Cyber Attacks and Political Events: The Case of the Occupy Central Campaign

Kam-Pui Chow, Ken Yau, Frankie Li

Chapter 2

CYBER ATTACKS AND POLITICAL EVENTS: THE CASE OF THE OCCUPY CENTRAL CAMPAIGN

Kam-Pui Chow, Ken Yau and Frankie Li

Abstract Occupy Central was a Hong Kong civil disobedience campaign that began in September 2014 with the goal of forcing Mainland China to allow Hong Kong to implement genuine universal suffrage as demanded by Hong Kong residents. The campaign initially encouraged citizens to block the Central District, Hong Kong's financial center. However, as the campaign evolved, large protests were organized all over Hong Kong.

While vigorous clashes occurred between Occupy Central protesters and police officers on the streets of Hong Kong, cyber attacks were launched quietly by supporters of both sides against each other's assets. The cyber weapons included mobile applications with malware for surveillance, tools for launching distributed denial-of-service (DDoS) attacks and sophisticated phishing emails with advanced persistent threat functionality. This chapter presents information about cyber attacks related to the Occupy Central campaign and classifies the attacks based on their purpose, techniques, targets and propagation. Based on the attack classification and timeline, a framework is provided that helps predict attack patterns and behavior in order to prevent or mitigate attacks launched during similar political events.

Keywords: Political events, cyber attacks, Occupy Central campaign

1. Introduction

In January 2013, the Occupy Central civil disobedience campaign was proposed by Benny Yiu-Ting Tai, an Associate Professor of Law at the University of Hong Kong. The campaign, which he named "Occupy Central with Love and Peace" (OCLP), encouraged citizens to block roads in Hong Kong's Central District and paralyze its financial infrastructure in order to force the Mainland Chinese and Hong Kong governments to implement universal suffrage for the

Hong Kong Chief Executive election in 2017 and the Legislative Council elections in 2020 according to international standards [18].

On September 22, 2014, the Hong Kong Federation of Students and Scholars began protesting outside the Hong Kong government headquarters against its decision on proposed electoral reforms made by the Standing Committee of the National People's Congress (NPCSC) [17]. This protest triggered the Occupy Central campaign. On September 28, 2014, Benny Tai announced that the civil disobedience campaign would start at 1:45 pm. The *South China Morning Post* reported that the organizers expected about 10,000 supporters to show up at Hong Kong's financial district. However, several tens of thousands of protesters filled the streets, paralyzing not just the Central District, but also parts of Causeway Bay, Admiralty and Mong Kok, through late September and early October 2014.

During the early days of the protests, the Hong Kong Police used tear gas and pepper spray to disperse the swelling crowds, especially when protesters attempted to break police lines to reach Occupy Central's main protest site at Tamar Park. The protesters were equipped with masks, goggles and umbrellas to fend off the tear gas and pepper spray. Therefore, the protest was also referred to as the Umbrella Revolution or the Umbrella Movement.

As the protesters and police clashed on the streets, cyber warfare was initiated on the Internet between protest supporters and the Hong Kong government. A variety of cyber attacks were launched, including injecting spyware into mobile devices for surveillance, executing distributed denial-of-service (DDoS) attacks on various government entities and sending phishing emails with advanced persistent threat (APT) functionality.

The cyber attacks launched by the two sides during the Occupy Central campaign are classified as: (i) silent attacks; and (ii) violent attacks. A silent attack is a low profile attack that mainly targeted protest supporters for purposes of conducting surveillance. A violent attack is a high profile attack that primarily disrupted the opponent's online services. This chapter presents a cyber warfare framework based on the timeline of silent attacks and violent attacks that occurred during the Occupy Central campaign. The framework can be used to predict cyber attack patterns and behavior in order to prevent or mitigate attacks during similar campaigns in the future.

2. Initial Violent Attacks

In June 2014, the Public Opinion Programme at the University of Hong Kong and the Centre for Social Policy Studies at Hong Kong Polytechnic University were commissioned by the Secretariat of Occupy Central with Love and Peace to organize the Occupy Central with Love and Peace 6.20-29 Civil Referendum [13]. The civil referendum was about the implementation of universal suffrage for the Chief Executive election in 2017 and the Legislative Council elections in 2020 according to international standards [12].

