Symantec™
Security Response

# Trojan.Taidoor:
## Targeting Think Tanks

Stephen Doherty
and Piotr Krysiuk

## Contents



## Executive summary

Trojan.Taidoor has been consistently used in targeted attacks during the last three years. Since May 2011, there has been a substantial increase in its activity. Taidoor's current targets are primarily private industry and influential international think tanks with a direct involvement in US and Taiwanese affairs. Facilities in the services sector that these organizations may use have also been targeted. There are a number of additional ancillary targets.

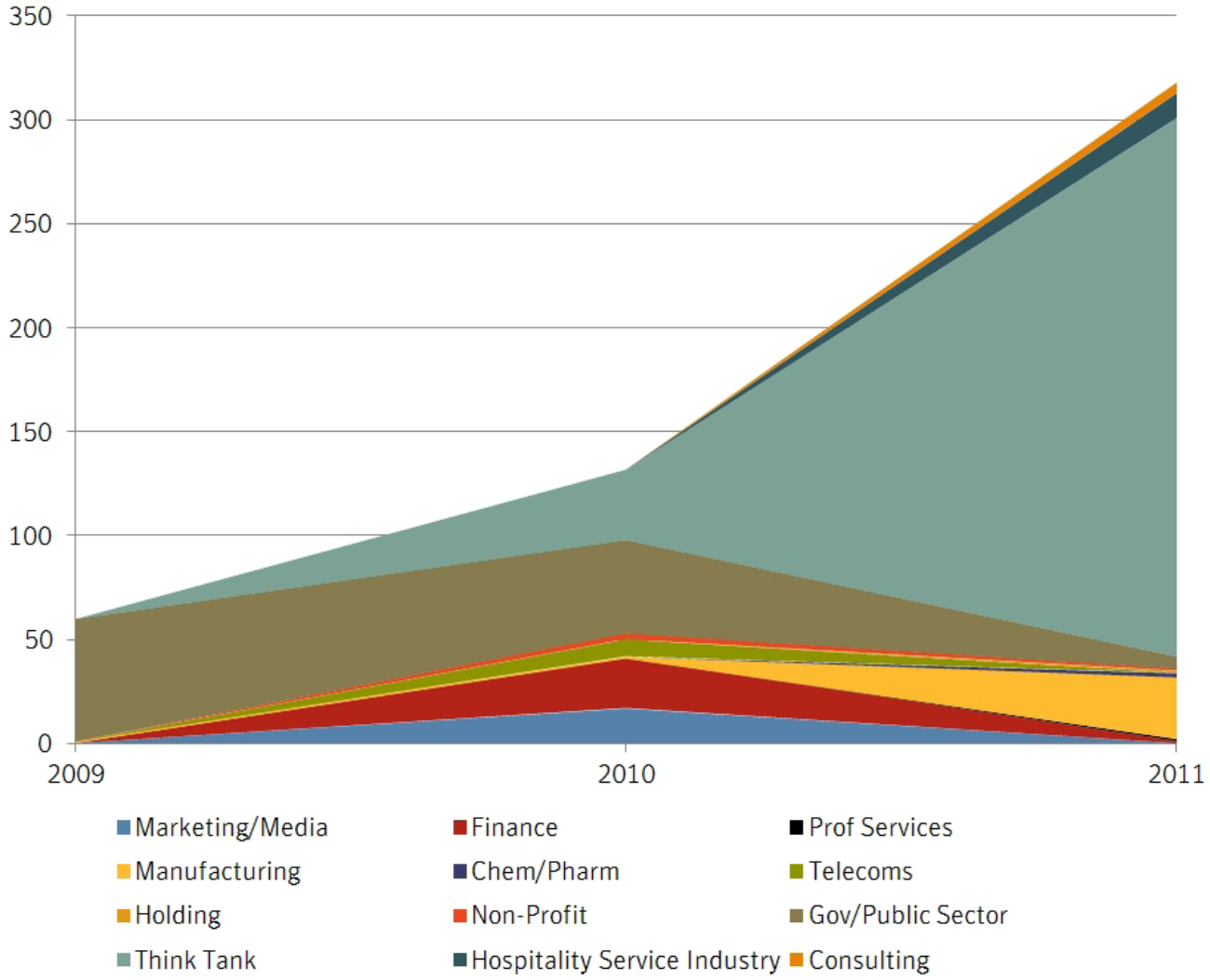
Trojan.Taidoor dates back to March 2008 and in-field telemetry has identified Taidoor being used in targeted attack emails since May 2009. Fourteen distinct versions and three separate families of the Trojan have been identified to date. The threat continues to evolve to suit the attackers' requirements.

## Introduction

During 2009, and the majority of 2010, government organizations and a range of private companies were targeted by the Taidoor attackers. However around the beginning of 2011, the attackers' focus shifted dramatically, with international think tanks, the manufacturing industry, and defense contractors who have interests in Taiwan consistently being targeted. The chart below illustrates the volumes and the industries targeted using Taidoor over the last three years. The shift in targets is clearly portrayed in figure 1.

Figure 1

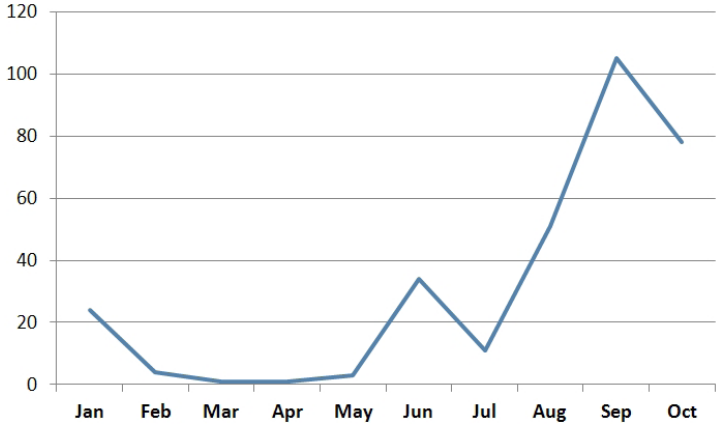
**Targeted Taidoor attacks per industry 2009-2011**




In 2011 the US had been involved in a variety of discussions with Taiwan, the most public of which was in relation to the upgrade of the Taiwanese Air Force. Around the same time Taidoor started to almost exclusively target individuals from influential think tanks, specifically those who have expertise in South Asian and South-East Asian policy and military strategy. Although these are not the first attacks on think tanks, the persistence and sheer volume of the Taidoor attacks has made them more notable. A timeline of the attacks highlights the increased volume of targeted Taidoor emails sent between May and October 2011, including their peak during the US-Taiwan Defense Industry Conference that was held September 18-20, 2011, as shown in figure 2.

Figure 2

**Increase of Trojan.Taidoor targeted attack emails**




While Taidoor's targets have changed over the years, the attack methodology has remained consistent. Currently the only known attack vector for Taidoor is through targeted emails. The email attachments exploit a variety of

vulnerabilities, yet the payload Trojan itself has seen little change in terms of functionality. Taidoor is limited to using publicly disclosed vulnerabilities; no zero-day exploits have been seen in use. This separates Taidoor from more recent high-profile attacks—such as those involving Duqu or the recent attacks on RSA—where the attacks are highly sophisticated and exploit zero-day vulnerabilities. The Taidoor group appears to play a numbers game when it comes to breaching networks, relying on targeting users running out-of-date, unpatched versions of software for the attacks. As one particular campaign gathered momentum, the attackers resorted to sending broad and repeated barrages of emails to large groups of individuals at the target organizations in an attempt to compromise the network.

The rest of the document will discuss these attacks in more detail, beginning with a breakdown of the typical stages of a Taidoor attack. Starting with crafting the targeted email, the focus will then move to the attachment and its components: the Taidoor dropper containing the true payload—an embedded, encrypted back door Trojan offering remote access to the attacker on the compromised computer. Detailed analysis of the command-and-control (C&C) functionality will be revealed, including the observation of hacked third-party servers as part of its infrastructure to forward communications to the attackers. During the analysis some live interactive sessions were captured revealing interaction with a human attacker, and his or her intentions once on the box. One of these interactive sessions is presented. The final section provides attributes that may point to the profile of the attackers.

Taidoor is not going away. It's persistent, it's constantly evolving, and the adaptability of the attackers will ensure that it remains a danger to any organization that falls within its scope.

# Technical details

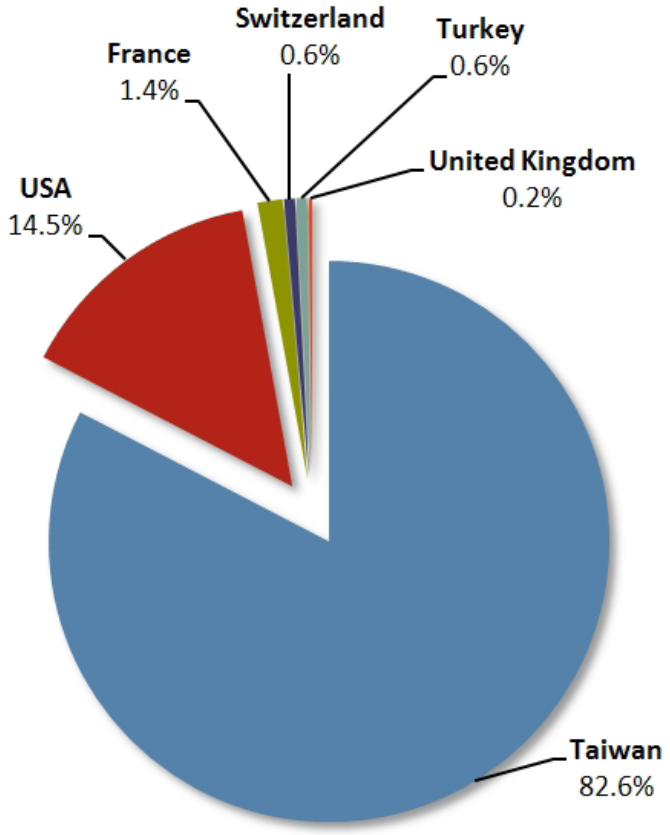
## *The email*

This is the breach component of Taidoor, which is pivotal to the attack. Taidoor emails are created with varying degrees of sophistication and are typically employed in a two-pronged attack.

The vast majority of emails used in these recent attacks are sent from mail servers based in Taiwan and the US, as shown in figure 3. The country of origin will change depending on the targets of the attack. For example the mails from France contained subject matter related to the G20 summit in Paris, while those coming from Turkey were directed at targets with Turkish email addresses.

Figure 3

**Mail server country of origin for Taidoor emails**



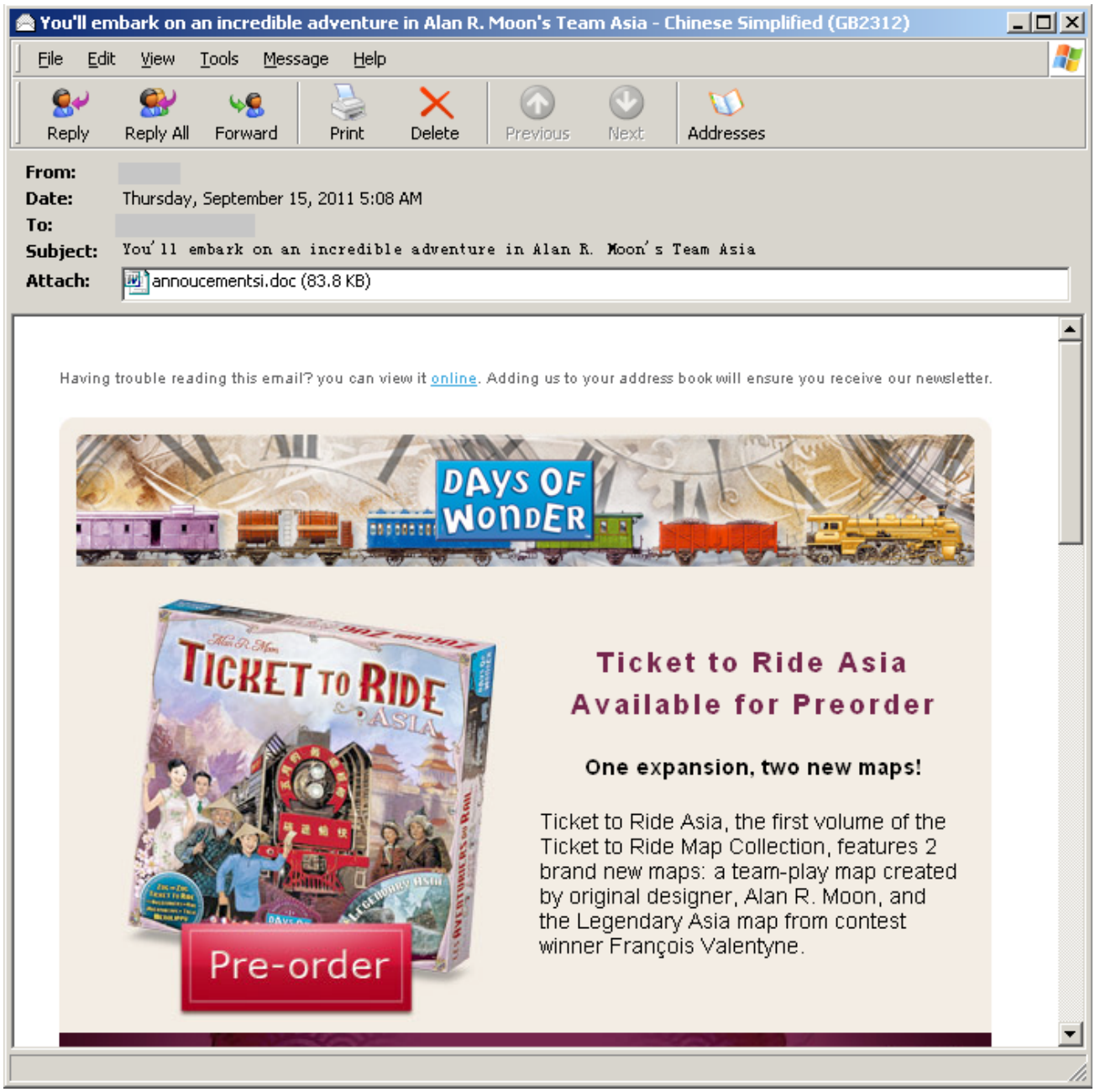

### Crafting the email

To begin with, the main target of interest is identified. The content of the email is specifically crafted in order to entice the chosen target into opening it. The email is then either sent solely to the target of interest or the target of interest plus a group of other personnel working at the same organization. This second strategy is popular with more recent Taidoor attacks, as it would prove useful in situations where compromising the main target is proving difficult. Compromising a lower-value target still provides a foothold within the organization from where the attacker can then attempt to move towards the true target.

