Attack Delivers ‘9002’ Trojan Through Google Drive

researchcenter.paloaltonetworks.com/2016/07/unit-42-attack-delivers-9002-trojan-through-google-drive/

Robert Falcone, Jen Miller-Osborn July 26, 2016

By Robert Falcone and Jen Miller-Osborn

July 26, 2016 at 5:00 PM

Category: Unit 42

Tags: 9002 Trojan, AutoFocus, Google Drive, HTTP, Poison Ivy, TinyURL, Trojan, WildFire

This post is also available in: 日本語 (Japanese)

Unit 42 recently observed a 9002 Trojan delivered using a combination of shortened links and a shared file hosted on Google Drive. The delivery method also uses an actor-controlled server hosting a custom redirection script to track successful clicks by targeted email addresses. The infrastructure associated with this 9002 Trojan sample was also found to have previous ties to attacks on Myanmar and other Asian countries that used Poison Ivy as the payload, including a recent, and possibly ongoing campaign against Taiwan.

Short but sweet…

While we do not have specific telemetry on the attack at this time, we believe the attack relies on a shortened link (in this case using the URL shortening service TinyURL) to deliver the 9002 payload. The shortened URL is as follows:

hxxp://tinyurl[.]com/zmu4dry

This shortened link redirects to an actor-controlled server that we refer to as a redirection server, as it hosts a script responsible for redirecting the browser to another location. The shortened link above points to:

hxxp://222.239.91[.]152?
<redacted>QGdtYWlsLmNvbWh0dHA6Ly90aW55dXJsLmNvbS9qZmo5b3V2

The URL above contains base64 encoded data, which we believe will then be decoded by the server. The base64 encoded parameter in the URL redirect decodes to:

<redacted>@gmail.comhttp://tinyurl[.]com/jfj9ouv

The Gmail address in the decoded data is the legitimate address of a well-known politician and human rights activist in Myanmar. The shortened URL within the decoded data, specifically ‘hxxp://tinyurl[.]com/jfj9ouv’ again redirects to:

hxxps://drive.google[.]com/uc?
id=0B0eVt8dSXzFuN2ltVlVkVl8zNVU&authuser=0&export=download

Actor's Redirection Server

The server with an IP address of '222.239.91[.]152' appears to run a script that parses parameters from inbound HTTP requests. To better determine the script's functionality, we issued a series of HTTP requests to the redirection server to figure out the purpose of the base64 encoded data within the URL and to determine the strings that the script uses to redirect the browser.

Our initial HTTP request, as seen in Figure 1, involved the URL pointed to by the initial shortened link associated with this attack. As seen from the HTTP response, the script issued an HTTP 302 Moved Temporarily response to relocate the browser to the URL in the "Location" field, which is the same URL from the decoded base64 data sent in the HTTP request.

```
1  $ curl -i -A "Mozzarella/4.0" 222.239.91[.]152?
2  <redacted>QGdtYWlsLmNvbWh0dHA6Ly90aW55dXJsLmNvbS9qZmo5b3V2
3  HTTP/1.1 302 Moved Temporarily
4  Connection: close
5  Content-Length: 0
6  Date: Mon, 18 Jul 2016 16:25:28 GMT
   Location: http://tinyurl[.]com/jfj9ouv
```

Figure 1 Response to HTTP request to initial delivery URL

The second test HTTP request we issued used the base64 encoded data for the string "fake@gmail.comhttp://yahoo.com", which as seen in Figure 2 would redirect the browser to "http://yahoo.com" via an HTTP 302 response. This suggests that the email string is not used for any sort of authentication for the inbound request, and instead is possibly used by the threat actors to track successful clicks by a targeted email.

```
1  $ curl -i -A "Mozzarella/4.0" http://222.239.91[.]152/?
2  ZmFrZUBnbWFpbC5jb21odHRwOi8veWFob28uY29t
3  HTTP/1.1 302 Moved Temporarily
4  Connection: close
5  Content-Length: 0
6  Date: Mon, 18 Jul 2016 17:10:33 GMT
   Location: http://yahoo.com
```

Figure 2 Test request confirming that the redirection server uses the base64 decoded data for redirection

We issued an HTTP request using the base64 encoded data for the string "fake@gmail.comyahoo.com". Figure 3 shows that the server responded with an HTTP 200 OK response that attempts to resemble an HTTP 403 Forbidden response, by writing "403 Forbidden" to the browser window. This error suggests that the redirection script on the server parses the base64 decoded data for the string "http" to determine the redirection location.

```
$ curl -i -A "Mozzarella/4.0" http://222.239.91[.]152/?
ZmFrZUBnbWFpbC5jb215YWhvby5jb20
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 89
Date: Mon, 18 Jul 2016 17:11:10 GMT

<html><head><title>403 Forbidden</title></head><body><h1>403 Forbidden</h1></body>
</html>
```

