[tr1adx]: Intel

tr1adx.net/intel/TIB-00004.html

tr1adx Intelligence Bulletin (TIB) 00004: A Pretty Dope Story About Bears: Early Indicators of Continued World Anti-Doping Agency (WADA) Targeting
[Published: January 14, 2017]

Summary

The tr1adx team identified what we believe to be a new campaign, which we assess to be attributed to the Russian Nation State Threat Actor APT28 (a.k.a. Fancy Bear), yet again targeting the World Anti-Doping Agency (WADA) . In September 2016, WADA confirmed they were the victim of a successful breach, which occurred over the summer of 2016, and purportedly attributed to APT28, as was reported in WADA's press release on the attack. For those interested, ThreatConnect published an informative write up on this breach, entitled "Russian Cyber Operations On Steroids", detailing the APT28 campaign targeting WADA.

Analysis

On January 14, 2017, the tr1adx team observed what we believe to be early stages of a new campaign targeting the World Anti-Doping Agency (WADA) or affiliates. A Threat Actor, following similar TTP's to those we have seen Russian Nation State Threat Actor APT28 use, has registered two domains which we assess may be used in further cyber attacks against the WADA or its affiliates. Additionally, in a move similar to TTP's described in ThreatConnect's "Russian Cyber Operations On Steroids" report, we believe the Threat Actor may be preparing to launch, or has already launched a phishing campaign against their targets.

Indicators of Compromise

Added on 2017-01-14:

Domain	Creation Date	Campaign Status	Targeted Org	Targeted Country	Targeted Domain	Analyst Notes (and other fun anecdotes)
worlddopingagency[.]com	2017-01-14	Active	World Anti-Doping Agency (WADA)	Canada	wada-ama.org	Identified 1 related indicator: ▪ mail[.]worlddopingagency[.]com (40.112.145.124)
dopingagency[.]com	2017-01-14	Active	World Anti-Doping Agency (WADA)	Canada	wada-ama.org	Identified 1 related indicator: ▪ mail[.]dopingagency[.]com (40.112.145.124)

Indicators of Compromise (IOCs) [Downloadable Files]:

- TIB-00004 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.

Recommendations

Evidence suggests this campaign may be in the early execution phase. As such, a number of preventative and detective controls can be instrumented to deter this Threat Actor from achieiving their mission:

- Block traffic to and from any of the above listed domains and IP addresses on proxies and firewalls.
- Block emails originating from or going to aforementioned domains (worlddopingagency[.]com and dopingagency[.]com).
- Search through SIEM/Log Analysis tools for traces of connections to and from these domains or IP addresses, as well as proactively create alerting rules in SIEM or IDS/IPS.
- Recommendation for WADA: Get these domains taken down ASAP.