There are two types of content typically found in Taidoor emails. The first type is simple, requiring little-or-no background research on the target. The content is general, typically including a catchy Subject line, a funny image, a brief message, or a topical subject that may entice the user into opening the malicious attachment, such as that displayed in figure 4.

Figure 4

## A generic Taidoor email



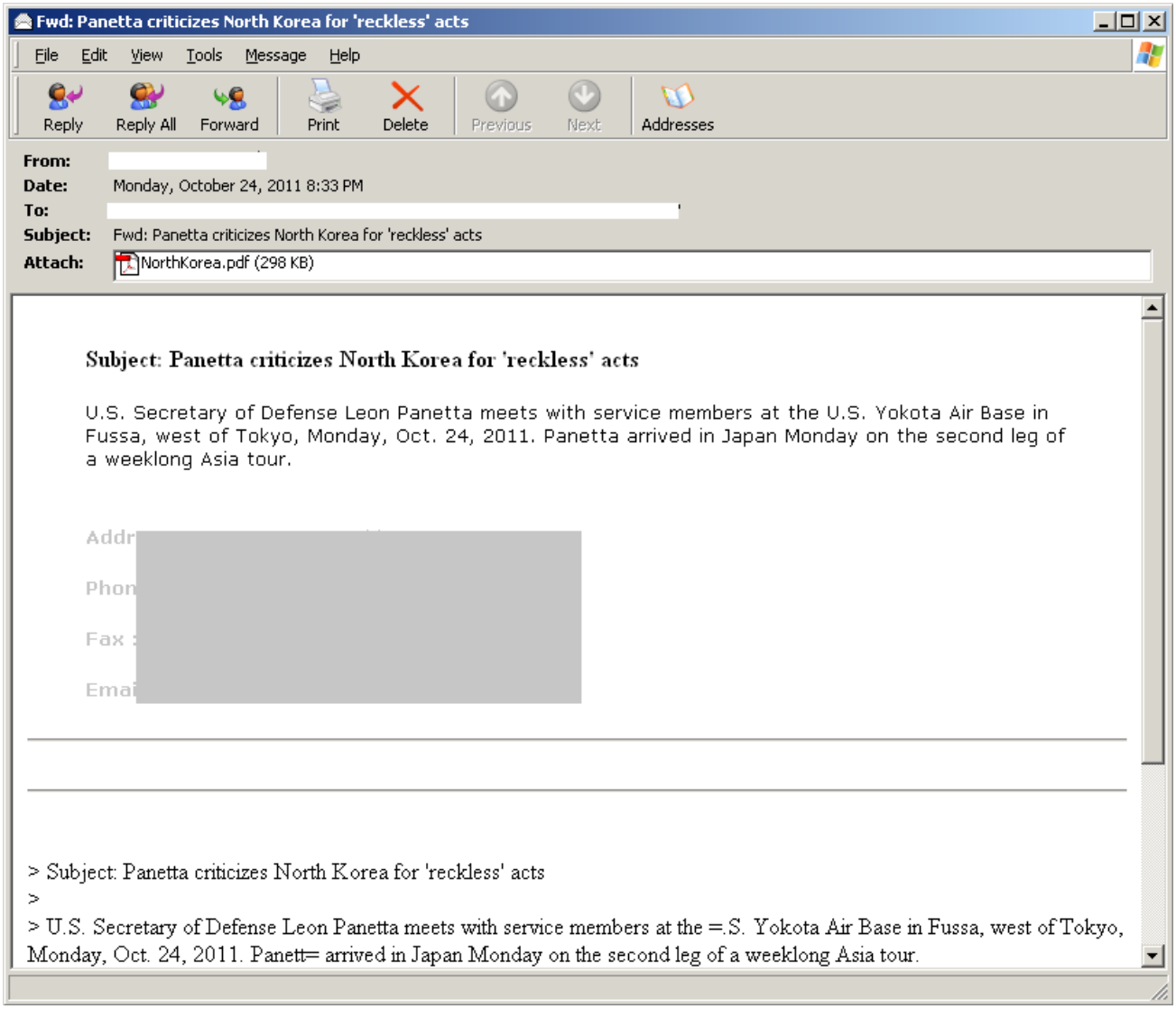

The second type requires some background research on the intended target. Far more preparation is required, as the email will need to contain content relevant to the target. The subject line, the message body and the attached document will all contain information that might entice them into reading what is inside the attachment. The content is typically related to policy or events that the target would be interested in or would likely attend. The sender's email address will also be doctored so that it appears to have come from a reputable source; someone they would probably recognize by name. This would likely be a co-worker, a speaker at an upcoming event, or a prominent individual in their chosen field.

Here is an example of a targeted attack that took place on October 24, 2011. Over the course of the day, targeted mails were sent to 25 individuals working at three separate organizations. The same malicious file was attached to all the emails; however, the subject line and the message content differed. Examining the malicious attachment we could see it was identical for each email. Here are the four subject lines used in these emails, followed by an example email:

- *Fwd: Panetta criticizes North Korea for reckless acts*
- *Panetta criticizes North for reckless acts*
- *Returned mail: see transcript for details*
- *Warning: could not send message for past 4 hours*

Figure 5

## An targeted Taidoor email



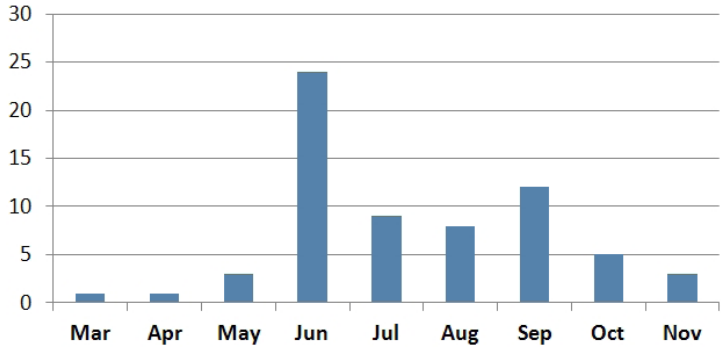

Out of the 25 emails, 22 were sent through a Taiwanese mail server. They targeted individuals working at an influential international think tank located in the US and were sent in quick succession. Later that day two more emails containing an identical attachment were sent through a mail server located in the US. However this time the emails targeted three prominent figures working at three separate organizations: one located in the US (the think tank that was targeted in the earlier batch of emails) and two others in Germany. These three targets are subject experts on military strategy and policy in South-East Asia. This tactic is typical of Taidoor, as mentioned earlier, where one of these targets appears to be the “real” target of interest and the rest appear to be of lesser interest, but could offer up useful information or be used as a stepping stone toward the true target.

Determining who the targets of interest are is straightforward when examining the frequency of targeted emails sent to individuals. As an example, a target of interest at one of these organizations is referred to as "Mr. X".