Figure 3 Test request showing the redirection server requires "http" within the base64 decoded data

We ran subsequent test requests to find additional strings that the script would check for within the base64 decoded data, which it uses to determine the location it should redirect the browser. We found that the script also supports redirection to URLs that begin with “https”. Also, the script is case sensitive, as requests for URLs with “HTTP” and “HTTPS” resulted in the same 403 Forbidden response seen in Figure 3. Lastly, we determined that the script does not require the “://” characters after “http” and “https”.

Trojan from the Cloud

In the delivery of this attack, the shortened link that the redirection server redirects to points to a Zip file hosted on Google Drive. The Zip file has a filename of “2nd Myanmar Industrial Human Resource Development Symposium.zip” (SHA256: c11b963e2df167766e32b14fb05fd71409092092db93b310a953e1d0e9ec9bc3) and contains one executable that was added on July 13, 2016.

The executable within this Zip archive has a filename “2nd Myanmar Industrial Human Resource Development Symposium.exe” (SHA256: 49ac6a6c5449396b98a89709b0ad21d078af783ec8f1cd32c1c8b5ae71bec129). It is a dropper Trojan that saves a decoy and a payload to the system then opens both. The executable uses the PowerPoint icon, as seen in Figure 4 to trick the victim into launching the executable by making the user think the file is a PowerPoint presentation.

Figure 4 Payload has a PowerPoint icon to trick the victim into double clicking the executable

The decoy, seen in Figure 5, is a PowerPoint presentation that contains details of a conference in Myanmar held on July 30, 2016, titled “Role of JMVTI Aung San and Building of Clean and Safe Automobile Society”. The Japan Myanmar Vocational Training Institute (JMVTI) Aung San is a forthcoming vocational training center established by the Asia Environmental Technology Promotion Institute under Myanmar's Ministry of Science and Technology.

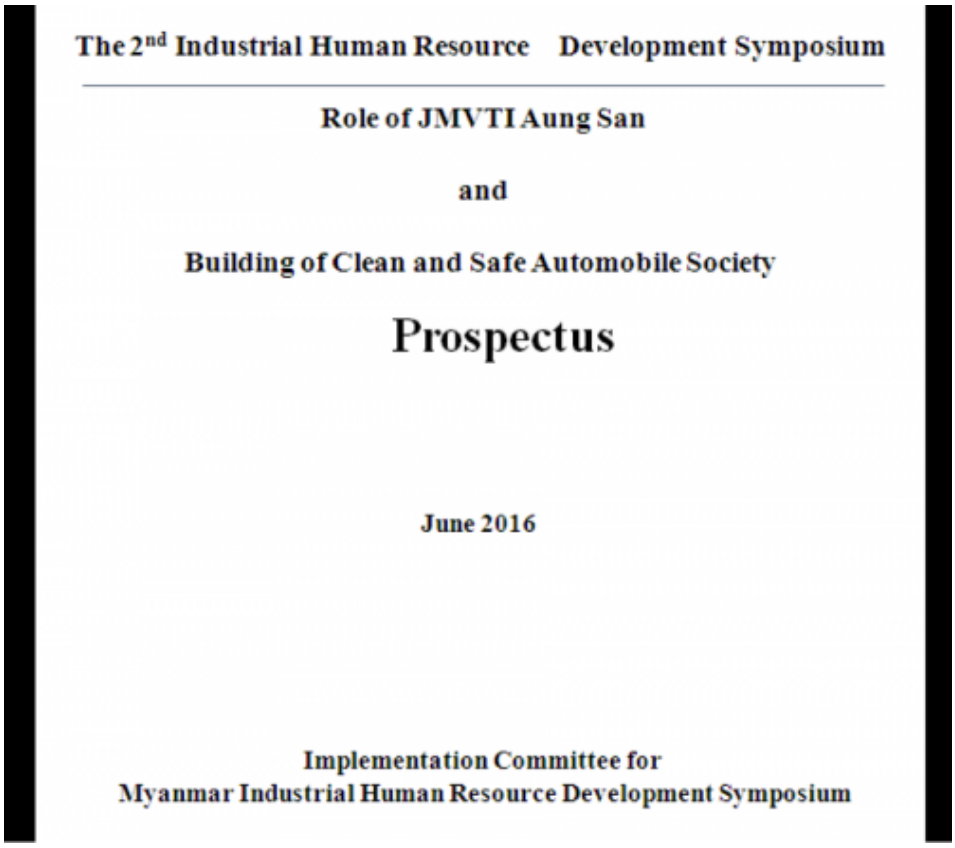

Figure 5 Decoy document opened during the installation of the 9002 Trojan

In regards to the payload, the dropper creates a randomly named folder within the current user's folder (%USERPROFILE%), which it uses to store the following files:

- RealNetwork.exe (SHA256: 10d40c51d85ea9ced6050b8951802aaebe81f7db13f42fe5a5589172af481a7e)
- main.dll (SHA256: 53671fe98a0c8c85f6f8eabfa851e27b437f6c392b46e42ddea3f0a656591b12)
- mpaplugins\MPAMedia.dll (SHA256: f76f639f2a7b8f39abf83737c6d3e533be66398c85ec95526e4b13561e15fbae)

The 'RealNetwork.exe' file is a legitimate executable signed to 'RealNetworks, Inc.' that loads 'mpaplugins\MPAMedia.dll' to call a function named 'BuildDeviceDatabase'. The threat actors however, leverage the legitimate executable to sideload a DLL they created by saving the 'mpaplugins\MPAMedia.dll' to the randomly named folder created by the dropper.

The sideloaded 'MPAMedia.dll' DLL first checks to make sure the system time is greater than May 20, 2016 as a likely attempt for sandbox evasion. It will then load the 'main.dll' file initially saved to the randomly named folder created by the dropper. The overall loading process of this Trojan can be seen in Figure 6.

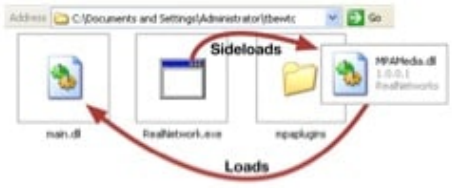

Figure 6 Overview of DLL sideloading process

The ‘MPAMedia.dll” DLL calls exported functions named "stdInstall" and "CreateFunc" from within ‘main.dll’. The 'stdInstall' function is responsible for creating the following autorun registry key for persistence purposes:

Software\Microsoft\Windows\CurrentVersion\Run\RealNetwork

The 'CreateFunc' exported function returns the offset within the 'main.dll' file to shellcode that contains 9002 Trojan's actual functional code, which 'MPAMedia.dll' DLL will then create a thread to execute the Trojan. The 9002 Trojan creates two mutexes during its execution: F16ME and widfasdf. It also creates the following registry key that it uses to store the path to the user's folder (%USERPROFILE%):

HKCU\Software\Microsoft\F6\uid

The Trojan uses the path stored in this registry key to locate its configuration, which it decrypts using a multiple-byte XOR algorithm and a key of “1pKFmjw”. Figure 7 shows a hexdump of the decrypted configuration for this sample of 9002.

