CREDENTIALS GATHERING CAMPAIGN

LARGE CLUSTERS OF MALICIOUS INFRASTRUCTURE TARGETING GOVERNMENT BODIES AND OTHER STRATEGIC ENTITIES

Version 1.0

2019-09-02

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

Sommaire

1 Introduction

During its investigations and with the cooperation of multiple partners, ANSSI has discovered several clusters of malicious activity, including domain names, subdomains and email addresses, used in a large attack campaign with traces going back to 2017. The threat actor registered multiple domain names, and created several subdomains with a naming pattern revealing its potential targets. The main purpose of these activities seems to be credentials gathering, thanks to spearphishing emails and phishing websites.

The range of supposed targets is wide, including country officials and think tanks. Five possibly targeted diplomatic entities belong to member countries of the United Nations Security Council (China, France, Belgium, Peru, South Africa).

Attribution of a cyber attack to a threat actor is a complex exercice and is not the goal of this document nor ANSSI's mission. This document only underlines the technical links found during ANSSI's investigations between some infrastructure used during these attacks and technical elements reported in open-sources as being used by the following threat actors : Kimsuky and Group123.

During the course of this analysis, the cybersecurity company ANOMALI released a publicly available report regarding the same activities [1].

This report provides the infrastructure clusters identified and some of the potential targets. Indicators of compromise may be found in the attached CSV file.

2 Recommendations

In order to prevent this kind of attacks, ANSSI recommends setting up two-factor authentication for email accounts and website authentication. Also, users are requested to be particularly wary of emails inviting them to authenticate to a website.

3 Summary

Several malicious subdomains discovered seem to spoof email or cloud service providers, but a few of them appear to target specific organizations. The table below provides the identity of these possible targets, according to the subdomain names used.

Targeted organization	Subdomains(s)
French ministry of foreign affairs	portalis.diplomatie.gouv.web-line.work portalis.diplomatie.gouv.doc-view.work
Congressional Research Service of the United States Congress	crsreports.congress.doc-view.work
Unknown ministry of foreign affairs	mail.mofa.gov.web-line.work mail.mofa.gov.doc-view.work
United Nations	delegate.int.doc-view.work
South African ministry of foreign affairs	ubmail.dirco.gov.doc-view.work ubmail.dirco.gov.web-line.work
Slovak ministry of foreign affairs	www.mzv.sk.doc-view.work
Royal United Services Institute	rusi.org.doc-view.work
FPS Chancellery of the Prime Minister	mail.fed.be.web-line.work
Asan Institute for Policy Studies	asaninst.accountss.work asaninst.info-setting.work asaninst.main-line.site asaninst.service-info.work
Permanent Mission of Peru to the United Nations	mail.unperu.yalnoo.com
POLITICO Europe	politico.eu.mai1.info
American Entreprise Institute	mail.aei.org.smail-live.work
Sumitomo Mitsui Banking Corporation	srnbc-card.com
South Korea ministry of foreign affairs and trade	mofa.go.kr.sub-state.work mail.mofa.go.kr.sub-state.work
Stanford University	securemail.stanford.doc-view.work

Moreover, some subdomain names show that members of specfic countries could be targeted.

Country	Subdomains(s)
Russia	www.mail.yandex.ru.classic.sdfwseferf34fds.mai1.info
China	login-history.vip-sina.com.smail-live.work
Japan	All subdomains matching ”edit-accounts.ntt-ocn.*”
South Korea	All subdomains matching ”*.naver.mai1.info” il.daumcdn.net.mailacounts.com / members.dauurn.net
Poland	poczta.hotrnall.com

Some of the email addresses found in the domains' *WhoIs* information have usurped Chinese VIP usernames, which could also be used as sender addresses in spearphishing emails.

Chinese VIP	Email address
Mr. Sun Lei. Counsellor, Non-Proliferation. Permanent mission of the people's republic of China to the United Nations	2014sunlei@india.com
Mr. Guanghui Tang. Second Secretary. Embassy of the People's Republic of China in the United States	tang_guanghui@hotmail.com
Mr Zong Jiahu. Official, National Authority. China national CWC Implementation Office	zongjiahu@yahoo.com

4 Malicious infrastructure

This chapter details the infrastructure identified. Many of the subdomains have resolved IP addresses belonging to the CIDR « `157.7.184.0/24` » hosted in GMO Internet and located in Japan, and share a similar naming pattern. Domains having an additional link or sharing *WhoIs* email address are grouped in a cluster.