Mr. X was sent up to 23 targeted Taidoor emails in June 2011 —a substantial increase from previous months. This individual was consistently targeted for over nine months—by far the most targeted individual. Such focus demonstrates the persistence of the Taidoor attackers. The repeated attempts indicate that this target has been extremely difficult to compromise and is considered of high value.

Figure 6

**Emails targeting "Mr. X" (2011)**



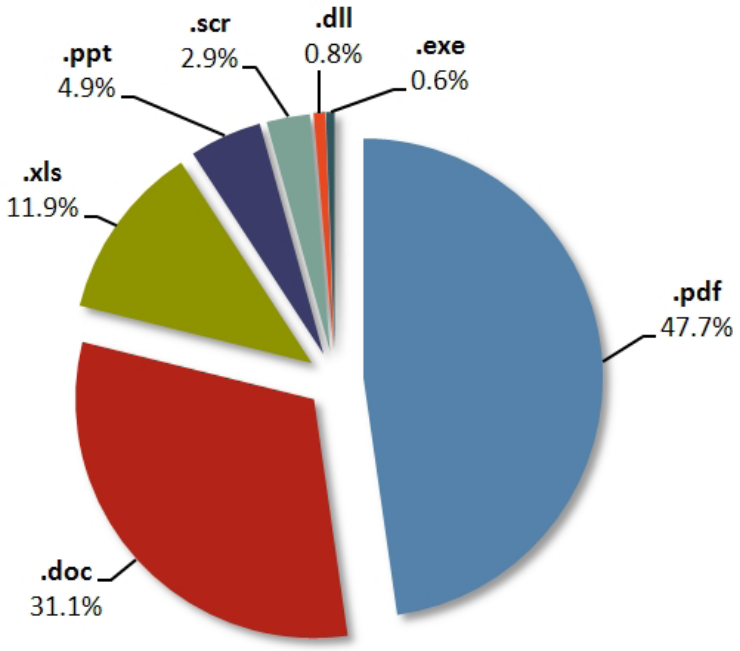

## The attachment

The sample email above contained a malicious PDF attachment; however, Taidoor doesn't confine itself to PDFs. Taidoor has been used in a wide variety of attachments, including malicious Microsoft PowerPoint, Word (.doc and .rtf file formats), and Excel files. Malicious executables and even DLLs (BID 47741) have been used as part of recent attacks. In these cases the malicious file is typically contained within an archive. In more recent attacks Word documents and PDFs have been the most popular attack vectors. However the malicious attachments constantly change, with new exploits appearing regularly.

Figure 7

**Popularity of attachment type**

**(.dll, .scr, and .exe files are typically contained within archive files)**




The malicious attachments have used a large set of vulnerabilities over the years, covering all main document formats. This clearly indicates that this group has both the focus and the intent to keep these exploits relevant and up-to-date. The group is clearly not afraid to try out new exploits. The number utilized is remarkable.

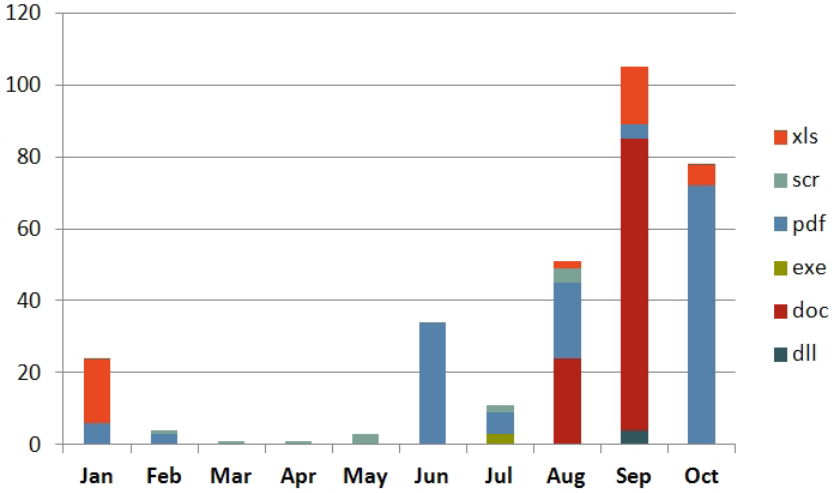
- Microsoft PowerPoint Malformed Record Remote Code Execution Vulnerability (BID 18382)
- Microsoft Word Malformed Data Structures Code Execution Vulnerability (BID 21518)
- Adobe Acrobat and Reader Multiple Arbitrary Code Execution and Security Vulnerabilities (BID 27641)
- Microsoft PowerPoint Sound Data (CVE-2009-1129) Remote Code Execution Vulnerability (BID 34839)
- Adobe Reader and Acrobat 'newplayer()' JavaScript Method Remote Code Execution Vulnerability (BID 37331)
- Microsoft Excel 'FEATHEADER' Record Remote Code Execution Vulnerability (BID 36945)
- Adobe Flash Player CVE-2011-0611 'SWF' File Remote Memory Corruption Vulnerability (BID 47314)
- Multiple Microsoft Products DLL Loading Arbitrary Code Execution Vulnerability (BID 47741)
- Adobe Acrobat and Reader CVE-2011-2100 DLL Loading Arbitrary Code Execution Vulnerability (BID 48252)

It is worth noting again that none of the vulnerabilities used by Taidoor are zero-day exploits. Taidoor simply leverages publicly disclosed security bugs in popular applications and therefore relies on the target or targets to be running unpatched software.

Figure 8 shows the email attachment types chosen by attackers in 2011.

Figure 8

**Breakdown of malicious attachment types for 2011**
**(.dll, .scr, and .exe files are typically contained within archive files)**

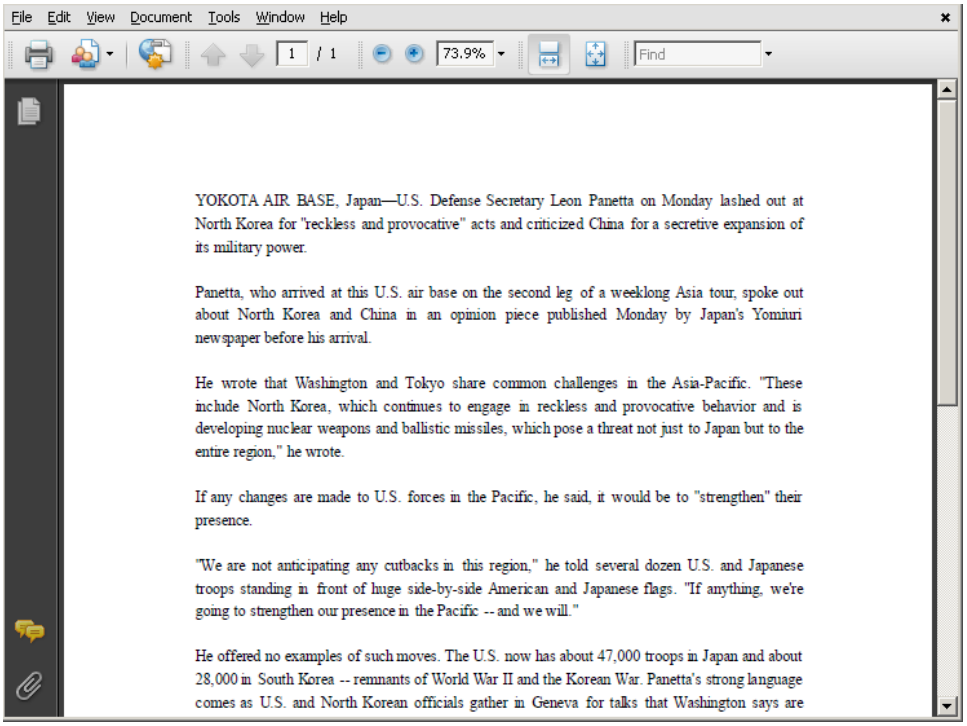



We can see a marked increase in the use of vulnerable Word documents in the run-up to the US-Taiwan Defense Industry Conference in September 2011. The group probably found more success with the Word exploit for this period of the campaign. However they switch to older vulnerabilities if the new ones are proving less successful, which was the case for BID 47741.

