Anchor Panda | Threat Actor Profile

crowdstrike.com/blog/whois-anchor-panda/

Adam Meyers March 22, 2013

Anchor Panda is an adversary that CrowdStrike has tracked extensively over the last year **targeting both civilian and military maritime operations in the green/brown water regions primarily in the area of operations of the South Sea Fleet of the PLA Navy**. In

addition to maritime operations in this region, Anchor Panda also **heavily targeted western companies in the US, Germany, Sweden, the UK, and Australia, and other countries involved in maritime satellite systems, aerospace companies, and defense contractors.**

Not surprisingly, embassies and diplomatic missions in the region, foreign intelligence services, and foreign governments with space programs were also targeted. We won't share too many details about this adversary – we don't want to make it too easy for them – but we will share some signatures specific to Anchor Panda. These signatures will help you find Anchor Panda, just remember to change the Signature ID (sid).

```
alert tcp $VICTIM any -> $CONTROLLER any (msg: "[CrowdStrike] ANCHOR PANDA - Adobe Gh0st Beacon"; flow: established, to_server; content: "Adobe"; offset: 0; depth: 5; content: "|e0 00 00 00 78 9c|"; distance: 4; within: 15; sid: xxx; rev: 1; reference: url,http://blog.crowdstrike.com/whois-anchor-panda/index.html; )
```

```
alert tcp $CONTROLLER any -> $VICTIM any (msg: "[CrowdStrike] ANCHOR PANDA - Poison Ivy Keep-Alive - From Controller"; dsize: 48; flow: established, from_server; content: "|54 90 1d b0 18 1b 7c ce f4 5b 24 2f ec c7 d2 21|"; depth: 16; sid: xxx; rev: 1; reference: url,http://blog.crowdstrike.com/whois-anchor-panda/index.html; )
```

```
alert tcp $VICTIM any -> $CONTROLLER any (msg: "[CrowdStrike] ANCHOR PANDA - Poison Ivy Keep-Alive - From Victim"; dsize: 48; flow: established, to_server; content: "|af c0 bb 65 5d 07 e0 0d  bf ab 75 2f 82 79 ae 26|"; depth: 16;  sid: xxx; rev: 1; reference: url,http://blog.crowdstrike.com/whois-anchor-panda/index.html; )
```

```
alert tcp $VICTIM any -> $CONTROLLER any (msg: "[CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message Header Local";  flow: established, to_server; dsize: 16; content: "|00 00 00 11 c8 00 00 00 00 00 00 00 00 00 00 00|"; depth: 16; flowbits: set,toread_header; flowbits: noalert; sid: xxx; rev: 1; reference: url,http://blog.crowdstrike.com/whois-anchor-panda/index.html; )
```

```
alert tcp $VICTIM any -> $CONTROLLER any (msg: "[CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message"; dsize: 200; flow: to_server,established; flowbits: isset,toread_header; content: "|40 7e 7e 7e|"; offset: 196; depth: 4; sid: xxx; rev: 1; reference: url, http://blog.crowdstrike.com/whois-anchor-panda/index.html; )
```

Other Known China-based Adversaries

Curious about other nation-state adversaries? *Visit our threat actor hub to learn about the new adversaries that the CrowdStrike team discovers.*

Be sure to follow @CrowdStrike on Twitter as we continue to provide more intelligence and adversaries over the coming weeks. If you have any questions about these signatures or want to hear more about Anchor Panda and their tradecraft, please contact: intelligence@crowdstrike.com and inquire about our intelligence-as-a-service solutions.