4.1 Cluster 1

The first cluster encompasses two email addresses that have registered 16 domains. One fake portalis website, « `portalis.diplomatie.gouv.web-line.work` » is linked with the email address « `dragon1988@india.com` », the other « `portalis.diplomatie.gouv.doc-view.work` » is linked to « `ringken1983@gmail.com` ».

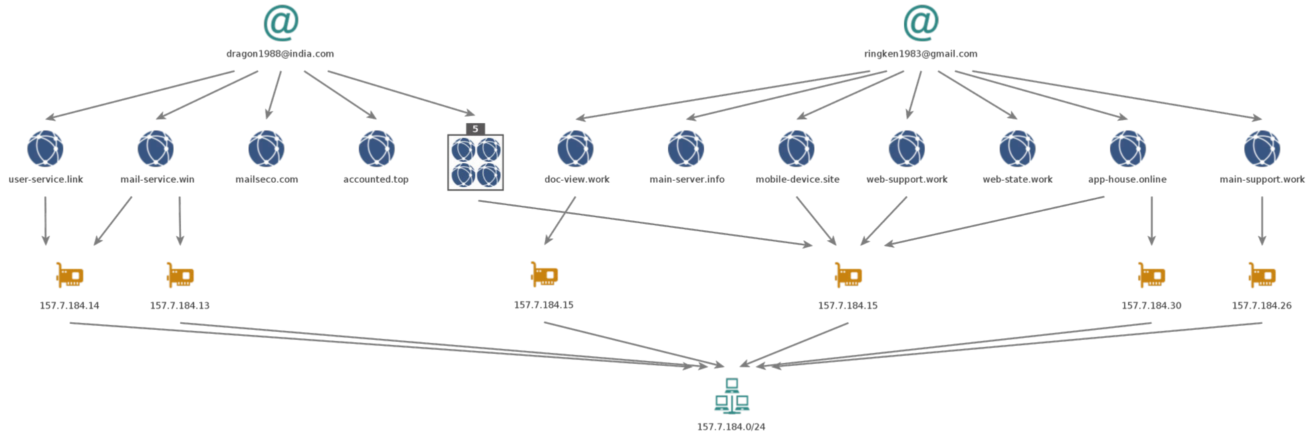

Fig. 4.1: Cluster number 1

Email addresses
ringken1983@gmail.com
dragon1988@india.com

ringken1983@gmail.com
app-house.online
doc-view.work
login-confirm.work
main-support.work
mobile-device.site
share-check.site
web-state.work

dragon1988@india.com
accounted.top
check-line.site
check-up.work
mailseco.com
mail-service.win
member-service.work
user-service.link
web-line.work
yah00.work

4.1.1 Technical links with a threat actor

A Twitter feed from a cybersecurity analyst, where the first message has been removed[1] shows that the domain name « `doc-view.work` » could be linked with the threat actor Kimsuky.

[1] https://twitter.com/blackorbird/status/1146609703494881280

4.2 Cluster 2

Three email addresses, usurping the username of chinese's VIPs, are linked with 15 domain names. Many subdomains have the same naming convention and have resolved IP addresses belonging to the CIDR « `157.7.184.0/24` ».