The goal of the email is to entice the recipient into opening the malicious attachment. The goal of the attachment is to surreptitiously copy the embedded Trojan onto the user's computer and launch it without drawing attention to the fact that the user has just been compromised.

Figure 9

**Taidoor PDF attachment**




Taking the attachment in the previous targeted email, let's examine what happens if the malicious document is opened. The PDF is exploiting BID 47314, a vulnerability in Adobe Reader that leads to code execution of the attacker's choosing. This code decrypts, extracts, and executes the embedded Taidoor dropper. It also extracts and presents the clean PDF in figure 9, so as not to alarm the user to any unusual behavior.

The content in the PDF was scraped from an Associated Press article that started to appear on most major news feeds the very day the email was sent: October 24, 2011.

## *The dropper*

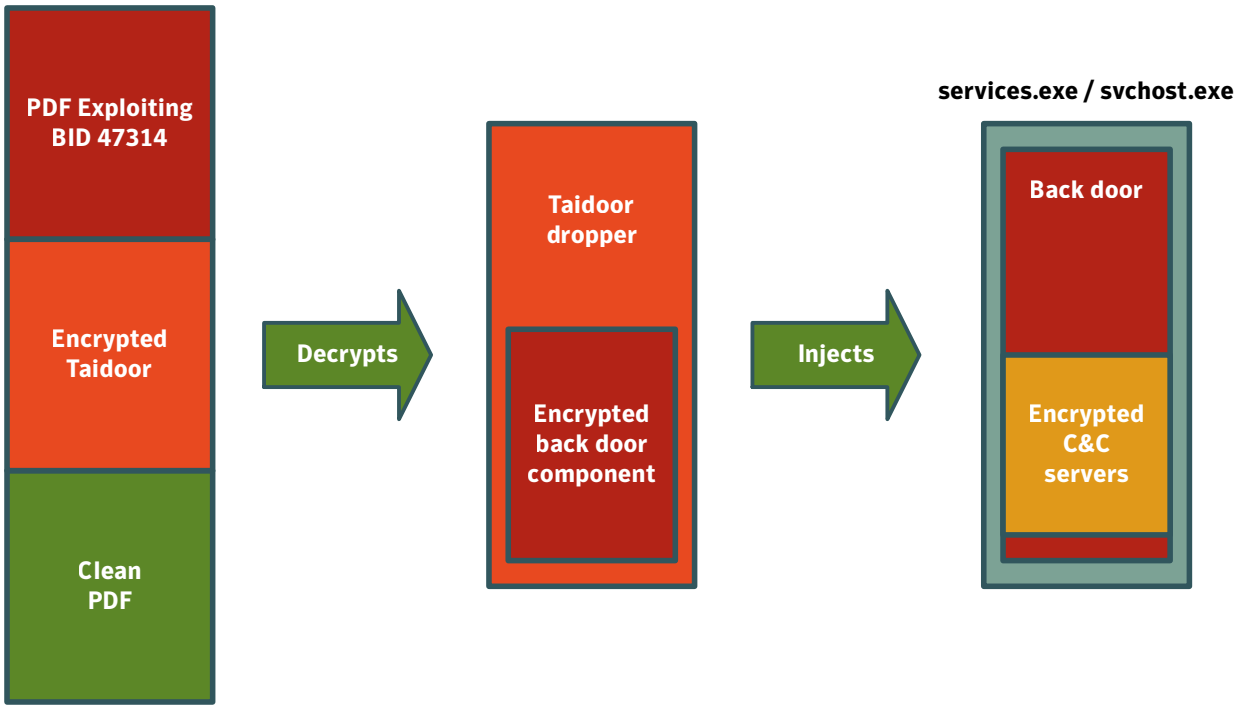
Once the user has opened the malicious attachment the infection process is set into motion. Once the dropper is created in the file system, it is executed. It starts one of the following legitimate processes, after which it will replace this clean, in-memory image with the malicious back door component:

- services.exe
- svchost.exe

The back door component is normally present in the form of either an encrypted resource entry or as an encrypted binary array within the code section of the dropper. Figure 10 helps illustrate the layout of each file and the steps taken once the malicious attachment is launched.

Figure 10

**Taidoor file layout**




## *The payload*

The final payload is now in place. This is the back door component that communicates with the C&C server. The back door stores configuration information in the ".data" section which is setup by the attackers. This configuration information contains up to three C&C servers, up to three ports per server, and a default sleep interval. Once the back door is successfully installed on the system it will attempt to communicate with the C&C server using the HTTP protocol. Let us examine this in more detail.

## *Command-and-Control server*

### Protocol

Trojan.Taidoor communicates with the controlling server using the HTTP protocol with requests using the following format and detailed in table 1:

```
http://[C&C _ SERVER]:[PORT]/[RANDOM].php?id=[RAND][ID][OPTIONAL]
```

Table 1

**HTTP communication format**

| Variable | Description |
|---|---|
| [C&C_SERVER] | Up to three configurable C&C servers |
| [PORT] | Up to three configurable ports |
| [RANDOM_PATH] | Five random, lower-case letters. Recreated every time Taidoor initializes or fails to contact its configured servers. |
| [RAND] | Six-decimal, random number recreated for each request. The values are between 0-32767 (limited by RAND_MAX). |
| [ID] | Twelve characters derived from MAC address of the compromised computer. |
| [OPTIONAL] | Is "&ext=[FILENAME]", which may be present in requests, related to specific commands. |

When the message body is present in a request or response, it is encrypted using RC4. The RC4 key is simply a string representation of the compromised computer's adapter address (e.g. 01-27-89-AB-CD-EF). This means that the C&C server must be able to compute the RC4 key from the [ID] present in the HTTP request. Because such an [ID] is unique for each computer it could also be used by the controlling server for tracking purposes.

Trojan.Taidoor uses an algorithm when generating the ID field. First it obtains a string representation of the adapter address. A default value of "01-01-01-01-01-01" is used if it fails to obtain the adapter address. It strips the "-" characters from the string and then increments the value of each character. If it encounters '9' this value will be set to '0'. For example "01-27-89-AB-CD-EF" would convert to "123890BCDEFG"

Trojan.Taidoor periodically queries the C&C server for commands by sending GET requests with an empty message body. This period is configurable by the attacker and is stored, along with the C&C information, in the data section. Values for this sleep interval has been seen as low as two and as high as 600 seconds. The server responds with RC4-encrypted commands in the message body. The first byte of decrypted message body is the command ID, followed by an optional parameter. Table 2 details the commands available to the attacker.