In order to enable citizens to familiarize themselves with the e-voting interface of the 6.22 Civil Referendum, the Public Opinion Programme at the Uni-

versity of Hong Kong launched a mobile application platform for pre-registration and mock voting on June 13, 2014 [13]. Online services for the system were provided by three prominent service providers, Amazon Web Services, CloudFlare and UDomain.

The system worked fine for the first 30 hours. However, after receiving more than 20,000 successful registrations, the three service providers came under large-scale distributed denial-of-service attacks. The attacks paralyzed the voting system, but did not compromise the security of its information. Records reveal that the domain name system (DNS) of Amazon Web Services received more than 10 billion queries in 20 hours, while CloudFlare and UDomain recorded distributed denial-of-service attacks at the rates of 75 Gbps and 10 Gbps, respectively. Reports indicate that the last batch of attacks originated from local Internet service providers.

According to analyses conducted by Internet security experts, the scale and duration of the distributed denial-of-service attacks on one targeted system over two days were unprecedented in Hong Kong (based on attacks known to the public). These large-scale distributed denial-of-service attacks are categorized as violent attacks in the proposed framework.

3. Silent Attacks on Protest Supporters

Smartphones belonging to Hong Kong democracy protesters were targeted by silent hacking attacks. In early September 2014, Hong Kong residents with Android smartphones received messages saying "Check out this Android app designed by Code4HK for the coordination of OCCUPY CENTRAL!" Code4HK is a group of coders that was attempting to improve government transparency in Hong Kong. However, according to the *South China Morning Post* of October 1, 2014, Code4HK said that it had neither developed nor distributed the Android application.

The silent attacks were discovered by researchers at Lacoon Mobile Security on September 30, 2014, just as the Occupy Central campaign started [11]. According to Lacoon Mobile Security, an advanced tool called mRat was installed on a smartphone after its user clicked on the link via WhatsApp messaging. The tool gave the hackers essentially complete access to an infected smartphone. The hackers could then extract information from the compromised device, including the address book, call logs, email and geographical locations. In addition, the hackers could upload files to a compromised device, call a number and delete specific files [2].

The mRat spyware targeted Android phones as well as iOS devices such as iPhones and iPads. The spyware that targeted iOS devices was given the name Xsser mRat. The attack behavior of Xsser mRat was very similar to mRat, but it only infected jailbroken devices. Since at least 30% of the iPhones in Hong Kong and China were jailbroken as of 2013, the reach of Xsser mRat was significant [11]. Michael Shaulov, CEO of Lacoon Mobile Security, said that mRat was the first attack to target Android and iOS devices simultaneously,

and that the iOS version used a "very sophisticated and very polished piece of malware."

The silent attack did not merely target protesters' mobile devices, it also targeted pro-democracy websites. An article posted by Steven Adair from the Volexity security firm on October 9, 2014 claimed that four websites that promoted democracy in Hong Kong had been rigged to deliver malicious software [1, 7]. The websites included the Alliance for True Democracy (`www.atd.hk`), Democratic Party Hong Kong (`www.dphk.org`; `eng.dphk.org`), People Power in Hong Kong (`www.peoplepower.hk`) and Professional Commons (`www.procommons.org.hk`).

The Alliance for True Democracy and the Democratic Party Hong Kong websites were injected with a suspected malicious JavaScript linked to the domain `java-se.com`. This domain was known to be associated with advanced persistent threat activity [1, 7].

The People Power in Hong Kong website contained a malicious iframe, which pointed to a Chinese URL shortened address that redirected visitors to an exploit page hosted by a Hong Kong IP address [1, 7]. The Professional Commons website also contained a suspicious JavaScript, which loaded an iframe that pointed to a South Korean hotel website. Steven Adair from Volexity discovered that the iframe attempted to load an HTML page that did not exist on the South Korean website, which indicated that it was a previously-active attack [1, 7].

