Identifying Critical Infrastructure Targeting through Network Creation

domaintools.com/resources/blog/identifying-critical-infrastructure-targeting-through-network-creation

DOMAINTOOLS®
Identifying Critical Infrastructure Targeting through Network Creation

Background

In addition to independent investigations, DomainTools closely tracks the work of other respected researchers to see what we might miss in our own efforts. Recently, we learned of possible new infrastructure related to the threat actor known as OilRig (aka, APT34 or Helix Kitten). In these situations, DomainTools works to understand the background for such infrastructure and any tendencies which may be revealed by their creation in order to learn how given adversaries operate.

Aside from learning about adversaries, such efforts may also yield new, independent results through further research and analysis. In this case, a preliminary search of DomainTools data yielded a number of interesting, related results to the initial domain:

Domain	Create Date	Email	I
7hillsgastro[.]com	2020-10-19	aerialthomas101@yandex.com	1

ababab[.]biz	2020-10-02	diandianlai@yandex.com	1
alcirineos[.]com	2020-10-05	user2020-clon@yandex.com	N
amazon-loveyou[.]com	2020-11-12	lzr0709000@yandex.com	1
bargertextiles[.]com	2020-10-27	chr1styjoe@yandex.com	1
berqertextiles[.]com	2020-10-27	chr1styjoe@yandex.com	1
careers-ntiva[.]com	2020-11-25	N/A	1
cererock[.]com	2020-11-02	chr1styjoe@yandex.com	1
chinaconstructioncorp[.]com	2020-11-15	cjay006@yandex.com	7
clearinghouseinternational[.]com	2020-10-17	ibm.partners@yandex.com	5
connect-roofing[.]com	2020-11-25	N/A	N
exmngt[.]com	2020-11-18	cjay006@yandex.com	1
hoganlouells[.]com	2020-11-16	mitchd2@yandex.com	1
hscminkjet[.]com	2020-10-27	chr1styjoe@yandex.com	1
huopay[.]top	2020-10-11	diandianlai@yandex.com	1
indeptheva[.]com	2020-10-05	evaluationfront@yandex.com	1
jiabolianjie0[.]com	2020-10-01	lzr070900@yandex.com	1
jinkangpu[.]co	2020-11-04	user2020-clon@yandex.com	N

jlrootfile[.]com	2020-10-20	chr1styjoe@yandex.com	1
kent-lawfirm[.]net	2020-11-12	N/A	1
klwebsrv[.]com	2020-11-26	N/A	N
oculus-au[.]info	2020-11-18	lovelead247@yandex.com	N
pet188[.]biz	2020-10-16	chr1styjoe@yandex.com	1
petrochinas[.]com	2020-11-15	cjay006@yandex.com	7
renrenbaowang[.]com	2020-10-28	diandianlai@yandex.com	1
renrenbaowang[.]net	2020-10-28	diandianlai@yandex.com	1
superrnax[.]com	2020-10-15	phillip.char@yandex.com	1
svn-stone[.]com	2020-10-23	zhovr04@yandex.com	N
us-customs[.]org	2020-10-28	domain45@yandex.com	6
virtual-slots[.]com	2020-10-23	giadafallaci@yandex.com	2
virtualcaresadvisor[.]com	2020-10-02	hostmaster@virtualcaresadvisor.com	2
wilsonconts[.]com	2020-11-09	user2020-clon@yandex.com	N
wiqzi[.]com	2020-10-24	chr1styjoe@yandex.com	1
zj-tunq[.]com	2020-11-18	lovelead247@yandex.com	N

Several items stood out in the above list of related infrastructure, notably related to common email addresses linked to registrations:

- cjay006[AT]yandex[.]com
- ch1styjoe[AT]yandex[.]com
- diandianlai[AT]yandex[.]com
- lovelead247[AT]yandex[.]com

Using DomainTools Iris, each of these observed email addresses become a launchpad for investigating additional, related infrastructure. Although at this point connections appear too weak to definitively tie activity back to OilRig behaviors, which is where this investigation began, we have nonetheless reached an interesting and potentially useful intermediate conclusion by identifying linked, suspicious network infrastructure.

