Operation: Shining Pearl

Overarching

Adversary Country 1: Hiisui

APT 1: COSMICPOWER (CMP) APT41

APT 2: METEORMASH (MRM) Volt Typhoon

Adversary Country 2: Galar

APT 1: SPACIALREND (SPR) APT29

APT 2: LUNARDANCE (LRD) APT28

1. Operational Environment (OE)
   1. Operation Shining Pearl is a joint mission encompassing all of Space Force’s Delta 26. Its primary mission partner is requesting the Delta to defend key cyber terrain from a number of highly active threat actors to protect and defend continued launch operations at Cape Canaveral. These threat actors originate from multiple countries: Hisui and Galar. While the threat actors all have different motivations, they all have one common goal: Deny, degrade, disrupt, destroy, and manipulate their targets with physical and real-world effects.
   2. Intelligence sources have identified the threat actors have previously targeted the mission partner. The threat actors have had successful attacks against their other targets in the past, including SolarWinds, the Olympics, and the Democratic National Committee.
   3. In response to the growing threat, Delta 26’s commander has ordered a collaborative competition amongst all of its cyber squadrons to defend the key cyber terrain.
   4. With over 70 space launches in 2023 alone, Cape Canaveral is the Premier Launch Site on Earth. A few of these launches were for Delta 26’s mission partner. Launching satellites into Space is the birth of the future national security outlook. Launching satellites today will mean having the high ground tomorrow.
2. Impact of Operational Environment
   1. The operational environment is critical for national security and national interests across the globe. Any disruption or degradation to the mission partner’s assets could be detrimental to the future of national security.
   2. The Space Launch mission provides communication, GPS, and ISR capabilities for the warfighter across the globe. In today’s destabilizing environment, pushing more capabilities to Space is now critical more than ever.
   3. A lack of space launches would mean a lack of communication, GPS, and ISR capabilities. The more capabilities that are launched today will result in a better posturing for the worst-case scenario.
3. Adversary Evaluation
   1. Intelligence sources have identified four active advanced persistent threat actors that could potentially have a planned attack against Delta 26’s mission partner: COSMICPOWER, METEORMASH, SPACIALREND, and LUNARDANCE. It is unknown whether or not these threat actors are working together or independently.
   2. COSMICPOWER - https://attack.mitre.org/groups/G0096/
      1. First discovered: 2012
      2. Notable Events
         1. 2011-2021: Data breach against commercial airliner, Air India
         2. 2021-2022: Compromise of at least 6 U.S. State Government Networks
      3. Expected/previously seen TTPs
         1. Keylogging
         2. Account creation
         3. Spearphishing via email
      4. Known Tools and Malware: Gearshift, Cobalt Strike, China Chopper
   3. METEORMASH - <https://attack.mitre.org/groups/G0005/>
      1. First Discovered: 2021
      2. Noteable Events:
         1. 2021: Gathered information about Guam possibly linked to recent cyber attacks against the U.S. territory
      3. Expected/Reported TTPs
         1. Living off the land by using what’s available on the host machine
         2. Remote system discovery via Powershell
         3. Masquerading malware and implants by matching legitimate names
      4. Known tools and Malware: mimikatz, ping, wevtutil
   4. SPACIALREND - <https://attack.mitre.org/groups/G0016/>
      1. First Discovered: 2008
      2. Notable Events
         1. 2015: Compromised Democratic Committee
         2. 2021: Solarwind Compromise
      3. Expected/Reported TTPs
         1. Enumeration techniques such as active directory account discovery
         2. Brute force via password guessing and password spraying
         3. Lateral movement via domain accounts
      4. Known tools and Malware: Sliver, Bloodhound, Mimicatz
   5. LUNARDANCE - <https://attack.mitre.org/groups/G0007/>
      1. First Discovered: 2004
      2. Noteable events
         1. 2016: Compromised Hillary Clinton presidential campaign
         2. 2016: Attempted to interfere with U.S. presidential election
         3. Between 2014-2018: Closed-access operations against a number of international agencies
      3. Expected/Reported TTPs]
         1. Brute force via password guessing and password spraying
         2. Living of the land via Powershell
      4. Known Tools and Malware: Advstoreshelll, Forfiles, Koadic
4. Adversary Courses or Action (COA’s)
   1. COA 1: Deny, degrade, or destroy Mission Partner’s infrastructure
   2. COA 2: Data theft and espionage
   3. COA 3: Political or military-related motives