Cyber Threat Operations

Tactical Intelligence Bulletin

Sofacy Phishing

Date: 2014-10-22

Contact: threatintelligence@uk.pwc.com

Reference: CTO-TIB-20141022-01C
TLP: WHITE

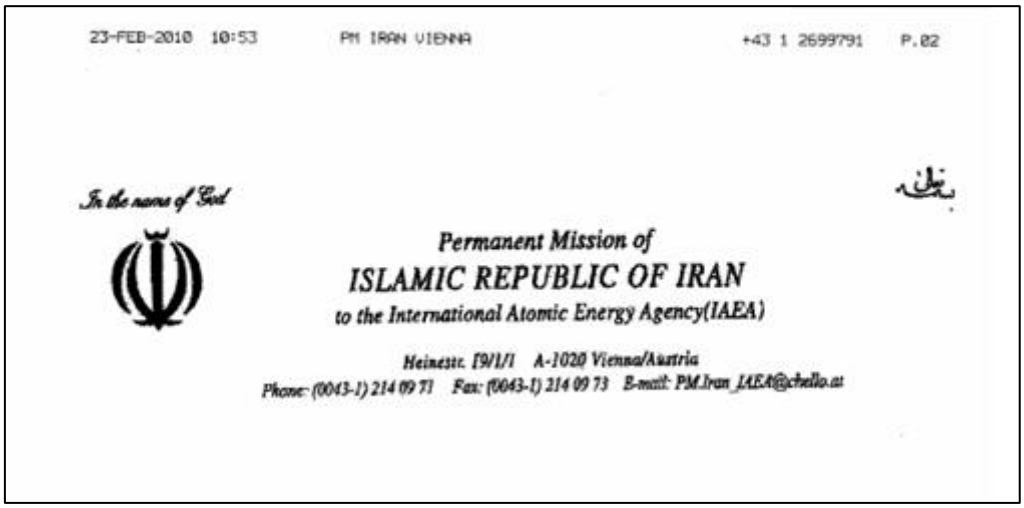
Background

Our analysts follow the activities of a number of threat groups with a wide range of motivations. In this bulletin we are sharing intelligence relating to a recent phishing campaign conducted by a group widely referred to as 'Sofacy', named after the antivirus[1] detection name for one of the malware families used by the group.

Over the years there have been a number of papers discussing variations to the malware used by the group, but little discussion of less sophisticated techniques employed by the same attackers.

Analysis

Sofacy has been discussed before as being used to target APEC members[2] and there has also been some prior analysis of the malware itself[3]. Variants of the malware have been in use for a considerable amount of time – for example, the screenshot below is from the decoy document loaded by one of the earliest versions present on ThreatExpert[4], from February 2010.


23-FEB-2010 10:53 PM IRAN VIENNA +43 1 2699791 P.02

In the name of God

Permanent Mission of
ISLAMIC REPUBLIC OF IRAN
to the International Atomic Energy Agency(IAEA)

Heinestr. 19/1/1 A-1020 Vienna/Austria
Phone: (0043-1) 214 09 71 Fax: (0043-1) 214 09 73 E-mail: PM.Iran_IAEA@chello.at

Sample 4684a377ac234fe86f468ea34d277fcd

Decoy documents are used in conjunction with malware droppers in order to make the target believe the file they have just opened is legitimate. The documents often give an indication of the attackers' intended targets.

More recently, ESET have reported[5] on related spear phishes using NATO/Ukrainian conflict themes and watering hole attacks likely targeting the defence industry and a Polish finance company. It has been publicly speculated before that Sofacy malware is Russian in origin. Indicators found in the malware analysis referenced in the appendix, such as embedded resources and targeting would appear to support this theory.

[1] http://www.symantec.com/security_response/writeup.jsp?docid=2011-090714-2907-99
[2] http://blog.trendmicro.com/trendlabs-security-intelligence/spoofed-apec-2013-email-mixes-old-threat-tricks/
[3] http://thegoldenmessenger.blogspot.de/2012/12/3-disclosure-of-another-0day-malware.html
[4] http://threatexpert.com/reports.aspx?find=netids.dll
[5] http://welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/

Targeting

Recently, we observed a number of new domain registrations by the Sofacy attackers, all of which are closely related via shared WHOIS data and infrastructure. New domain registrations are usually indicative of a new campaign, and so we were eager to find new samples of the malware which connected to the infrastructure. The domain names chosen were almost identical to the legitimate domains of several organisations, a common technique and, like carefully chosen decoy documents, often gives clues as to the likely targets of the campaign. The new domain names mimicked organisations in the following categories:

- International and European diplomatic institutions
- Popular providers of web services
- Military institutions, contractors and conferences
- Energy companies
- News organisations based out of the United States and Central Europe

In addition to new malware samples, we also found examples where the attackers were using the simple technique of phishing for credentials. The usage of malware in targeted attacks to steal information of value to attackers has been widely reported, however the simple technique of phishing for credentials, whilst still relatively common in targeted attacks, is still more typically associated with criminal attackers involved in day to day cyber-fraud.

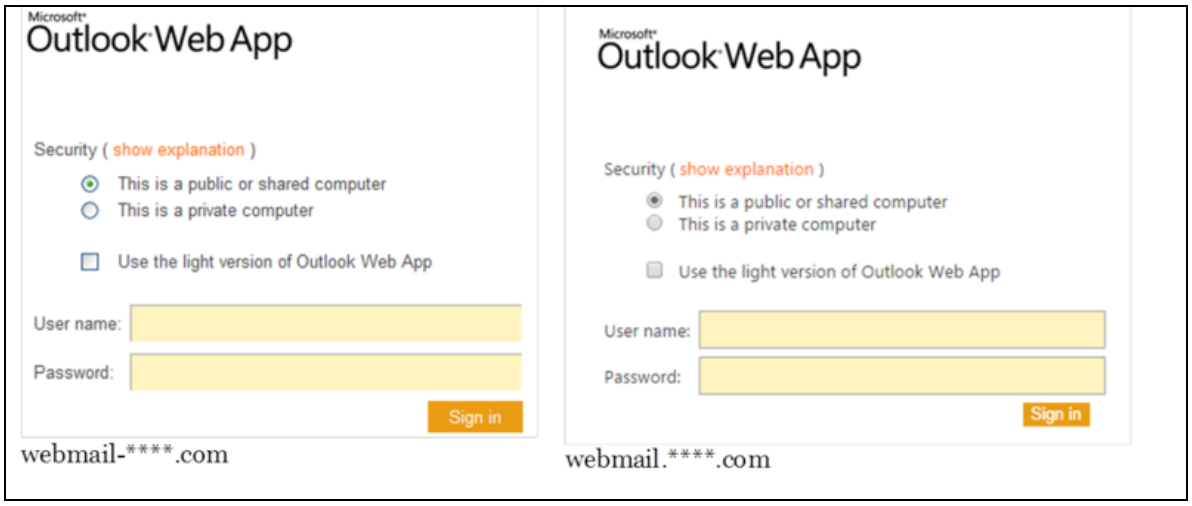
The pages used for phishing typically used obfuscated code to redirect the user to another webpage:

```
<script type="text/javascript">
    var _0x949d = ["\x6C\x6F\x63\x61\x74\x69\x6F\x6E",
                   "\x6F\x70\x65\x6E\x65\x72",
                   "\x68\x74\x74\x70\x73\x3A\x2F\x2F\x6C\x6F\x67\x69\x6E\x2D\x6F\x73\x63\x65\x2E\x6F\x72\x67\x2F
    window[_0x949d[1]][_0x949d[0]] = _0x949d[2];
</script>
```

In some pages the malicious redirect was disabled by the attackers, by placing additional JavaScript on the page which would redirect users to a legitimate site preferentially.

Fake login pages were observed both for webmail and two factor-authentication platforms. In the second case this would require the attackers to log in at the same time as affected victims, showing a level of dedication to the cause. As well as the domains used being similar to those of the targeted, the pages were also made to appear the same as their legitimate counterparts, making it difficult for end-users to tell they were being duped.

For example the screenshot below shows the contents of a credential phishing website designed to mimic the legitimate OWA site of a defence contractor. The attacker's version is on the left, the real version is on the right:



Two of the domains we identified have previously been associated in open source with credential phishing, although not attributed to this group of attackers:

- In October 2013 the domain chmail[.]in was reported[6] as being used in widespread attacks against users of the Iranian mail service chmail[.]ir

- In January 2014 the domain google-settings[.]com was reported7 as being used in credential theft against some gmail users.