Identifying Network Infrastructure

Most notable among the common items above are those linked to the "cjay006" address:

Domain	Email	IP Address	Mail Ex
anhuisiafu[.]com	**cjay006@yandex.com**	**N/A**	**mailho**
boardexecutivemanagement[.]com	**cjay006@yandex.com**	**N/A**	**mailho**
boardsexecutives[.]com	**cjay006@yandex.com**	**198.54.117.197**	**mailho**
chinaconstructioncorp[.]com	**cjay006@yandex.com**	**77.55.219.100**	**chinac**
cornerstoneconect[.]com	**cjay006@yandex.com**	**77.55.217.184**	**corners**
exmngt[.]com	**cjay006@yandex.com**	**198.54.117.197**	**mailho**
groupsexecutive[.]com	**cjay006@yandex.com**	**46.28.109.165**	**groups**
lavalingroup[.]com	**cjay006@yandex.com**	**77.55.233.217**	**lavalin**
mngtboard[.]com	**cjay006@yandex.com**	**46.28.109.164**	**mailho**
petrochinas[.]com	**cjay006@yandex.com**	**77.55.216.70**	**petrocl**
stagmein[.]pl	**cjay006@yandex.com**	**N/A**	**N/A**

Several themes emerge in the above list, looking at the actual names used for domain creation:

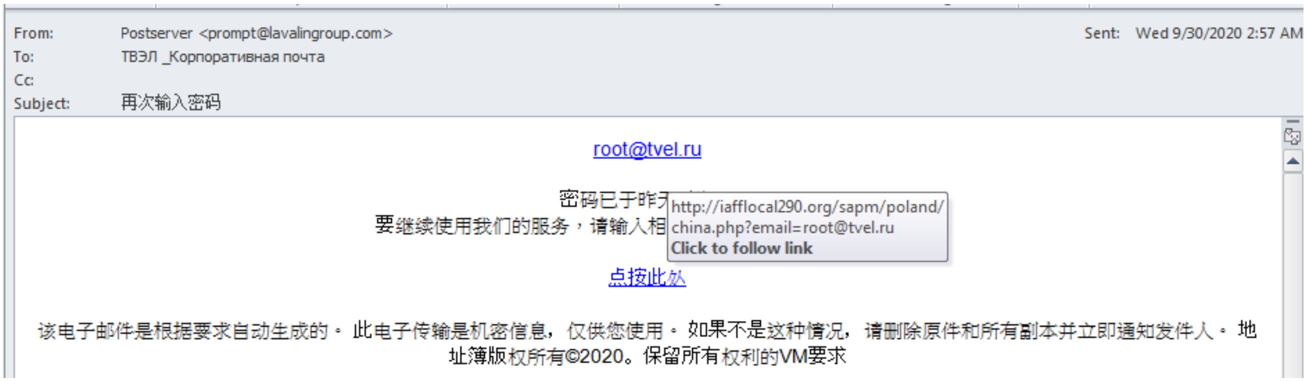
- Mimicking corporate or executive themes (e.g., "boardsexecutives," "mngtboard").

- Themes linked to the People's Republic of China (PRC) (e.g., "chinaconstructioncorp," "petrochinas," "anhuisiafu").
- Construction or engineering company spoofing (in addition to "chinaconstructioncorp," "lavalingroup" is similar to Canadian engineering company SNC-Lavalin).

Hosting patterns aside, reviewing registration and DNS data showed that some domains featured interesting Mail Exchange (MX) records referring back to the original domain. As described in previous DomainTools blogs, identifying certain hosting and functional characteristics to infrastructure can yield insights into adversary activity. In this case, the presence of the MX records, especially for items such as the construction-themed domains, may indicate use for phishing purposes.

Unearthing a Phishing Campaign

Researching several malware repositories, DomainTools researchers uncovered multiple emails sent from the infrastructure described in the previous section. Reviewed messages are similar to the following item:



From: Postserver <prompt@lavalingroup.com>
To: ТВЭЛ _Корпоративная почта
Cc:
Subject: 再次输入密码

Sent: Wed 9/30/2020 2:57 AM

root@tvel.ru

密码已于昨天

要继续使用我们的服务，请输入相

http://iafflocal290.org/sapm/poland/china.php?email=root@tvel.ru
Click to follow link

点按此处

该电子邮件是根据要求自动生成的。此电子传输是机密信息，仅供您使用。如果不是这种情况，请删除原件和所有副本并立即通知发件人。地址簿版权所有©2020。保留所有权利的VM要求

