Samurai Panda | Threat Actor Profile

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

April 12, 2013

Who is Samurai Panda

April 12, 2013

Adam Meyers Research & Threat Intel

This week we're back to our old friends with a Chinese nexus. To recount the last few weeks of our adversary blog posts, we first introduced Anchor Panda, an adversary we attribute to China and associate with the PLAN.

We then moved on to another Chinese adversary we dubbed Numbered Panda to highlight the issue of community naming for adversaries and the lack of a common lexicon for characterizing these attackers.

Next, in an effort to demonstrate it wasn't relegated to China, we exposed Clever Kitten, an actor we track out of Iran who leverages some very distinct TTPs when viewed next to a more visible adversary. **This week we will discuss another Chinese nexus adversary we call Samurai Panda.**

Samurai Panda is interesting in that their **target selection tends to focus on Asia Pacific victims in Japan, the Republic of Korea, and other democratic Asian victims**. Beginning in 2009, we've observed this actor conduct more than 40 unique campaigns that we've identified in the malware configurations' campaign codes. These codes are often leveraged in the malware used by coordinated targeted attackers to differentiate victims that were successfully compromised from different target sets.

When conducting programmatic espionage activity, it can presumably become quite confusing if the attacker targets a heavy industry company, an avionics program, and seven other unique targets as to which infected host you will collect what information from. While investigating these targeted attacks, the campaign key can be leveraged in much the same way by the investigator to sort out how various malware samples are related, and perhaps what sectors the various builds were meant for.

Samurai Panda's Installation Process

The implant delivered by Samurai Panda uses a typical installation process whereby they:

1. **leverage a spearphish with an exploit to get control of the execution flow of the targeted application**. This file "drops" an XOR-encoded payload that unpacks itself and a configuration file.
2. Next, the implant, which can perform in several different modes, typically will install itself as a service and then begin beaconing out to an adversary-controlled host.
3. If that command-and-control host is online, the malicious service will download and instantiate a backdoor that provides remote access to the attacker, who will see the infected host's identification information as well as the campaign code.

Using CrowdRE with IDA Pro, you can import the CrowdStrike Intelligence Team's annotations for this malware and the associated backdoor to leverage the reverse engineering that we have already conducted.

How to Detect Samurai Panda

Here are some Snort rules that will enable you to detect Samurai Panda activity on your enterprise. These rules detect the malware "beaconing" to the command-and-control server, the initial malware check-in, and an attempt to download a backdoor module.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike]
[SAMURAI PANDA] C2 Heartbeat"; flow: to_server,established;
content: "POST"; http_method; content: "/NfStart.asp?ClientId=";
http_uri; content: "&Nick="; http_uri; content: "&dtime=T:";
http_uri; content: "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.0; .NET CLR 1.1.4322)"; http_header; classtype:
trojan-activity; sid: xxx; rev: 1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike]
[SAMURAI PANDA] C2 Communication"; flow: to_server,established;
content: "POST"; http_method; content: "/NfCommand.asp?"; http_uri;
content: "ClientId="; http_uri; content: "User-Agent: Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)";
http_header; classtype: trojan-activity; sid: xxx; rev: 1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike]
[SAMURAI PANDA] Initial Check or Backdoor Download - Malformed User
Agent"; flow: to_server,established; content: "User-Agent:
Mozilla/5.0 (compatible; MSIE 7.0;Windows NT 5.1)"; http_header;
classtype: trojan-activity; sid: xxx; rev: 1; )
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike]
[SAMURAI PANDA] Attempt to download Backdoor Module UA2"; flow:
to_server,established; content: "POST"; http_method; content:
"/Nfile.asp"; http_uri; content: "User-Agent: Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1)"; http_header;
classtype: trojan-activity;  sid: xxx; rev: 1; )
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "[CrowdStrike]
[SAMURAI PANDA] Initial Reachability Check "; flow: to_server,
established; content: "POST"; http_method; content: "TTip.asp";
http_uri; sid: xxx; rev: 1;)
```

Other Known China-based Adversaries

- Anchor Panda
- Deep Panda
- Goblin Panda
- Mustang Panda

Curious about other nation-state adversaries? *Visit our threat actor center 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 Samurai Panda and their tradecraft, please contact: intelligence@crowdstrike.com and inquire about our intelligence-as-a-service solutions where we provide additional actionable intelligence feeds such as the rules included in this post.

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell