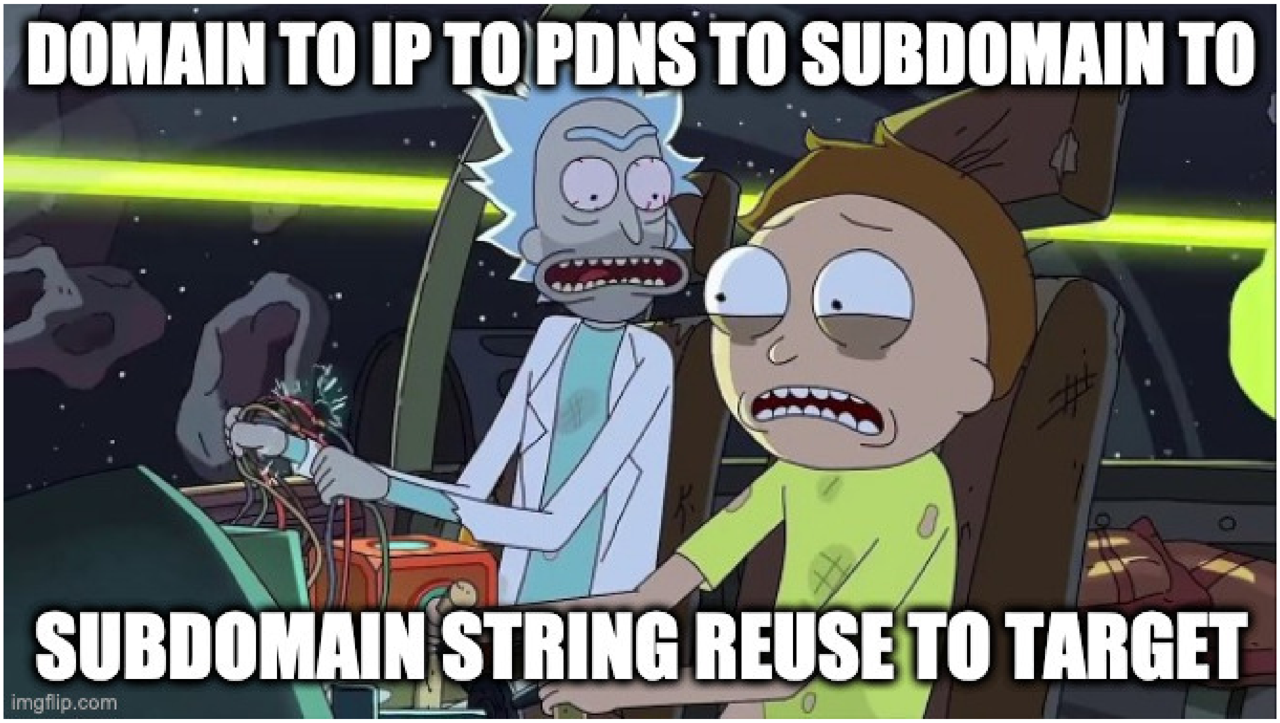


Office of the United Nations High Commissioner for Human Rights

Department of the Secretariat of the United Nations that works to promote and protect the human rights that are guaranteed under international law

The Office of the United Nations High Commissioner for Human Rights, commonly known as the Office of the High Commissioner for Hum...

Figure 7: OHCHR


DOMAIN TO IP TO PDNS TO SUBDOMAIN TO
SUBDOMAIN STRING REUSE TO TARGET
imgflip.com

Subdomain String Pivot

Pivoting off of the subdomain string intranet.ohchr.* using DomainTools Iris we identify additional, most likely related, domains.