In addition to attacks on pro-democracy websites, phishing emails were sent to protesters. Since many of the protesters were students, the phishing emails were a good way to target college and university computer systems and networks. The Chinese University of Hong Kong and the University of Hong Kong sent announcements to their staff and students to ignore phishing emails with the subject Occupy Central written in Chinese. The phishing emails contained a virus-infected file named `dblleft Letter To Hong Kong.rar` [4, 16].

A cyber attack that targeted Apple iCloud users was discovered on October 2, 2014 [6, 11]. According to the anti-censorship group `GreatFire.org`, when a user visited Apple's iCloud site in China, the site returned an invalid digital certificate, a sign that the connections had been tampered with using a man-in-the-middle attack. `GreatFire.org` alleged that the Chinese government was behind the attack, which was used to eavesdrop on communications and steal username and password information from Apple iCloud users. However, a spokeswoman from the Chinese Foreign Ministry emphasized that the country was opposed to any form of hacking.

4. Violent Attacks on Protest Supporters

Violent attacks were frequently launched on social networking sites to block communications between protest supporters. On September 29, 2014, the *South China Morning Post* [3] reported that access to the Instagram photo-sharing platform appeared to have been blocked in Mainland China on September 28,

2014 after photos of the Hong Kong pro-democracy protests were circulated via Instagram.

On September 29, 2014, the Instagram website could not be accessed by servers in Beijing, Shenzhen, Inner Mongolia, Heilongjiang and Yunnan, according to the Chinese censorship monitoring website, Great Firewall of China (`greatfirewallofchina.org`). The censors added Instagram to the growing list of foreign services blocked by Mainland China. Facebook, YouTube and Twitter have been blocked for years. Almost all of Google's online services have been blocked since June 2014. The Japanese messaging service Line and South Korea's Kakao Talk have also been blocked. Additionally, DuckDuckGo, a U.S.-based Internet search engine with a focus on user privacy, has been made inaccessible in China.

The shutting down of access to Instagram generated numerous angry comments and turned into one of the highest trending topics in Chinese microblogs on September 29, 2014, according to Weibo's own rankings. Conversations on Weibo with the hashtag Instagram could not be accessed on September 29, 2014. The microblogging service said the conversations were "in the process of being audited."

5. Violent Attacks on the Government

On October 15, 2014, the Anonymous hacker collective officially declared "cyber war" on the Mainland Chinese regime in a video announcement [11]. A few days later, on October 18, 2014, coordinated attacks were launched against Chinese government websites.

According to an October 13, 2014 report in the *South China Morning Post* [8], Anonymous had already released hundreds of phone numbers and email addresses associated with the Ningbo Free Trade Zone in the Zhejiang coastal province and a job-search site run by the Changxing county administration, also in the Zhejiang province. The reason for targeting these websites remains unknown. However, Anonymous did announce that it had successfully penetrated more than 50 Chinese government databases and leaked 50,000 user names and emails.

Anonymous had previously targeted Hong Kong government websites after first issuing a warning on October 2, 2014. In a video message, Anonymous declared cyber war on the Hong Kong government and police force for using tear gas against Occupy Central demonstrators. Attacks by Anonymous on October 3, 2014 rendered some Hong Kong government websites inaccessible or intermittently accessible. Distributed denial-of-service attacks were also launched against Chinese government websites; the sites were overloaded with artificial traffic and taken offline.

According to an October 23, 2014 report in the *South China Morning Post* [15], eleven people were arrested for launching cyber attacks on more than 70 government websites after the hackers' warning about retaliation for the use of tear gas on democracy protesters. The attacks were apparently conducted

under the banner of Anonymous, a brand adopted by hackers and activists around the globe.

After the series of the cyber attacks, Kam-Leung So, the Secretary for Commerce and Economic Development of Hong Kong, said that no information was altered or stolen, and that the government's online services were not affected significantly; the attackers merely made the sites intermittently inaccessible by issuing a flood of access requests. He also said that "attacks launched by the hacker group originated partly from Hong Kong, and partly from other regions." Hong Kong police arrested eight men and three women, aged between 13 to 39, on suspicion of accessing computers with criminal or dishonest intent.