Table 2

### Taidoor C&C commands

| ID* | Format | Command | Details |
|---|---|---|---|
| 2 | DWORD | Set Delay | Period in milliseconds for the sleep time in between requests. |
| 3 | STRING | Execute Command | Command to be executed. The generated output is collected in a temporary file and sent in a separate POST request. The POST request does not contain any indication about the corresponding command.** |
| 4 | STRING | Download and Execute | The URL location to download a file, which is saved to the %Temp% folder and executed. |
| 5 | STRING | Download File | Path of the file to be created. The content of the file is downloaded using a separate GET request with [OPTIONAL] set to "&ext=[BASE64_ENCODED_FILENAME]" |
| 7 | STRING | Upload File | Parameter is the path of the file to be uploaded. Content of the file is uploaded using separate POST request with [OPTIONAL] set to "&ext=[BASE64_ENCODED_FILENAME]" |

*All other commands are IDs treated as pings. **A strong indicator this back door is designed for human operators.

## Live interactive session

Our honeypots were able to capture some live, interactive sessions of the attackers in action. Table 3 presents logs of the activities of an attacker during one of these sessions on September 16, 2011. This is the first 60 seconds of the attacker in action, logged from 02:23:06 UTC.

Table 3

### Example of attacker activities through back door

| Timeline | Commands Received |
|---|---|
| 2011-09-16 02:23:06 UTC: RECV | [Ping] |
| 2011-09-16 02:23:15 UTC: RECV | [Set sleep interval to 1 second] |
| 2011-09-16 02:23:23 UTC: RECV | cmd /c net start |
| 2011-09-16 02:23:31 UTC: RECV | cmd /c dir c:\docume~1\ |
| 2011-09-16 02:23:52 UTC: RECV | cmd /c dir "c:\docume~1\<CurrentUser>\recent" /od |
| 2011-09-16 02:24:00 UTC: RECV | cmd /c dir c:\progra~1\ |
| 2011-09-16 02:24:12 UTC: RECV | cmd /c dir "c:\docume~1\<CurrentUser>\desktop" /od |
| 2011-09-16 02:24:25 UTC: RECV | cmd /c netstat –n |
| 2011-09-16 02:24:32 UTC: RECV | cmd /c net use |

Before the attacker starts an interactive command shell, Taidoor is instructed to reduce the sleep interval to one second. This improves Trojan.Taidoor's response time to subsequent commands sent by the attacker. Over the next 60 seconds the attacker will look for the following information about the compromised host:

- Currently running services.
- Contents of the "Documents and Settings" folder: What users are on the system?
- Contents of the "Recently Used Documents" item.
- Contents of the "Program Files" folder: What software is installed?
- Contents of the Desktop.
- A list of the currently open TCP/IP connections.
- A list of available network connections.

The attacker initially searches for documents and users of interest on the compromised computer. If the user is not a target of interest, the attacker can search for other computers of higher value on the network using the shell or by downloading additional tools on to the compromised computer in order to assist in traversing the network. It is worth noting that this is not automated, but that an actual attacker sitting at the other end, typing these commands.

## Hacked third-party servers

Some basic reconnaissance was done on the C&C servers used by Trojan.Taidoor. Many of the Taidoor C&C servers probed appeared to be compromised third-party servers, as opposed to leased servers commonly used as part of a C&C infrastructure. The servers are probably used in an effort to hide the true location of the attacker and they simply forward the malicious communication to another location. The highest concentrations of Trojan.Taidoor C&C servers are in the US and Taiwan, as shown in figure 11.

Simple fingerprinting on these computers revealed that they were consistently running a number of services. It is probable that such services were vulnerable to basic attacks, as several of the C&C servers had been compromised by third-party hackers prior to their use by the Taidoor attackers. The screenshot in figure 12 is from a cached Web page defacement of one particular server. Such defacements are typically performed by attackers with limited skill sets. This implies that the services on the computer were trivial to compromise or that it was poorly maintained, with little or no patching.

Figure 11

### C&C servers by country

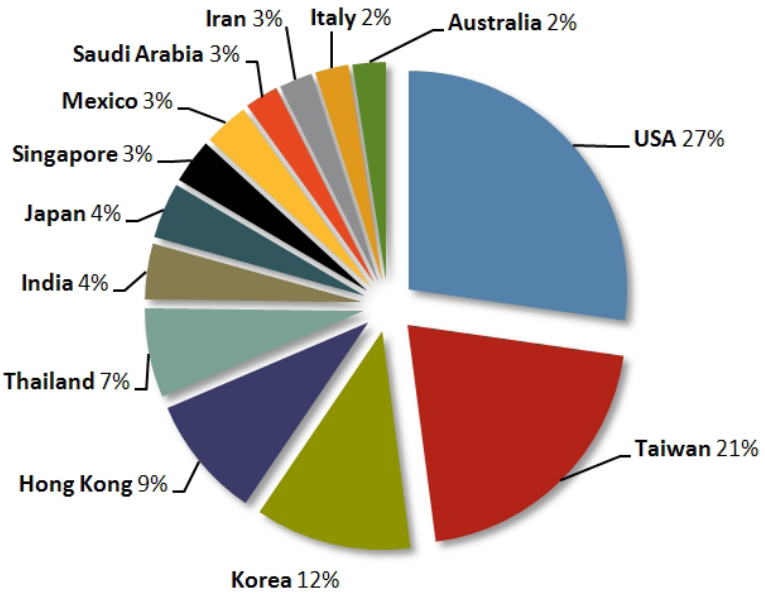



Figure 12

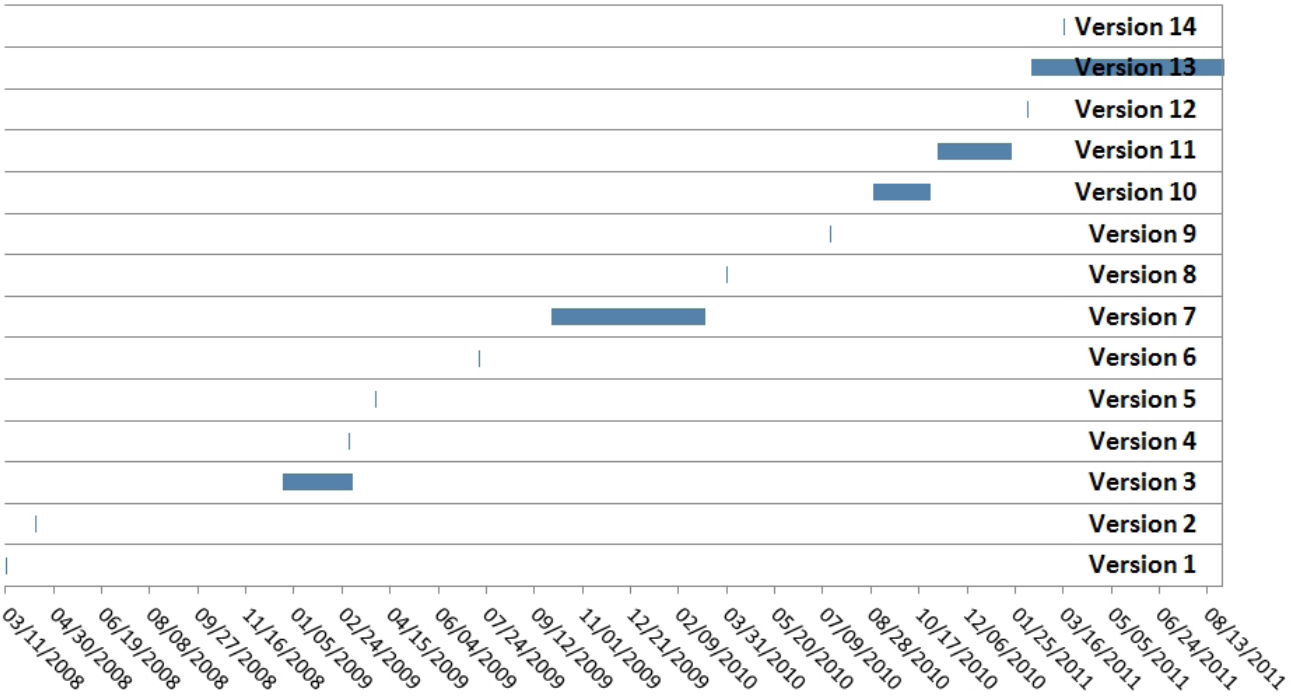
### Previously hacked C&C server, as shown in a publicly accessible website