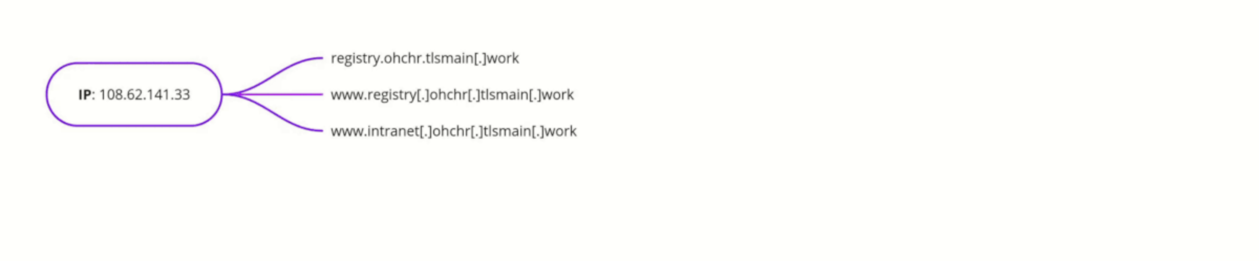

IP: 108.62.141.33
registry.ohchr.tlsmain[.]work
www.registry[.]ohchr[.]tlsmain[.]work
www.intranet[.]ohchr[.]tlsmain[.]work

Figure 8: Subdomain String Pivot

In particular these three domains appear to be related:

- intranet.ohchr.account-protect[.]work
- intranet.ohchr.org-view[.]work
- intranet.ohchr.org-view[.]pw

Upon inspecting org-view[.]work further we find:

- amaniafrica-et.org-view[.]work
- doc-view.docomo.ne.org-view[.]work
- intranet.ohchr.org-view[.]work
- login-yahoo.org-view[.]work
- login.aei.org-view[.]work
- login.gordonchang.org-view[.]work
- login.microsoftonline.org-view[.]work
- login.un.org-view[.]work
- login.yahoo.co.jp.org-view[.]work
- login.yahoo.com-service.org-view[.]work
- offerhubs.org-view[.]work
- ohchr.org-view[.]work
- preview.manage.org-view[.]work
- spurgentaction.in.ohchr.org-view[.]work
- www.intranet.ohchr.org-view[.]work
- webmail.org-view[.]work

Additional potential targets can be gleaned from this list. At a high level these targets are civil society organizations.

First, the subdomain amaniafrica-et appears to be masquerading as amaniafrica-et.org.

In addition to being a civil society organization, interest in this organization could be due to commercial ties North Korea has had with different African nations over the years, according to the Washington Post.

The next one on the list that jumps out is the American Enterprise Institute (AEI). According to their website, AEI focuses on defending human dignity.

Figure 9: Amani Africa Logo from their website

Figure 10: AEI from their site

Connecting the Dots

Connecting the indicators with the potential targets graphically, we see a fair number of resources targeting OHCHR.

