[tr1adx]: Intel

tr1adx.net/intel/TIB-00001.html

tr1adx Intelligence Bulletin (TIB) 00001: Bear Hunting Season: Tracking APT28
[December 28, 2016]

Summary

Our APT28 (a.k.a. Fancy Bear, Sofacy) friends in the Russian Federation have been busy once again. Not only have they been busy staying in the spotlight with recent news coverage around the DNC breach and tracking of Ukrainian Field Artillery Units, but also with registering plenty of domains at a pace akin to those mileage runs folks do before year end to re-qualify for airline status.

Investigations we have conducted show recent campaigns focused on a plethora of targets in various countries and/or regions, including:

- Armenia
- Turkey
- Lithuania
- Belarus
- Malaysia
- Middle East
- Ukraine
- Slovakia
- Kazahstan
- Spain
- United Kingdom
- Argentina
- Japan
- Hong Kong
- India
- Taiwan
- Ghana
- European Union Institutions
- NATO Affiliated Targets

Targets include:

- Military
- Defense Industry
- Government
- Non Governmental Organizations (NGO's)
- Advocacy Groups
- Law Enforcement
- Law Firms and Legal Services
- Journalism / News Organizations
- Particular individuals / persons of interest
- Oil & Gas Industry

Analysis

TTP's associated with this Threat Actor allow us to track APT28's activities with a high/moderate degree of confidence, and follow their trail of breadcrumbs. From an overall TTP perspective, not much has changed; APT28 is a huge fan of registering domain names that appear to be legitimate and/or associated with their targets. APT28 will then leverage spear phishing or other methods to entice their targets to visit web sites hosted on these domains in an attempt to harvest credentials, or other desired information. Subsequently, the Threat Actor will generally install Sofacy, Agent-X malware for persistence and command & control of the acquired targets.

While the majority of TTP's (tradecraft) related to APT28 have not changed, we did discover two separate instances where registered domains were specifically tailored to target particular individuals / persons of interest, down to the level of showing what seem to be copies of passport photographs of these individuals in what appears to be an attempt to legitimize the infrastructure associated with the campaign. Furthermore, investigation of configuration files associated with these campaigns concluded that the Threat Actor had already gathered valid credentials of the user, which were hard coded into the mock application. It appears extortion may be an intended effect of this particular piece of the campaign; as such we have made a conscious decision not to publicize any Indicators of Compromise associated with the extortion elements.

Indicators of Compromise

Indicators of Compromise (IOCs): Domains (130+) - Summary Table

- 365msoffice[.]com
- acccountverify[.]com
- accgmail[.]com
- account-close-status[.]com
- accountsteam-en[.]com
- accounts-updated[.]com
- accountverify[.]com
- accountverify[.]info
- adobe-flash-updates[.]org
- adobemainsecurity[.]com
- akadns[.]info
- akamaichecker[.]com
- apple-assistance-localisation[.]com
- apple-care-support[.]com
- apple-cloud-connect[.]com
- applecloudupdate[.]com
- apple-iclouds[.]net
- appleid-security-icloud[.]com
- apple-id-service[.]com
- apple-iphonesecurity-icloud[.]com
- apple-iphone-services[.]com
- apple-location-id[.]com
- apple-security-support[.]info
- apple-support-securityiphone[.]com

- iadb-online[.]com
- icloud-id-en[.]com
- icloud-id-localisation[.]com
- icloud-id-security[.]com
- icloud-id-services[.]com
- icloud-iphonesecurity[.]com
- icloud-iphone-services[.]com
- icloud-localisation-id[.]com
- icloud-security-support[.]com
- icloud-service-apple[.]com
- icloud-support-id[.]com
- identification-apple[.]com
- identification-apple-id[.]com
- identification-icloud-id[.]com
- id-icloud-localisation[.]com
- id-icloud-support[.]com
- imf-eu[.]org
- istoreapple[.]com
- itune-app[.]com
- itunes-helper[.]net
- limited-resolution[.]com
- limited-verification[.]com
- localisation-apple[.]com
- localisation-apple-id[.]com
- localisation-apple-

- protectingcorpind[.]com
- proxysys-config[.]com
- reinstate-account[.]com
- reportscanprotecting[.]org
- reservecorpind[.]com
- rsshotmail[.]com
- samsvung[.]com
- secureconnectcompany[.]com
- secure-remove-limitation[.]com
- secure-verification-center[.]com
- security-apple-id[.]com
- security-icloud-apple[.]com
- security-icloud-localisation[.]com
- security-resolution-center[.]com
- security-verification[.]net
- security-verifications[.]com
- shcserv[.]com
- signin-icloudsupport[.]com
- support-icloud-apple[.]com
- support-icloud-localisation[.]com
- support-localisation-icloud[.]com
- support-security-icloud[.]com
- support-svc[.]com
- transfersevices[.]net

- apps4updates[.]com
- arghpxdge01-airgas[.]com
- cavuslawfirm[.]com
- checkfindmyiphone[.]com
- cloud-apple-support[.]com
- cloud-id-localisation[.]com
- csert[.]net
- dateosx[.]com
- defenceglobaladviser[.]com
- delivery-mail-service[.]com
- diplomatscouncil[.]org
- emailprovider[.]org
- emails-aol[.]com
- exchangetrusts[.]com
- facebookonlinenotice[.]com
- facebookservices[.]org
- fbarticles[.]com
- generalscaningcorp[.]org
- generalsecuritycorp[.]org
- generalsecurityscan[.]com
- getwindowsupdates[.]com
- globaldefencetalk[.]com
- gmailservicegroup[.]com
- gmailservices[.]org
- gnpad-gh-gov[.]org
- google-vservice[.]com

security[.]com

- localisation-id-apple[.]com
- localisation-id-icloud[.]com
- localisation-security[.]com
- localisation-support[.]com
- login-resolve-limitations[.]com
- login-security-center[.]com
- login-security-notification[.]com
- login-security-verifications[.]com
- mailerfeed[.]net
- mail-periodistas[.]net
- microsoftdccenter[.]com
- microsoftfont[.]com
- microsoftofficeupdate[.]net
- mobilehostsvc[.]com
- msfontsrv[.]com
- msmodule[.]net
- msofficeinstall[.]com
- nato-nevvs[.]org
- netcorpscanprotect[.]com
- nvidiagforceup[.]com
- officefont[.]com
- offlineupdates[.]com
- politicsadvertisment[.]com
- pressservices[.]net
- privacy-ukr[.]net

- transfersevices[.]net
- transworldpetroleum[.]com
- twiterservices[.]org
- update-adobe[.]com
- updatepple[.]com
- update-security-information[.]com
- updatesrvx[.]net
- us-facebook[.]com
- windowsofficeupdate[.]com
- winsystemsvc[.]net
- wpadsettings[.]net
- wsusconnect[.]com
- xn--amazo-d8a[.]com
- yuotubc[.]com

Indicators of Compromise (IOCs) [Downloadable Files]:

- TIB-00001 Domain IOCs [TXT]

If a log search for any of these Indicators of Compromise returns positive hits, we recommend you initiate appropriate cyber investigative processes immediately and engage Law Enforcement where appropriate.