6. Attack Characteristics

Silent attacks mainly target protesters to conduct surveillance. In the case of the Occupy Central protests, the objective of the silent attacks was to steal protesters' personal information and monitor protesters' activities and movements in order to develop a strategy for dealing with the protests.

The first step in conducting a silent attack is to install malicious code on the target device. The target device could be a web server, computer, smartphone or tablet. Smartphones and tablets are the best devices to conduct surveillance because their users (i.e., protesters) carry them wherever they go. These devices also contain valuable information such as photographs, contact lists, email and user locations, making them perfect devices to conduct spying activities [11]. It is important that the attack be performed silently without impacting normal device operations and performance; otherwise, the victims might suspect the presence of spyware and attempt to have it removed. A silent attack must be well planned and organized before it is launched. Indeed, a silent attack always involves a high level of technical skill to ensure that the malicious code is persistent on the target device and performs its activities in a stealthy manner.

Violent attacks mainly target government entities or public organizations to disrupt their online services. The objective typically is to temporarily or indefinitely interrupt or suspend host computer services that are provided over the Internet. Sometimes, violent attacks are launched to disrupt protesters' online social networking activities and online pro-democracy websites, the goal being to disrupt communications and hinder command and control of demonstrations and other protest activities.

Violent attacks are generally implemented as denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks. A violent attack can be implemented with little technical skills because attack tools are easily purchased or downloaded from the Internet. Violent attacks are destructive and difficult to defend against; they can be launched against practically any target, anytime and anywhere. These attacks are often performed by hactivist groups and criminal organizations; however, there are instances where violent attacks have been launched by nation states or their proxies. Unlike their silent counterparts, violent attacks are very high profile and their symptoms are obvious. The U.S.

Computer Emergency Readiness Team (US-CERT) lists the following symptoms of denial-of-service attacks:

- Unusually slow network performance (opening files or accessing web sites).
- Unavailability of a web site.
- Inability to access a web site.
- Dramatic increase in the number of spam email received (this type of attack is called an e-mail bomb).
- Disconnection of wireless or wired Internet connections.
- Long-term denial of access to the web or Internet services.

All the symptoms listed above were observed at the targeted government websites as well as the university websites that supported the online opinion surveys.

7. Motivation for the Cyber War Framework

According to Kam-Leung So, Secretary of Commerce and Economic Development of Hong Kong, significant damage was not observed as a result of the attacks launched during the Occupy Central campaign. However, cyber attacks can cause massive economic losses when the targeted systems do not have adequate protection. A cyber warfare framework can help predict attack trends and behavior in order to understand the risk and mitigate the damage to systems that may be targeted.

In November 2014, cyber attacks were launched against Sony Pictures Entertainment, whose global operations encompass motion picture production, acquisition and distribution; television production, acquisition and distribution; television networks; digital content creation and distribution; operation of studio facilities; and development of new entertainment products, services and technologies [14]. On December 15, 2014, Sony Pictures Entertainment announced that it had experienced a significant disruption on November 24, 2014. It determined that the cause of the disruption was a cyber attack and passed the case to leading cyber security consultants and law enforcement agencies. On December 1, 2014, Sony Pictures Entertainment was informed that the security of personally identifiable information about its current and former employees, and their dependents who participated in health plans and other benefits, may have been compromised.

According to the Australian news and entertainment website, `News.com.au` [9], the Guardians of Peace hacker group essentially stole every bit of information and private data in Sony's possession and then deleted the original copies from Sony's computers. The hacker group informed Sony that, if their demands were not met, all the files would be posted online.

The Guardians of Peace began by releasing five Sony movies to the public; four of these movies had not yet been released to theaters. Following this,

