[tr1adx]: Intel

tr1adx.net/intel/TIB-00003.html

tr1adx Intelligence Bulletin (TIB) 00003: Bear Spotting Vol. 1: Russian Nation State Targeting of Government and Military Interests
[Published: January 9, 2017]   [Last Updated: January 15, 2017]

Summary

The tr1adx team performs on-going research into Threat Actors, irrespective of their motivation, provenance, or targets. tr1adx Intelligence Bulletin #00003 shares intel on Russian Nation State Cyber Activity targeting Government and Military interests around the world. Please note this is an active bulletin, meaning we will occassionally add intel and information to this bulletin as we uncover new campaigns, targets or actors which meet the criteria.

tr1adx's research was able to identify targets in various countries and/or regions, including:

- Turkey
- Japan
- Denmark
- United States
- Venezuela
- India
- NATO Affiliated Targets
- United Nations

Analysis

TTP's associated with Russian Nation State Threat Actors (Civil and Military Intelligence/GRU/APT28/APT29) allow us to track these Threat Actors' activities with a high/moderate degree of confidence, and follow their trail of breadcrumbs through past, present, and future campaigns. While, for operational security reasons, we cannot go into detail on our techniques, practices, and sources for intelligence collection and analysis, we can say that the majority of the information published in this bulletin is based on in-depth research leveraging available Open Source Intelligence (OSINT) sources. In a few cases, intel data has been enriched by, derived from, and collected through other non-OSINT means.

Indicators of Compromise

Added on 2017-01-15:

Domain	Creation Date	Campaign Status	Targeted Org	Targeted Country	Targeted Domain	Analyst Notes (and other fun anecdotes)
dpko[.]info	2016-10-29	Unknown	United Nations (UN) Department of Peacekeeping Operations (DPKO)	United States	un.org	UN DPKO website
unausanyc[.]com	2015-12-02	Unknown	United Nations Association of New York	United States	unanyc.org	Identified phishing originating from this domain targeting the Venezuelan government (minpal.gob.ve)
ausa[.]info	2015	Inactive	Association of	United	ausa.org	ESET identified

ausa[.]info	2015-07-19	Inactive	Association of the United States Army (AUSA)	United States	ausa.org	ESET identified similar indicator (ausameetings[.]com) in their APT28/Sednit report.
mea-gov[.]in	2015-02-20	Inactive	Ministry of External Affairs (MEA)	India	mea.gov.in	N/A
mfa-news[.]com	2015-04-30	Inactive	Ministry of Foreign Affairs (MFA) Fake news site	N/A	N/A	N/A
defenceinform[.]com	2015-05-05	Inactive	MDefense Related Fake news site	N/A	N/A	N/A
middle-eastreview[.]com	2015-04-15	Inactive	Middle East Review of International Affairs (MERIA)	United States	rubincenter.org	N/A
middle-easterview[.]com	2015-04-15	Inactive	Middle East Review of International Affairs (MERIA)	United States	rubincenter.org	N/A
foreign-review[.]com	2015-04-14	Inactive	Foreign Affairs Fake news site	N/A	N/A	N/A

Added on 2017-01-09:

Domain	Creation Date	Campaign Status	Targeted Org	Targeted Country	Targeted Domain	Analyst Notes (and other fun anecdotes)
afceaint[.]org (*)	2016-11-02	Inactive	Armed Forces Communications and Electronics Association (AFCEA)	United States	afcea.org	Identified 2 related indicators, one of which ties in to another campaign: ▪ ns1[.]afceaint[.]org (216.155.143.28) ▪ ns2[.]afceaint[.]org (216.155.143.27)
af-army[.]us	2016-10-17	Active	Army / Air Force	United States	army.mil / af.mil	The af-army[.]us domain was seen resolving to 167.114.35.70, which is listed as one of the IP

						listed as one of the IP addresses in the GRIZZLY STEPPE report.
webmail-mil[.]dk (*)	2015-03-25	Inactive	Defence Command	Denmark	webmail.mil.dk	Domain was hosted on 216.155.143.27, also seen in AFCEA campaign. Seriously? We know it's been 2 years and the Denmark Defense campaign may not have been publicized but come on guys... #BadOpsec!
nato-nevvs[.]org	2016-10-05	Unknown	North Atlantic Treaty Organization (NATO) Affiliates	N/A	N/A	N/A
jimin-jp[.]biz	2016-12-27	Active	Liberal Democratic Party of Japan	Japan	jimin.jp	Per our Japanese Gov't sources, domain has been observed in targeted malware.
jica-go-jp[.]biz	2016-12-27	Active	Japan International Cooperation Agency	Japan	jica.go.jp	Per our Japanese Gov't sources, domain has been observed in targeted malware.
mofa-go-jp[.]com	2016-12-27	Active	Ministry of Foreign Affairs	Japan	mofa.go.jp	Per our Japanese Gov't sources, domain has been observed in targeted malware.
turkey-mia[.]com	2016-12-20	Active	Ministry of Interior Ankara (MIA)	Turkey	mia.gov.tr	Spoofed domain points to legitimate MIA domain: icisleri.gov.tr
turkey-icisleri[.]com	2016-12-20	Active	Ministry of Interior Ankara (MIA)	Turkey	icisleri.gov.tr	Spoofed domain points to legitimate MIA domain: icisleri.gov.tr

(*) Legitimate organization appears to have claimed control over the spoofed/mimicked domain.

Indicators of Compromise (IOCs) [Downloadable Files]:

- TIB-00003 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.