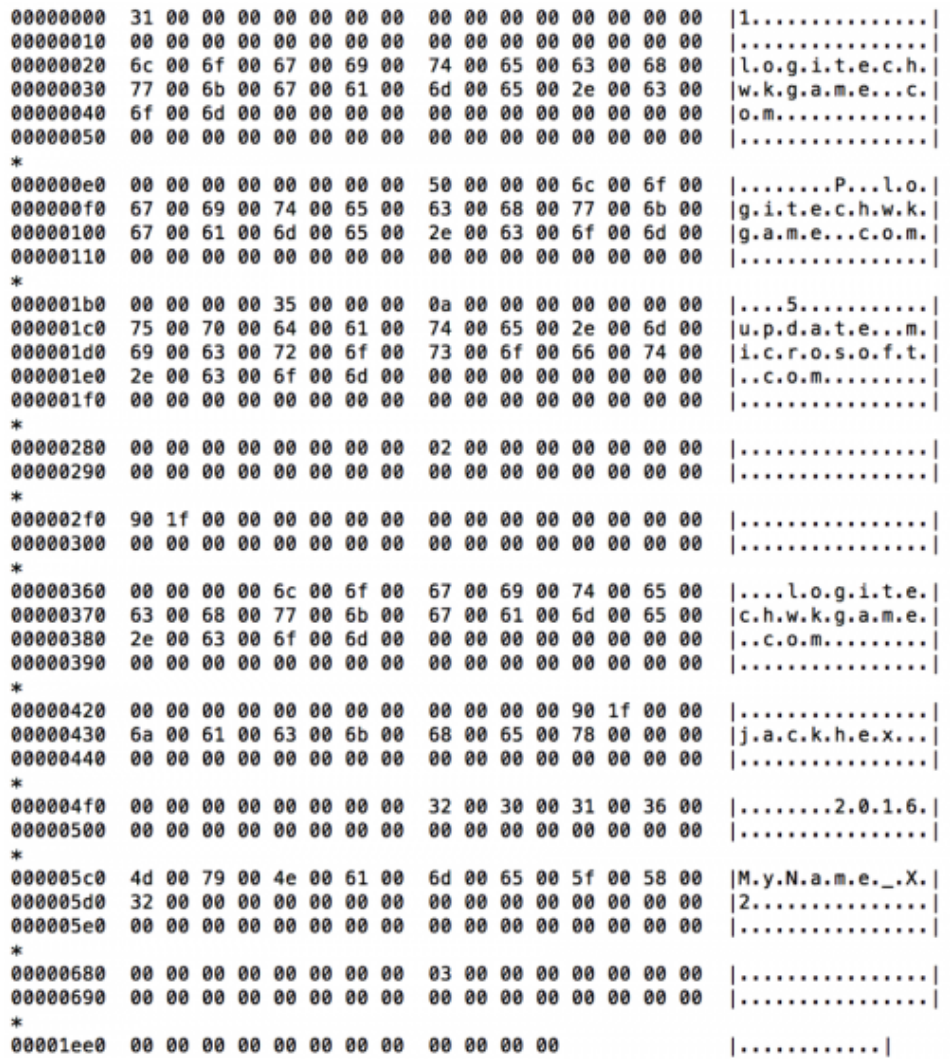

Figure 7 9002 Trojan's configuration

Using the configuration file above, the 9002 Trojan communicates with the following domain that acts as its command and control (C2) server:

logitechwkgame[.]com

The Trojan sends network beacons to its C2 server using two different methods. The first method, seen in Figure 8 uses a custom protocol on TCP port 80 that begins with the string ‘9002’, which is the basis of the tool’s name. If the C2 server responds, the Trojan will send system specific information along with the strings “jackhex” and “2016” from the configuration file. "jackhex" has also been seen in a C2 for what is likely related Poison Ivy activity, discussed briefly later in this blog.

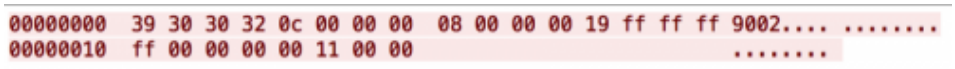

Figure 8 Network beacon using custom 9002 protocol

The second beacon method also uses TCP port 80, but this method uses HTTP requests to communicate with its C2 server. Figure 9 shows a sample HTTP request issued by this Trojan, which has a user-agent of “lynx” and POST data of “AA” that are both hardcoded into the payload.

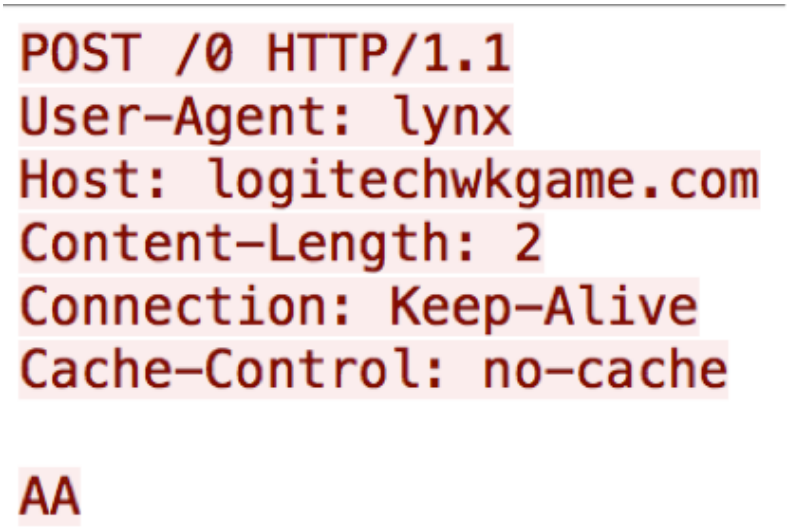

Figure 9 Network beacon from 9002 using HTTP request

The two beacons seen generated by this payload are very similar to those generated by the ‘3102’ variant of 9002 that we previously analyzed. The capabilities within this 9002 sample are very similar to the 3102 variant discussed, as its main functionality is to load plugins provided by the C2 server and call an exported function named “CreatePluginObj”.

