Whois Numbered Panda

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

Adam Meyers

March 29, 2013

Last week's Intelligence blog post featured Anchor Panda, one of the many adversary groups that CrowdStrike tracks. The adversary is the human component in an attack that one should focus on. It is not sufficient to simply identify 'Chinese-based hackers'; it is important to understand the adversary group that has targeted your enterprise and what intelligence they are there to collect. By understanding that there are multiple groups and that they all have different tactics, techniques, and practices (TTPs), you can begin to understand the nature of the threat, what they are looking to collect, and raise the operational cost in order to make targeting your enterprise a costly and difficult endeavor.

Attribution is a tricky subject with regard to incident response and intrusion investigation; it can take years of research to get the home address or the location of the Technical Reconnaissance Bureau (TRB) affiliated with the threat actor. We have to rely on the categorization of the adversary and understanding their TTPs, victims, objectives, and prior art to fully evaluate the threat that adversary poses to us. Understanding the tasking orders the adversary has received can be revealing of the adversary, who they are working for, and their future targeting objectives. If we understand that an adversary has targeted a high-tech company's intellectual property, then when we encounter that adversary at a different technology company, we have a pretty good idea what they are after. Victims of a targeted attack by a "known" adversary benefit from understanding their intent in order to help gauge response and hopefully make strategic decisions about what is the appropriate countermeasure. If the adversary is known to target mergers and acquisitions intelligence of companies involved in the Chinese market, then when that adversary shows up prior to, or during, some M&A activity, the victim can begin to take actions to limit the effectiveness of the compromised data, feed deceptive information or perhaps wage a formal complaint. With this in mind, this week we are providing some indicators for a China based adversary who we crypt as “NUMBERED PANDA.”

Numbered Panda has a long list of high-profile victims and is known by a number of names including: DYNCALC, IXESHE, JOY RAT, APT-12, etc. Numbered Panda has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments. Numbered Panda has targeted organizations in time-sensitive operations such as the Fukushima Reactor Incident of 2011, likely filling intelligence gaps in the ground cleanup/mitigation operations. Screen saver files, which are binary executables and PDF documents, are common Numbered Panda weaponization tactics. One of the most interesting techniques that Numbered Panda likes to use is to dynamically calculate the Command and Control (C2) port by resolving a DNS. This effectively helps Numbered Panda bypass egress filtering implemented to prevent unauthorized communications on some enterprises. The malware will typically use two DNS names for communication: one is used for command and control; the other is used with an algorithm to calculate the port to communicate to. There are several variations of the algorithm used to calculate the C2 port, but one of the most common is to multiply the first two octets of the IP address and add the third octet to that value. This is typically represented as: (A * B) + C – common values might be 200.2.43.X, which would result in communication on port 443. Numbered Panda will frequently use blogs or WordPress in the c2 infrastructure, which helps to make the network traffic look more legitimate. CrowdStrike has observed Numbered Panda targeting high-tech, defense contractors, media organizations, and western governments. The following intrusion detection rules were written and tested by the CrowdStrike Global Threat Analysis Cell (GTAC) with performance and low false positives in mind – just remember to change the Signature ID (SID) in the IDS rules. Disclosure of this information went through the same IGL process as discussed in the Whois Anchor Panda blog post.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike]
NUMBERED PANDA - Joy RAT Variant 1"; flow: from_client,established;
content: "6YmV|7c 22|"; depth: 6; sid: xxx; rev: 2; )

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike]
NUMBERED PANDA - Joy RAT Variant 2"; flow: from_client, established;
content: "Fyoj`U"; depth: 6; sid: xxx; rev: 2;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any  (msg: "[CrowdStrike]
NUMBERED PANDA - Joy RAT Variant 3"; flow: from_client,established;
content: "yb|13|j["; depth: 5; sid: xxx; rev: 2;)
```

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 Numbered Panda and their tradecraft, please contact: intelligence@crowdstrike.com and inquire about our intelligence-as-a-service solutions.