Cyber Threat Operations

Tactical Intelligence Bulletin

Sofacy II– Same Sofacy, Different Day

Date: 2015-04-20
Contact: threatintelligence@uk.pwc.com
Reference: CTO-TIB-20150420-01A
TLP: WHITE

Background

There has been some recent news regarding further activities of a group variously described as Sofacy[1]. We are releasing this flash bulletin containing network indicators to aid security professionals in detecting this activity.

Please contact us on threatintelligence@uk.pwc.com and we would be happy to send you a TLP-GREEN version of this report containing further indicators that you are welcome to distribute further in line with US-CERT definition for TLP.

Recent Reports

In the past few days Trend Micro and FireEye have both released reports relating to similar activity:

- Trend[2] described spear phishes containing links to malicious websites that deploy malware through apparent browser exploits and phishing for web-mail credentials.
- FireEye[3] have recently described the use of CVE-2015-3043 and CVE-2015-1701 exploits in suspected Sofacy attacks.

Interestingly, despite the use of zero-day exploits for delivery, there is some evidence that the attackers continue to use old variants of their malware[4].

PwC Threat Intelligence subscribers can refer to CTO-TIB-20150306B published in March 2015 for further details on some of the novel methods we are seeing Sofacy currently employ and the wider context to this activity.

Please review our earlier bulletin[5] or contact us for further information on analysis, targeting and recommended actions relating to Sofacy's credential phishing.

Network Indicators

Below we list a number of domains which you may wish to review network logs for. Typically registered domains are employed for phishing and/or malware command and control.
This is a redacted list of domains that are likely related to Sofacy and we note that related domains have been observed by others[6], as well as in the cited reports.

[1] Other names include APT28, Fancy Bear, Sednit and Pawn Storm.

[2] See http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/

[3] See https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

[4] For example see https://www.virustotal.com/en/file/67ecc3b8c6057090c7982883e8d9d0389a8a8f6e8b00f9e9b73c45b008241322/analysis/

[5] See http://pwc.blogs.com/files/tactical-intelligence-bulletin---sofacy-phishing-.pdf

[6] See https://twitter.com/ThreatConnect/status/589168650759884800

Appendix 1 Domains

TLP WHITE

defencereview[.]net
brnlv-gv[.]eu
militaryobserver[.]net
netassistcache[.]com
asus-service[.]net
aolnets[.]com
natopress[.]org
natopress[.]com
defencereview[.]eu
intelsupport[.]net
globalnewsweekly[.]com
osce-oscc[.]org
enisa-europa[.]com
enisa-europa[.]org
techcruncln[.]com
nato-hq[.]com
iacr-tcc[.]org
nato-int[.]com
nato-info[.]com
bmlv-gv[.]eu
foreignreview[.]com
mediarea[.]org
osce-military[.]org
europeanda[.]com
softupdates[.]info
settings-yahoo[.]com
settings-live[.]com
delivery-yahoo[.]com
privacy-yahoo[.]com
privacy-live[.]com
westinqhousenuclear[.]com
webmail.westinqhousenuclear[.]com

References

- http://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/
- http://pwc.blogs.com/cyber_security_updates/2014/10/phresh-phishing-against-government-defence-and-energy.html
- http://pwc.blogs.com/files/tactical-intelligence-bulletin---sofacy-phishing-.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
- https://www.fireeye.com/resources/pdfs/apt28.pdf
- http://pwc.blogs.com/cyber_security_updates/2014/12/apt28-sofacy-so-funny.html
- http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/
- https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html