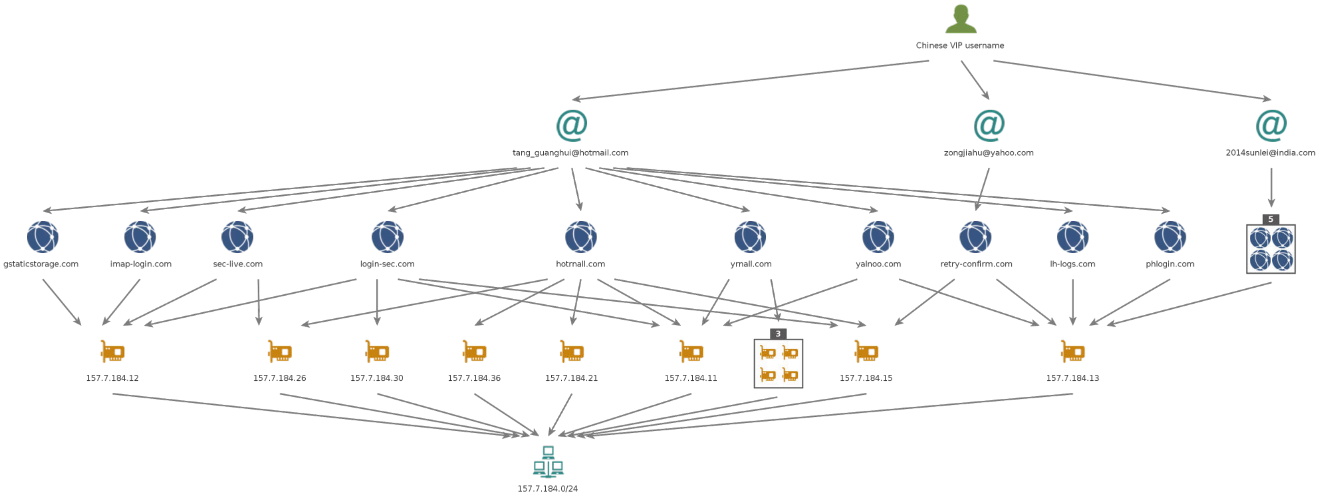

Fig. 4.2: Cluster number 2

Email addresses
2014sunlei@india.com
tang_guanghui@hotmail.com
zongjiahu@yahoo.com

« `2014sunlei@india.com` » has the same username as « `2014sunlei@gmail.com` », which is the email address of Mr. Sun Lei, a chinese United Nation's counsellor for the non proliferation of nuclear weapons, at least in July 2017 according the website « `china-un.org` »[2].

A list found in open source[3] shows that « `tang_guanghui@yahoo.com` » is the email address of Mr. Guanghui Tang, the second secretary of the embassy of the people's republic of China in the United States.

Finally, « `zongjiahu@yahoo.com` » refers to Mr. Zong Jiahu, a chinese official within the China national CWC[4] Implementation Office, according to open source data[5].

The tables below list the domain names found with these email addresses.

2014sunlei@india.com
accountss.work
check-operation.site
main-line.site
service-info.work
sign-in.work

[2] `http://www.china-un.org/eng/dbtxx/dprwueng/P020170704365690549730.doc`
[3] `https://heehorse.com/heehorse_content/scribblings/all.CSV`
[4] Chemical Weapons Convention
[5] `https://www.opcw.org/documents/untitled-document-39`

tang_guanghui@hotmail.com
gstaticstorage.com
hotrnall.com
imap-login.com
lh-logs.com
login-sec.com
phlogin.com
sec-live.com
yalnoo.com
yrnall.com

zongjiahu@yahoo.com
retry-confirm.com

4.3 Cluster 3

Five email addresses registered on « `yahoo.co.jp` » have been used to register several malicious domain names. Many subdomains have resolved IP addresses belonging to the CIDR « `157.7.184.0/24` » and follow a similar naming pattern.

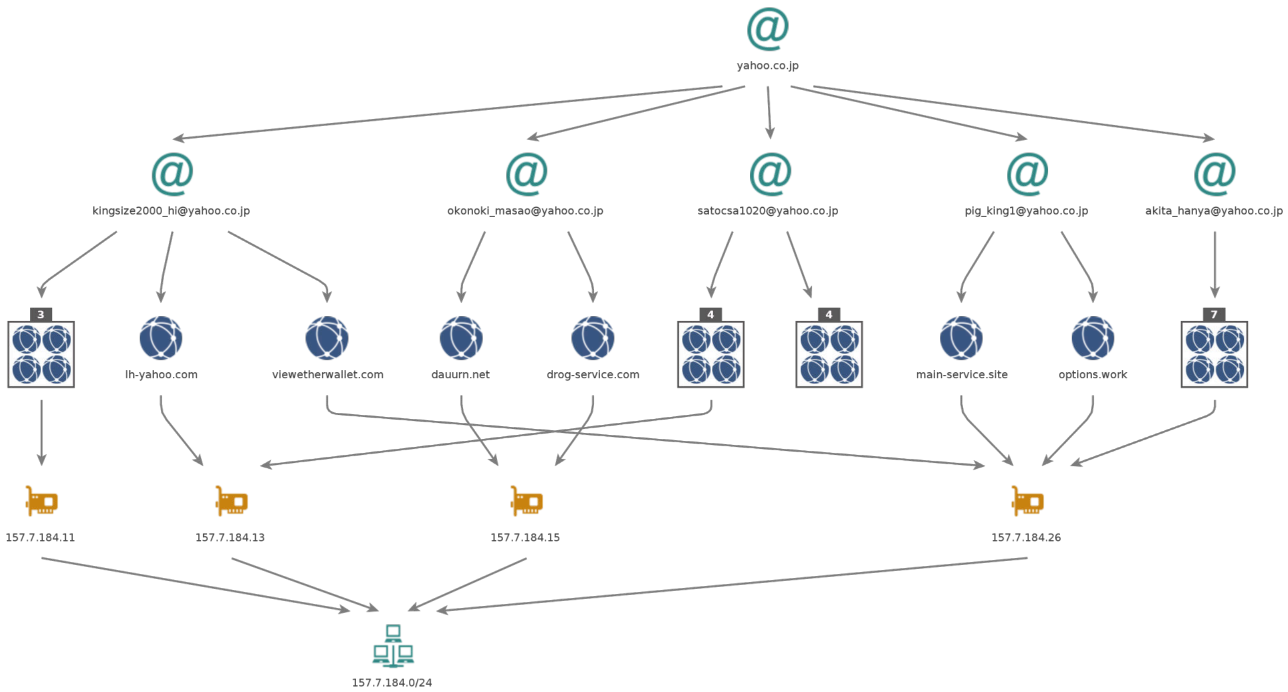

Fig. 4.3: Cluster number 3

Email addresses
akita_hanya@yahoo.co.jp
kingsize2000_hi@yahoo.co.jp
okonoki_masao@yahoo.co.jp
pig_king1@yahoo.co.jp
satocsa1020@yahoo.co.jp

akita_hanya@yahoo.co.jp
first-state.work
main-line.work
net-policies.work
online-support.work
protect-com.work
web-info.work
web-online.work

kingsize2000_hi@yahoo.co.jp
lh-login.com
lh-yahoo.com
log-yahoo.com
logins-yahoo.com
viewetherwallet.com

okonoki_masao@yahoo.co.jp
dauurn.net
drog-service.com

pig_king1@yahoo.co.jp
main-service.site
options.work

satocsa1020@yahoo.co.jp
acounts.work
eposcard.co
mailacounts.com
myprivacy.work
srnbc-card.com
user-account.link
user-accounts.net
user-service.work

4.3.1 Technical links with a threat actor

A report from Talos [2] mentionned the domain name « `mailacounts.com` », found in a compilation path of a NavRAT sample. Talos assesses with medium confidence that the campaign they observed and NavRAT are linked to Group123.

4.4 Cluster 4

Another email address has been identified, with 4 domains linked. Many subdomains have the same naming pattern and have resolved IP addresses belonging to the CIDR « `157.7.184.0/24` »

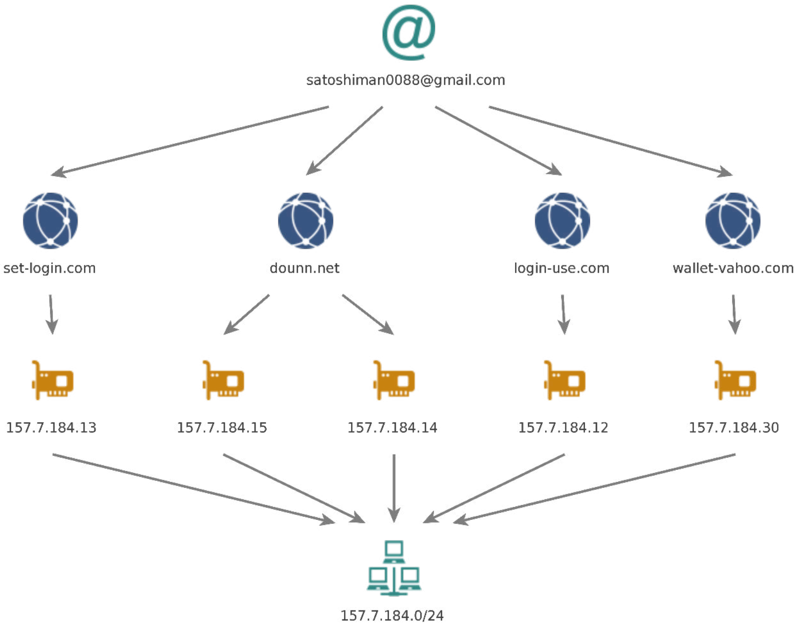

Fig. 4.4: Cluster number 4

Email address
satoshiman0088@gmail.com

satoshiman0088@gmail.com
dounn.net
login-use.com
set-login.com
wallet-vahoo.com

4.5 Cluster 5

A final email address has been identified with 5 associated domains. Many subdomains follow the same naming convention and have resolved IP addresses belonging to the CIDR « `157.7.184.0/24` ».