Infrastructure and Poison Ivy Ties

The C2 server ‘logitechwkgame[.]com’ resolves to the IP address '222.239.91[.]30', which also resolved to 'admin.nslookupdns[.]com' at the same time as 'logitechwkgame[.]com', suggesting that these two domains are associated with the same threat actors. 'admin.nslookupdns[.]com' was found to also be a C2 for Poison Ivy samples associated with attacks on Myanmar and other Asian countries as discussed in a blog published by Arbor Networks. An additional tie between the activity is the Poison Ivy C2 'jackhex.md5c[.]net', as "jackhex" is not a common word or phrase and is also seen in the beacon activity with the previously discussed 9002 sample.

In addition to those noted in the blog by Arbor Networks, we found several other Poison Ivy samples using the same mutex, created by the same parent processes, and using most of the same C2 infrastructure. However, the samples we collected lack campaign IDs and all use "version2013" as the password to encrypt its communications. The additional Poison Ivy samples also provided us three new C2 domains:

- outhmail[.]com
- mxdnsv6[.]com
- microsoftserve[.]com

Also, some of the C2 domains associated with these Poison Ivy samples were registered with emails that were used to register the following possibly related domains:

- gooledriveservice[.]com
- queryurl[.]com
- appupdatemoremagic[.]com

While we do not have complete targeting information associated with these samples, several of the decoy files were in Chinese and appear to be part of a recent and possibly ongoing campaign targeting organizations in Taiwan. The decoy themes centered primarily around cross-strait relations and the Taiwanese Mainland Affairs Council (MAC), which is a cabinet-level organization tasked with creating, implementing, and overseeing policies between Taiwan and the People's Republic of China (PRC).

Conclusion

The use of Google Drive to host malicious files is not a new tactic in attacks. However, using a well-known hosting platform may allow the downloading of a payload to blend into other legitimate traffic from the hosting provider. The actors still use spear phishing as their primary attack method, but because that technique has been so well publicized, intended victims are perhaps more cautious about opening suspicious email attachments or links. As spear phishing becomes less successful, threat actors need to continue to adapt and find new methods to successfully deliver malware. The use of a URL shortening service and a redirection server further aids the chances of a successful attack, as it becomes more challenging to determine the validity of the link within an email due to the way link shorteners obfuscate link content.

The files used in these attacks are properly classified as malware by WildFire. AutoFocus customers can find out more about both 9002 and Poison Ivy via the respective malware family tags.

IOCs

9002 samples

C11b963e2df167766e32b14fb05fd71409092092db93b310a953e1d0e9ec9bc3
49ac6a6c5449396b98a89709b0ad21d078af783ec8f1cd32c1c8b5ae71bec129

Poison Ivy samples

193ae4da14874aa29902052d08064395afa5e4763f949e7369157d893fa08653
ac8fc264c7ec3cf70836e1bb21f9a20174b04ad49731b8797d7d8bb95cb353e2
12759f7fd01ffdea97954be5404d7e43a3941a7388129e7b6ace85f56b500cd8
0940602e7d47941f36c975afa9d2c6b1b0d2bd15bbea6ad4baf0f828420d72bf
6bdd45cb6c021512c203cf01a051dce28449e364627e1366412c0051094f60a0
f0ab826ea65b4a9eb66528ad74c4d3e747c1ecebfca6bdafd2504e0f794195d9
e2fb4a53e54774f1645c940f905e76beb5fc729e9e968b736b8377312cb2454a
0af768b4ba8fe7aac7a7da7fd5f21e7496d5617dccdf2321f526fd1091d64a6d

fd21cd1846f25d42b1997ec1fd5ae6e14ea9b5bb0161ab7edf0ce184174e6da6
12759f7fd01ffdea97954be5404d7e43a3941a7388129e7b6ace85f56b500cd8
08dee1f5ced372716ad5c6e3f2041bcdeb25e905efc19d3749fe637d0a589ccc
269c03e205c403ab8fa1033caa1c8e3a86a1495cc33a7f3a3a3c9b8a9ea77490
3a9ab623c8a0a9f6c65e108e83c90da7620d2d6b22192c857556117587d0d038

C2 Domains

logitechwkgame[.]com
jackhex.md5c[.]net
webserver.servehttp[.]com
admin.nslookupdns[.]com
outhmail[.]com
mxdnsv6[.]com
microsoftdefence[.]com
microsoftserve[.]com
gooledriveservice[.]com
queryurl[.]com
appupdatemoremagic[.]com