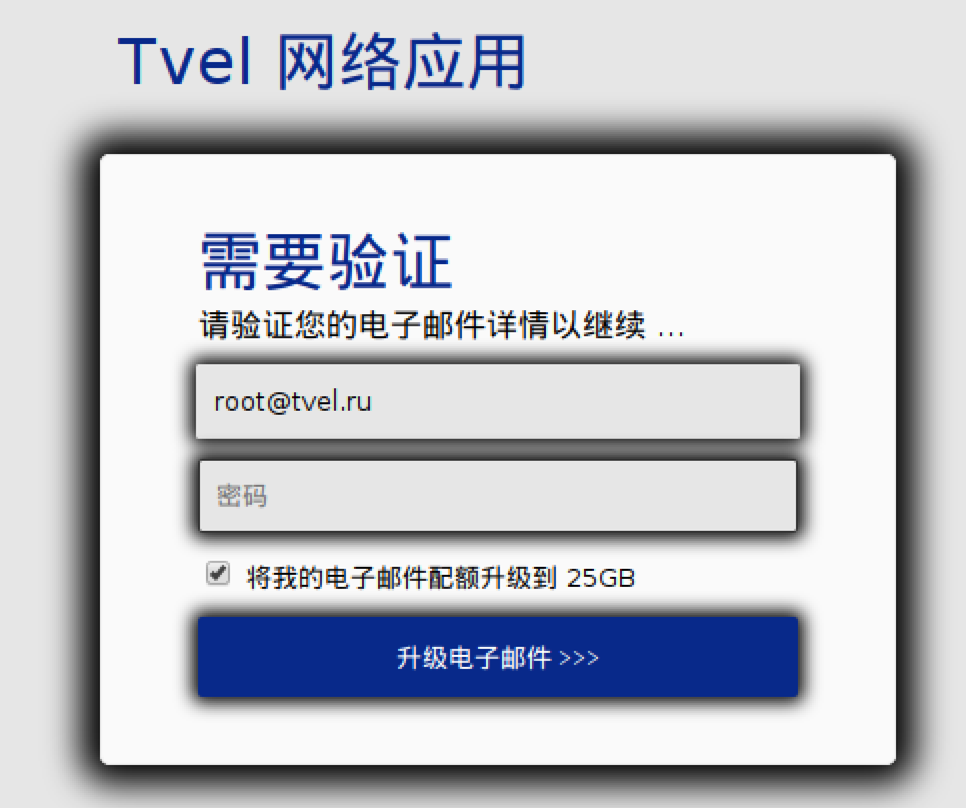
Email messages had the following purpose and themes:

- Addressed to either the Russian state nuclear energy firm ROSATOM or its nuclear fuel production subsidiary TVEL.
- Written in Chinese with a "password reset" theme.
- Sent from the SNC-Lavalin spoofing domain.

Furthermore, all samples identified by DomainTools contained a link to a common resource:

```
hXXp://iafflocal290[.]org/sapm/Poland/china[.]php
```

The page presents a logon screen:



Tvel 网络应用

需要验证

请验证您的电子邮件详情以继续 ...

root@tvel.ru

密码

☑ 将我的电子邮件配额升级到 25GB

The page appears to be a straightforward credential harvester, submitting credentials entered into the form fields as a POST to the same hosting domain. The domain itself appears to be either an abandoned or compromised legitimate website associated with a local fire department in the United States.

Further research identified the above as a common spoofed logon page for likely credential harvesting purposes. Among other entities identified, DomainTools researchers uncovered pages targeting:

- A major automobile manufacturer.
- A major automotive parts supplier.
- An Internet-of-Things (IoT) technology company.

Purpose and Context

The activity above is interesting on several levels. While Canadian-based SNC-Lavalin has operations worldwide, including in the nuclear industry, the company has no known links to Rosatom, TVEL, or Chinese nuclear projects. However, Rosatom and TVEL have significant operations involving Chinese reactor construction and development. Based on these links, DomainTools assesses some possibility for phishing themes combining Russian nuclear organizations with Chinese construction and critical infrastructure entities against individuals working on such projects.

Yet the samples in question all leverage the Lavalin theme, which does not align with any known projects or activity. The combination of Canadian engineering company spoofing, Russian nuclear technology targeting, and Chinese language phishing messages is therefore somewhat confusing.

Further research identified the credential harvesting pages associated with other entities, largely with technology or manufacturing themes. Based on this information, a likely intention for the Lavalin-ROSATOM campaign would appear to be credential harvesting to further follow-on espionage and data theft. Unfortunately, insufficient evidence exists to definitively support this claim.

While this investigation began by pivoting off of infrastructure linked to OilRig— associated with Iranian interests by multiple entities—there is nothing conclusive linking the identified phishing activity to behaviors associated with Iranian threat groups. This is especially the case after uncovering the additional, similarly-structured logon pages targeting other industries. At this time DomainTools cannot align the observed phishing activity with any known, tracked threat actor.

Conclusion

Threat hunters and researchers need to incorporate third-party findings and investigations into their own work to expand horizons and ingest new observations for subsequent enrichment. By expanding upon identified work and threat indicators, researchers can unearth related or potentially even completely separate campaigns that happen to overlap in certain characteristics.

Such is the case with the above investigation, where initial analysis of likely OilRig-related observables revealed a phishing campaign targeting the Russian nuclear industry with Chinese language characteristics, as well as several other manufacturing and technology companies. While much remains unknown about this newly identified campaign, we as threat researchers now have awareness of and insight into the activity that was previously unknown based on dogged analysis and enrichment of third-party research.