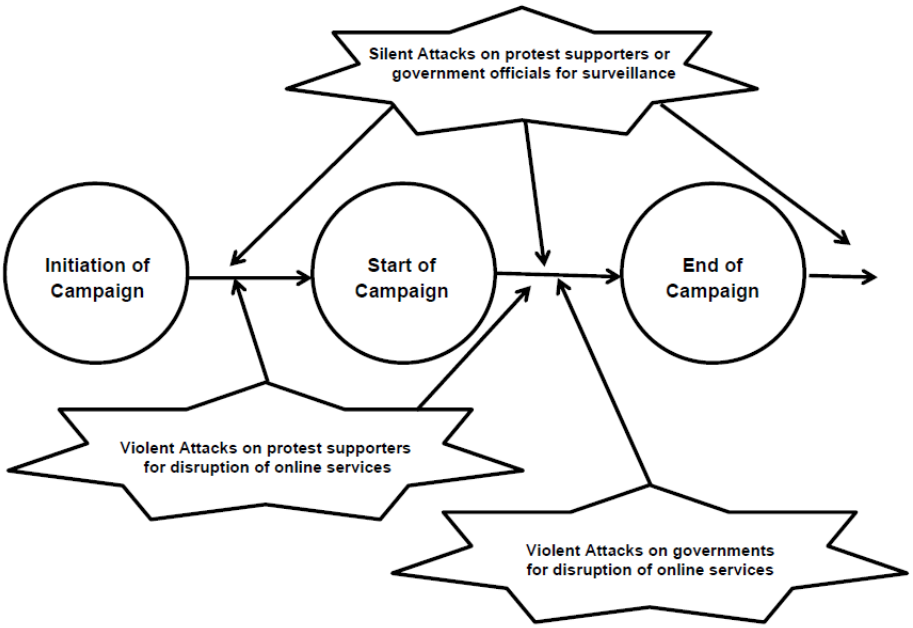

Figure 1. Cyber warfare framework.

thousands of Sony confidential documents were posted on the Internet. The documents included everything from private email messages between Sony employees to performance data and the salaries of employees, including stars in Sony films – this was considered to be the real damage to Sony.

It is hard to imagine how serious the consequences would be if similar cyber attacks were launched during the Occupy Central campaign. The damage could be mitigated if attack patterns and behavior could be predicted and appropriate actions could be taken before the attacks. Indeed, a cyber warfare framework would be an important and valuable tool for cyber attack prediction and mitigation.

8. Cyber Warfare Framework

Table 1 provides the timeline and details of the cyber attacks that were launched by both sides during the Occupy Central campaign, Figure 1 presents the cyber warfare framework constructed based on the information in Table 1. According to the cyber warfare framework, a campaign has three stages. The first stage is the initiation of the campaign, the second stage is the start of the campaign and the third and final stage is the end of the campaign. Spyware for the silent attacks would have to be ready before the start of the campaign. After the silent attacks have been launched, the spyware must continue to be active even if the protest ends. This is because the silent attacks seek to gather information about the protesters' plans ahead of time and to monitor

Table 1. Cyber attacks launched during the Occupy Central campaign.

Date	**Attack Type**	**Description**	**Victim**	**Purpose**	**Target Device**	**Technique**	**Propagation**
06/13/2014	Violent	Mock e-voting system attacked	Protest supporters	Shut down e-voting system	Web server	DDoS attack	N/A N/A
09/29/2014	Violent	Instagram website blocked	Protest supporters	Stop photo sharing	Web server	Website blocking	N/A N/A
10/10/2014	Silent	iCloud user accounts leaked	iCloud users	Steal user information	iCloud server	Man-in-the-middle attack	N/A N/A
10/03/2014	Violent	DDoS attack by Anonymous	Mainland Chinese and Hong Kong governments	Disrupt online services	Web server	DDoS and DoS attacks	N/A N/A
10/09/2014	Silent	Pro-democracy websites attacked	Protest supporters	Surveillance	Web server	Cross-site scripting	Code injection
10/12/2014 10/13/2014	Silent	Phishing attacks on university users	Protest supporters	Unknown	Computer	APT	Email
10/13/2014	Violent	Data leaked by Anonymous	Mainland Chinese and Hong Kong governments	Leak sensitive data	Network	Intrusion	N/A N/A

the protesters' activities after the protest ends [11]. Government officials may well be targets of silent attacks in future campaigns. Also, mobile devices such as smartphones and tablets are most likely to be the targets of silent attacks.