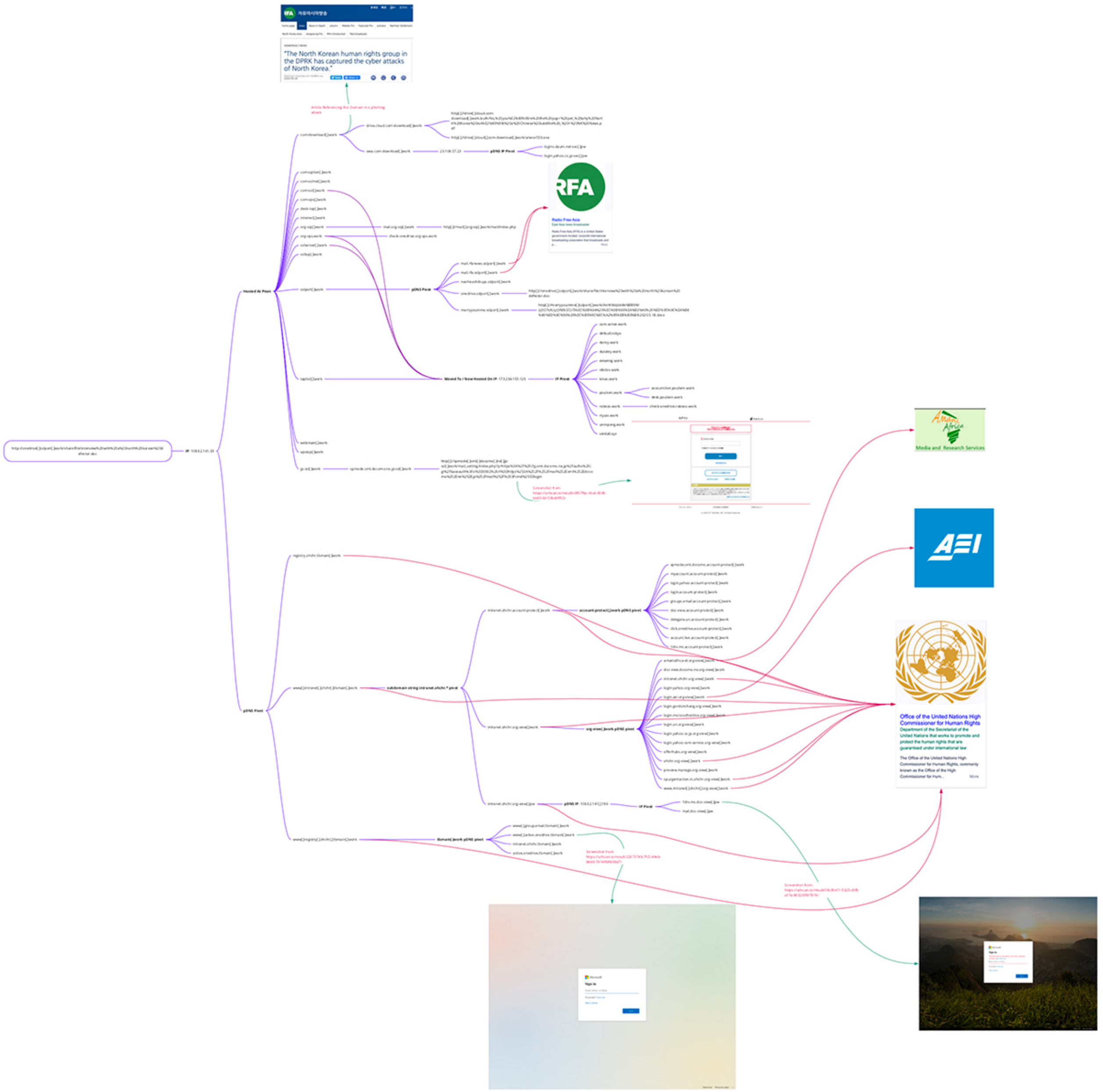

"The North Korean human rights group in the DPRK has captured the cyber attacks of North Korea."
Article Referencing this Domain in a phishing attack
Hosted At Pivot
pDNS Pivot
pDNS IP Pivot
IP Pivot
Moved To / Now Hosted On IP
RFA
Radio Free Asia
East Asia news broadcaster
Screenshot from
Amani Africa Media and Research Services
AEI
Office of the United Nations High Commissioner for Human Rights
Microsoft
Sign in

Figure 11: Adventure Graph (click to enlarge)

Timeline

Taking just the domains and subdomains in this article and mapping it to a timeline, we can see the continuous efforts Kimsuky is going through to gather credentials. The activity covered here, according to DomainTool's Iris, goes back as far as December of 2019 and is as recent as August of this year.

Potential Targets Uncovered

Based on the identified subdomains, the following organizations are possible targets of this campaign, or their likeness was spoofed in targeting other organizations:

- Amani Africa

- Radio Free Asia
- American Enterprise Institute
- Office of the United Nations High Commissioner for Human Rights

In addition to these, Korean Studies Institute at George Washington University didn't have a subdomain that was indicative of them being targeted; however, they were still found via infrastructure pivoting along with a public report of them being targeted. For the rest, we acknowledge that the subdomains used could be indicative of the target; they could also be used to go after third parties that might trust those organizations.

Conclusion

ThreatConnect believes that Kimsuky will continue to target journalism and civil society organizations, particularly those focusing on North Korean issues. Organizations reporting on North Korea human rights violations or working with North Korean defectors need to remain especially vigilant of phishing attacks that take advantage of the information sharing culture they are part of. Be wary of any link and/or attachment, especially those asking for credentials, and enable two factor authentication to mitigate actors' access with compromised credentials.

Appendix

- ThreatConnect Incident
- IoC CSV