Recommended Actions

As ever with phishing attacks, one of the most important preventative steps you can take is to educate staff on how to identify suspicious emails – especially as there are fewer technical measures that can be taken to prevent low distribution phishing attacks which aim to steal credentials than there are for similar attacks involving malware.

Organisations with good logging for their e-mail data could attempt to detect activity relating to compromised accounts by alerting on "impossible journeys", where locations from which users log in are monitored and where alerts are produced when a single user logs in from two separate countries in a short period of time.

Snort Signatures

We have developed some SNORT signatures to detect the current template used by the attackers in their phishing campaigns. The following signatures detect Javascript that is present on many obfuscated redirects, not necessarily related to this activity but which may be indicative of Sofacy phishing:

[6] http://www.asriran.com/fa/news/299798/%D8%A7%DB%8C%D9%85%DB%8C%D9%84-%DA%86%D8%A7%D9%BE%D8%A7%D8%B1-%D9%87%D8%AF%D9%81-%D8%AD%D9%85%D9%84%D9%87-%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%D9%82%D8%B1%D8%A7%D8%B1-%DA%AF%D8%B1%D9%81%D8%AA

[7] http://www.spamfighter.com/News-18805-Security-Researcher-Intercepted-Phishing-Email-Campaign-which-Aimed-at-Google-Users.htm

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"Potential Sofacy Phishing Redirect";
flow:established,to_client; content:"\"\\x6C\\x6F\\x63\\x61\\x74\\x69\\x6F\\x6E\"";
classtype:trojan-activity;
reference:url,http://pwc.blogs.com/cyber_security_updates/2014/10/phresh-phishing-against-
government-defence-and-energy.html; sid:xxxxxx; rev:1;)

alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"Potential Sofacy Phishing Redirect";
flow:established,to_client; content:"\"x6Cx6Fx63x61x74x69x6Fx6E\""; classtype:trojan-activity;
reference:url,http://pwc.blogs.com/cyber_security_updates/2014/10/phresh-phishing-against-
government-defence-and-energy.html; sid:xxxxxx; rev:1;)
```

The following comment occurs in many of the pages we've observed relating to this campaign, but can also appear in some legitimate sites:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"Potential Sofacy Phishing Redirect";
flow:established,to_client; content:"// stop for sometime if needed"; classtype:trojan-activity;
reference:url,http://pwc.blogs.com/cyber_security_updates/2014/10/phresh-phishing-against-
government-defence-and-energy.html; sid:xxxxxx; rev:1;)
```

For more information on this threat actor and further indicators of compromise, please get in touch with us at threatintelligence@uk.pwc.com.

Appendix 1 - Domains

Domains involved in this phishing campaign and associated domains used by the same threat actor:

```
northropgrumman[.]org.uk
counterterorexpo[.]com
nato.nshq[.]in
bostondynamlcs[.]com
natoexhibitionff14[.]com
vice-news[.]com
world-oil-company[.]com
hushmali[.]com
mfanews[.]info
azureon-line[.]com
us-mg6mail-service[.]com
mail.telecharger-01[.]com
ns1.mfanews[.]org
updatepc[.]org
ya-support[.]com
changepassword-hotmail[.]com
mail.sofexjordanx[.]com
kavkazcentr[.]info
webmail.windows-updater[.]com
abbott-export[.]com
mfapress[.]com
www.eurosatory-2014[.]com
yavuz16[.]org
mfauz[.]com
mrthelp[.]org
egreetingsfrom[.]us
kitegacc[.]net
kitegacc[.]com
mail.rnil[.]am
hothookup[.]net
NETSCHECKER[.]com
webmail-saic[.]com
intuitstatistics[.]info
flickr-service[.]com
n0vinite[.]com
assaas[.]org
rnil[.]cl
helpfromhome[.]co
gdforum[.]net
set121[.]com
academl[.]com
changepassword-yahoo[.]com
greetingcardproject[.]com
adawareblock[.]com
securitypractic[.]com
rnil[.]am
YA-LOGIN[.]com
mx1.g0b[.]mx
product-update[.]com
memoinfo[.]ru
privacy-live[.]com
tolonevvs[.]com
us-westmail-undeliversystem[.]com
test.chmail[.]in
kakashka.chmail[.]in
gov.hu[.]com
```