Violent attacks can be launched anytime and anywhere. Tools and services for launching denial-of-service and distributed denial-of-service attacks are easily purchased or downloaded from the Internet. Violent attacks targeting protesters would ideally be launched between the initiation of the campaign and the end of the campaign because they are intended to disrupt communications and information sharing and, thereby, impact planning, coordination and command and control activities. Violent attacks targeting government entities would typically be launched between the start of the campaign and the end of the campaign to influence the government to accept the protesters' demands.

Civil disobedience campaigns are often supported by hacktivist groups such as Anonymous. For example, in 2012, hacktivist groups were involved in a protest against amendments to Japanese copyright laws (#opJapan), dissent against Chinese censorship (#opChina) and anti-government efforts in Russia (#opRussia), Israel (#opIsrael) and North Korea (#opNorthKorea) [10].

Violent attacks almost always involve denial-of-service and distributed denial-of-service attacks. These attacks are destructive and hard to avoid. The attacks mainly target government websites and services, and also expose sensitive government data to the public. It is expected that the Mainland Chinese and Hong Kong governments would be targeted by violent attacks if a campaign similar to Occupy Central were to occur again.

9. Conclusions

The classification of cyber attacks launched by both sides during the Occupy Central protests in Hong Kong in 2014 provide useful insights into attack timelines, patterns and behavior. The resulting cyber warfare framework involving silent and violent attacks can be used to predict the patterns and behavior of cyber attacks launched in similar campaigns. Additionally, the framework could serve as a valuable tool for risk assessment and mitigation.

Future research will focus on enhancing the framework by incorporating the results of digital forensic investigations. Additionally, cyber attack campaigns launched during recent protests and conflicts in other countries will be analyzed and the results used to refine and augment the cyber warfare framework.

References

[1] S. Adair, Democracy in Hong Kong Under Attack, Volexity, Reston, Virginia (`www.volexity.com/blog/?p=33`), 2014.

[2] O. Bobrov, Chinese Covernment Targets Hong Kong Protesters with Android mRAT Spyware, Check Point Software Technologies, San Carlos, California, September 30, 2014.

[3] P. Boehler, Instagram appears blocked in China as photos of "occupied" Hong Kong circulate, *South China Morning Post*, September 29, 2014.

[4] Chinese University of Hong Kong, Phishing Emails Report, Hong Kong, China, 2014.

[5] J. Griffiths, TIMELINE: How Occupy Central's democracy push turned into an Umbrella Revolution, *South China Morning Post*, October 9, 2014.

[6] M. Kan, China attacks push Apple to warn users of iCloud threats, *Computerworld*, October 21, 2014.

[7] J. Kirk, Hong Kong pro-democracy activist websites compromised, *Computerworld*, October 13, 2014.

[8] C. Luo, Anonymous group of hackers release data from Chinese government sites, *South China Morning Post*, October 12, 2014.

[9] News.com.au, FBI confirms North Korea behind Sony hacks: The explainer, December 19, 2014.

[10] P. Paganini, Hacktivism: Means and Motivations ... What Else? InfoSec Institute, Elmwood Park, Illinois (`resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else`), 2014.

[11] J. Philipp, A cyberwar quietly rages over Hong Kong, *Epoch Times*, October 24, 2014.

[12] Public Opinion Programme, 6.20-29 Civil Referendum, University of Hong Kong, Hong Kong, China (`popvote.hk/english/project/vote_622`), 2014.

[13] Public Opinion Programme, Mock voting system of "6.22 Civil Referendum" under severe attack, University of Hong Kong, Hong Kong, China (`hkupop.hku.hk/english/release/release1149.html`), 2014.

[14] Sony Pictures Entertainment, Culver City, California (`www.sonypictures.com`), 2014.

[15] E. Tsang, Eleven arrested over cyber attacks on 70 government websites, *South China Morning Post*, October 22, 2014.

[16] University of Hong Kong, Spam Email Reports, Hong Kong, China (`www.its.hku.hk/spam-report?page=2`), 2014.

[17] Wikipedia, 2014 Hong Kong protests (`en.wikipedia.org/wiki/2014_Hong_Kong_protests#September_2014`), 2014.

[18] Wikipedia, Occupy Central with Love and Peace (`en.wikipedia.org/wiki/Occupy_Central_with_Love_and_Peace`), 2015.