## Variants

To date we have seen at least 14 different variants of Trojan.Taidoor. The earliest compilation date is March 11, 2008. Trojan.Taidoor doesn't track version information itself. However, examining modifications to the compiled code section of the back door component over time allows for version tracking. Most of the distinct PE images share identical code sections, and only the details of the C&C servers in the data section differ between attacks. Some versions have seen extensive use, while others have been seen far less frequently, and for very brief periods of time. Figure 13 tracks the modifications over time.

Figure 13

**Taidoor versioning 2008-2011, based on PE code section similarity**

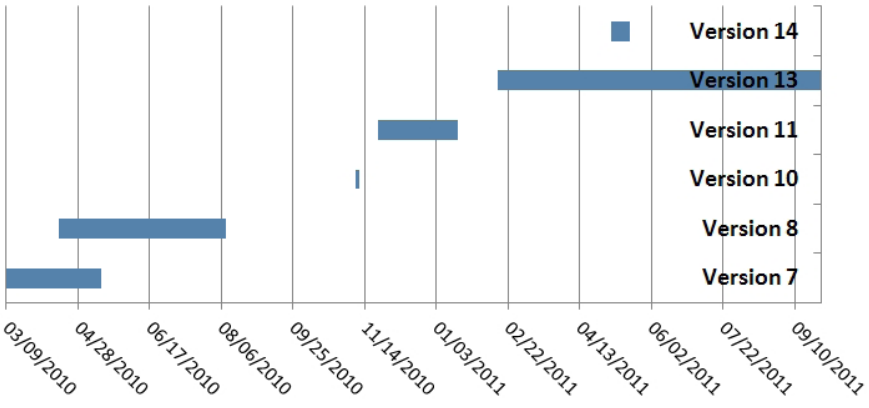



This chart shows the date and timestamp of the compiled files with the identified version of the back door. Version 1 was used on March 11, 2008 and version 13 was used from March 16, 2011 up until August 13, 2011. There is very little overlap in use of the back doors between versions. This indicates that a single entity is responsible for development. If the source code of the threat was shared amongst multiple entities, there would be a much larger number of versions, and their use would overlap more. Several variants were used for an extended period of time, the most widely being version 13—the version used to target think tanks.

The chart in figure 14 compares the date of emails, instead of compile time, with the back door version. There is some degree of overlap, but the majority of usage is again distinct between versions. This reinforces the assumption that a single entity is in control of the source code.

Figure 14

**Taidoor version distribution in emails (2010-2011)**



## Patterns of activity

Some interesting patterns of behavior were observed during the interactive sessions with the C&C servers. For most of the day the servers would issue a connection reset or return an HTTP 404 (Not Found) message. These servers then "woke up" for certain periods of the day. These times typically occurred between 1:00 and 8:00 UTC. This was the case for the majority of successful C&C interactions logged, indicating some regular pattern of activity for these attackers.

## Attacker profile

Attributing the Taidoor attacks to a particular party is not likely, but there are a number of factors in the Trojan.Taidoor attacks that may offer an indication as to the source of the threat.

Taidoor has been maintained with new versions and new exploits relatively consistently from 2008, up to the end of 2011. Such consistency is possible for an individual working full-time. However, the additional work required to maintain the infrastructure behind Taidoor—hacking C&C servers, investigating targets in order to tailor attacks, and then actually spreading within a network once it is compromised—is beyond the capabilities of an individual. A number of people are clearly involved. This is likely an organized group of individuals who have a broad range of skills and a reasonable level of hacking ability, given the number of compromised C&C servers. It is quite possible that individuals within the group are given particular roles for each stage of the operation, since this work would divide up easily.

However, although the group is active and must consist of several people, their resources are limited. No zero-day exploits have been found associated with Taidoor; only previously published ones. The group does not have the skills to develop a zero-day, nor the funds to obtain them. The C&C servers are hacked, not purchased. Although hacking of the C&C servers does offer a level of anonymity, it is also an unreliable method of control. The hacked C&C servers may be discovered by the owner of the compromised computer and shut down at any time. As such, it is unlikely that the group has access to substantial funds.

Table 4
**Time zones**

| Region | Local Time |
|---|---|
| Japan | 10:00am—5:00pm |
| Taiwan | 9:00am—4:00pm |
| China (Beijing) | 9:00am—4:00pm |
| India | 6:30am—1:30pm |
| Russia (Moscow) | 5:00am—12:00pm |
| UK | 1:00am—8:00am |
| US (Eastern) | 8:00pm—3:00am |
| US (Pacific) | 5:00pm—12:00pm |

The times of operation of the attackers may be an indicator as to their location. As described earlier, interactions with the C&C servers occurred primarily between 1:00 and 8:00 UTC. Table 4 shows these times for various countries around the world.

In addition, the group can write competent emails in both English and Traditional Chinese.

The motivations of the group are difficult to determine. Clearly there was a major shift in the group in 2011, judging from the change in targets. Initially starting with a wide range of disparate targets, the group began to focus almost exclusively on one particular type of target—policy think tanks—and in relation to one particular topic: US-Taiwanese dealings. The nature of the topic is something that would be of most interest to parties involved in the discussions, parties who may be affected by the discussions such as private industry looking for a competitive advantage or nation states, or possibly hackers looking to expose confidential information on such discussions for ideology or fame.

# Conclusion

Trojan.Taidoor's attack methodology follows a consistent pattern associated with targeted attacks: a crafted email with a malicious attachment. It's clear that this group is highly motivated and persistent, which is evident from the longevity of the Taidoor campaign and the variation in targeted organizations. These attacks are ongoing, so we will continue to provide Symantec customers with cutting-edge solutions to protect themselves against both current and future Taidoor attacks.