us-mg6-transfermail-service[.]com
us-mg6-mailreport[.]com
aadexpo2014[.]co.za
www.gdforum[.]info
militaryinf[.]com
valuetable[.]hk
googlesetting[.]com
hotmail-monitor[.]com
junlper[.]net
www.ya-support[.]com
g-analytics[.]net
www.sofexjordanx[.]com
privacy-yahoo[.]com
yahoo.chmail[.]in
windous[.]kz
youtubeclip[.]org
aa.69[.]mu
qov.hu[.]com
vvorthyhands[.]org
dkvnz[.]com
mail.account-flickr[.]com
bulletin-center[.]com
yovtube[.]co
skidkaturag[.]com
defenceiq[.]us
mail-google[.]info
soft-storage[.]com
clickchekkker[.]com
intuitanalys[.]com
sofexjordanx[.]com
intuitstatistic[.]com
militaryexponews[.]com
caciltd[.]com
windows-updater[.]com
mail.securitypractic[.]com
www.surll[.]me
heidelberqcement[.]com
armypress[.]org
sweetcherry[.]org
account-flickr[.]com
setnewpass-yahoo[.]com
scanmalware[.]info
greetingcardsproject[.]com
q0v[.]pl
link-google[.]com
www.forsvaret[.]co
link-google[.]com
cubic.com[.]co
mail.mrthelp[.]org
www.us-mg7mail-transferservice[.]com
vVortHyHands[.]org
www.vljaihln[.]com
ifcdsc[.]org
smigroup-online[.]co.uk
100plusapps[.]com
pruintco[.]com
www.yahoo-monitor[.]com
www.chmail[.]in
litu.su
www.dkvnz[.]com

mail.yahoo-monitor[.]com
us-mg7mail-transferservice[.]com
evrosatory[.]com
wind0ws[.]kz
farnboroughair2014[.]com
mfa-gov[.]info
y-privacy[.]com
login-osce[.]org
helpmicrosoft[.]net
sofexjordan2014[.]com
malwarecheck[.]info
update-hub[.]com
mx3.set121[.]com
srv-yahoo[.]com
Us-westmail-undeliversystem[.]com
bostondyn[.]com
aerospacesystem[.]us[.]com
eurosatary[.]com
telecharger-01[.]com
chmali[.]ir
privacy.google-settings[.]com
yandex-site[.]com
www.7daysinabudhabi[.]org
www.account-flickr[.]com
google-settings[.]com
ns1.greetingcardproject[.]com
eurosator[.]com
update-zimbra[.]com
asisonlline[.]org
mfapress[.]org
ya-login[.]com
stockliquidationgroup[.]com
pasport-yandex[.]com
konami-game[.]com
www.adawareblock[.]com
persa124[.]in
eurosatory-2014[.]com
clickchekker[.]com
al-wayi[.]com
molodirect[.]net
com-0cd[.]net
us-mg6mailyahoo[.]com
finance-reports.everyday[.]com-w13[.]net
apple-iclouds[.]com
unizg[.]net
mfanews[.]org
mail.ya-support[.]com
checkmalware[.]org
geaviations[.]com
flashsecurity[.]org
imperialc0nsult[.]com
cublc[.]com
evronaval[.]com
xuetue2013[.]com
www.valuetable[.]hk
mail.chmail[.]in
nshq[.]in
forsvaret[.]co
in-eternal-memory-of[.]com
www[.]us-westmail-undeliversystem[.]com

gdforum[.]info
sex-toy-shop[.]org
novinitie[.]com
yahoo-monitor[.]com
standartnevvs[.]com
pornforyou[.]in
mail.q0v[.]pl
mail.windows-updater[.]com
allcashin[.]com
changepassword-yahoo[.]com
arnf[.]bg
gpwpl[.]com
updateapi.longmusic[.]com
chmail[.]in
brokersads[.]com
testservice24[.]net
kavkazjlhad[.]com
livemicrosoft[.]net
surll[.]me
accesd-de-desjardins[.]com
mail.hushmali[.]com
sunmicrosystem[.]info
bytly[.]org
mx.rnil[.]cl
poczta.mon.q0v[.]pl
ns.mfanews[.]org
7daysinabudhabi[.]org
privacy-hotmail[.]com
ns1.al-wayi[.]com
ecards-yahoo[.]com
eurosatory2014[.]com
yahoo-analytics[.]com
www.srv-yahoo[.]com
set133[.]com

References

http://smallmedia.org.uk/sites/default/files/u8/IIIPSepOct.pdf
https://twitter.com/MalCrawler/status/489128440323252226