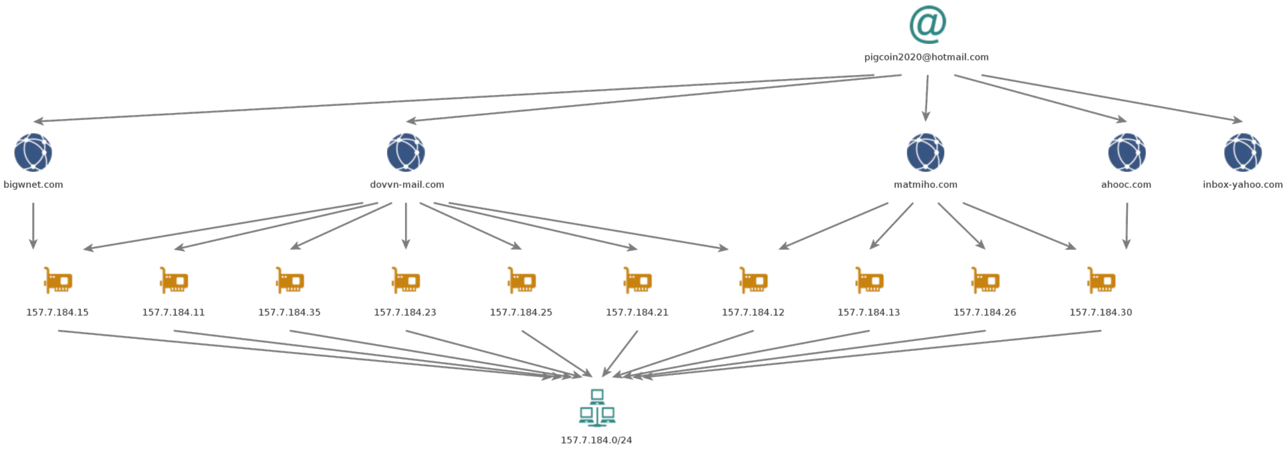

Fig. 4.5: Cluster number 5

Email address
pigcoin2020@hotmail.com

pigcoin2020@hotmail.com
ahooc.com
bigwnet.com
dovvn-mail.com
inbox-yahoo.com
matmiho.com

4.5.1 Technical links with a threat actor

These domain names as well as the email address are present in an Alien Vault community feed[6] intitled *New BabyShark Malware Targets U.S. National Security Think Tanks* and sourced by a Palo Alto Networks' report [3]. This campaign is associated with the threat actor Kimsuky.

The domain name «`login-main.bigwnet.com`» is a C2 server for a malicious document intitled «`Speaking notes-ExMon Deterrence Summit-24-Mar-rev-26-Mar19.doc`». This annual summit, about nuclear deterrence, took place in february 2019.

Hashes	Creation time	File type
7ca1a603a7440f1031c666afbe44afc8 e12d0655cc09cddb4fb836c641f73179d4bc1121 9c6f6db86b5ccdda884369c9c52dd8568733e126e6fe9c2350707bb6d59744a1	2018-11-25 23:57:00	Office Open XML document

This document is also linked with the threat actor Kimsuky, according to a report from ESTsecurity [4].

4.6 Other similar domain names

Other domain names where subdomains have resolved IP addresses belonging to the CIDR «`157.7.184.0/24`» and which follow a similar naming pattern have been found.

Domains
alive-user.work
alone-service.work

[6] https://otx.alienvault.com/pulse/5c70388b371f594e27973c86

app-house.online
app-main.site
app-support.site
app-support.work
client-mobile.work
com-main.work
confirm-main.work
hotrnall.co
inbox-mail.work
info-setting.work
local-link.work
login-confirm.site
login-history.pw
login-yahoo.info
mai1.info
mail-down.com
mail-inc.work
message-inbox.work
minner.work
mobile-phone.work
old-version.work
open-auth.work
page-view.work
profile-setting.work
protect-mail.work
protect-main.site
script-main.site
sec-line.work
setting-main.work
share-check.site
short-line.work
smail-live.work
sub-state.work
weak-online.work
web-mind.work
web-rain.work
web-store.work

5 Sources

[1] 2019-08-22, *Suspected North Korean Cyber Espionage Campaign Targets Multiple Foreign Ministries and Think Tanks*, ANOMALI,
`https://www.anomali.com/blog/suspected-north-korean-cyber-espionage-campaign-targets`

[2] 2018-05-31, *NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea*, TALOS,
`https://blog.talosintelligence.com/2018/05/navrat.html`

[3] 2019-02-22, *New BabyShark Malware Targets U.S. National Security Think Tanks*, PALO ALTO NETWORKS,
`https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security`

[4] 2019-04-17, *Kimsuky's APT Campaign 'Smoke Screen' Revealed for Korea and US*, ESTSECURITY,
`https://blog.alyac.co.kr/2243`