# Symantec protection

Many different Symantec protection technologies play a role in defending against this threat, including:

## *File-based protection (traditional antivirus)*

Traditional antivirus protection is designed to detect and block malicious files and is effective against files associated with this attack.

- Trojan.Taidoor
- Trojan Horse
- Trojan.Pidief

## *Network-based protection (IPS)*

Network-based protection in Symantec Endpoint Protection can help protect against unauthorized network activities conducted by malware threats or intrusion attempts. Symantec Critical System Protection and Symantec Web Gateway can block access to the C&C servers.

## *Behavior-based protection*

Symantec products, like Symantec Endpoint Protection, with behavior-based detection technology can detect and block previously unknown threats from executing, including those associated with this attack. Files detected by this technology will be reported as Bloodhound.Sonar.9.

## *Reputation-based protection (Insight)*

Symantec Download Insight, found in Symantec Endpoint Protection and Symantec Web Gateway, can proactively detect and block files associated with this attack using Symantec's extensive file reputation database. Files detected by this technology will be reported as WS.Reputation.1.

## *Email-based protection*

The Skeptic heuristic engine in Symantec MessageLabs Email Security.cloud can proactively detect and block emails that are associated with this attack.

## *Other protection*

**Application and Device Control** — Symantec Endpoint Protection users can enable this feature to detect and block potentially malicious files from executing.

Symantec Critical System Protection can also prevent unauthorized applications from running.

IT Management Suite provides comprehensive software and patch management. Critical System Protection can protect servers against vulnerabilities between patching cycles.

# Appendix

## *Sample files*

The following files are a representative sample of those used in the Taidoor attacks.

Table 5

### Sample MD5s

| MD5 | Type | Target Region | Date |
|---|---|---|---|
| 50c3de93fc5ee424b22c85c5132febe9 | scr | USA | 18/05/2011 |
| d6a23c475907336d5bf0f11111e62d44 | scr | USA | 17/05/2011 |
| e0255a0bbd6d067bc5d844819fee4ec6 | pdf | USA | 20/06/2011 |
| 28f7eca368fd18b0a7c321927281e387 | pdf | USA | 23/06/2011 |
| 8e3d7fcfa89307c0d3b7951bd36b3513 | pdf | USA | 22/06/2011 |
| c2e05204221d08d09da1e3315b1b77a1 | pdf | USA | 24/06/2011 |
| e8390f9960e1acb2ca474a05fdbd1feb | pdf | USA | 24/06/2011 |
| 02a1a396e3607a5d2f8ece9fc5d65427 | pdf | USA | 26/06/2011 |
| a41186ac5bef467204c721e824b550cf | pdf | USA | 27/06/2011 |
| 46c6da9be372f64ef17205fd3649fa80 | pdf | USA | 27/06/2011 |
| 4c874b2bf0a5ee4bdebf7933af0d66b1 | pdf | USA | 29/06/2011 |
| 002cec5517c17ffac2e37908fcab45ff | pdf | USA | 28/06/2011 |
| 207e770f53bf1ea6bfb8068614ad0f70 | pdf | USA | 29/06/2011 |
| d49024573cb0763c1b33259ddbf4dd72 | exe | USA | 05/07/2011 |
| e05b832dc588b1055d64daa7dfd03eb7 | scr | USA | 06/07/2011 |
| f8c670662bc2043664269671fb9a2288 | pdf | USA | 07/07/2011 |
| 18471c628a29e602ec136c52f54f1f83 | scr | USA | 08/08/2011 |
| 34d333a18b5b8b75cad46601163469ce | scr | USA | 04/08/2011 |
| ec8a87a00b874899839b03479b3d7c5c | pdf | USA | 10/08/2011 |
| c645169173c835c17abb0bde59b594bb | xls | USA | 05/08/2011 |
| 60d519e00f92b5d635f95f94c2afdc68 | doc | USA | 16/08/2011 |
| 804011277338eb3c372ae4b520124114 | scr | USA | 21/08/2011 |
| b817c2335e520312d0ae78c309d73d22 | doc | UK | 15/08/2011 |
| 50a713a00c8468f7f033e79a97f6b584 | pdf | USA | 30/08/2011 |
| d642d3dde179ce5be63244c0f6534259 | pdf | USA | 31/08/2011 |
| 8810f26133d5586477c8552356fc4439 | doc | USA | 02/09/2011 |
| 527a6cd21f0514ef5baa160b6e6b1482 | doc | USA | 30/08/2011 |
| 90ed80f18b05a52bf2801c7638b371e3 | pdf | USA | 06/09/2011 |
| e8291553bd947082476a123c64ac8e82 | doc | USA | 14/09/2011 |
| b25c3e81cdef882f532ba78a8fdcd7ca | pdf | USA | 14/09/2011 |
| 60a8524d36d8a5e70d853bf3212616c5 | doc | USA | 16/09/2011 |
| b8c89fdc109db7522faf2180648dad2f | doc | USA | 15/09/2011 |
| 4859ba249a200d34189166abfd57a3dd | doc | USA | 09/09/2011 |
| 309ac58218250726b3588d61738d5b21 | pdf | USA | 29/09/2011 |
| 90c88267efd63fd8e22fb0809be372bc | dll | USA | 20/09/2011 |
| 6491873b351b8d0deccd6e30211ce137 | pdf | USA | 14/10/2011 |
| 2a0dcb1915c0465949e7aecfb06f47ea | pdf | USA | 18/10/2011 |
| 08cdc6213d63ea85fbccd335579caec4 | pdf | USA | 20/10/2011 |
| c898abcea6eaaa3e1795322d02e95d7e | pdf | USA | 24/10/2011 |
| de095f05913928cf58a27f27c5bf8605 | pdf | USA | 25/10/2011 |
| 8c57fe2c1112d2122bfd09f5f91f7154 | xls | USA | 29/10/2011 |
| b4cb1b1182ea0b616ed6702a2b25fac2 | pdf | USA | 01/11/2011 |
| 86730a9bc3ab99503322eda6115c1096 | pdf | USA | 03/11/2011 |

# Recommendations

## Update antivirus definitions

Ensure that your antivirus software has up-to-date antivirus definitions and ensure that your product has the auto-protect feature enabled. You can obtain the latest definitions through LiveUpdate or download the latest definition files from our website.

## Apply patches for the following vulnerabilities

Symantec recommends that users apply patches for the following vulnerabilities to help protect against this and similar attacks:

- Microsoft PowerPoint Malformed Record Remote Code Execution Vulnerability (BID 18382)
- Microsoft Word Malformed Data Structures Code Execution Vulnerability (BID 21518)
- Adobe Acrobat and Reader Multiple Arbitrary Code Execution and Security Vulnerabilities (BID 27641)
- Microsoft PowerPoint Sound Data (CVE-2009-1129) Remote Code Execution Vulnerability (BID 34839)
- Adobe Reader and Acrobat 'newplayer()' JavaScript Method Remote Code Execution Vulnerability (BID 37331
- Microsoft Excel 'FEATHEADER' Record Remote Code Execution Vulnerability (BID 36945)
- Adobe Flash Player CVE-2011-0611 'SWF' File Remote Memory Corruption Vulnerability (BID 47314)
- Multiple Microsoft Products DLL Loading Arbitrary Code Execution Vulnerability (BID 47741)
- Adobe Acrobat and Reader CVE-2011-2100 DLL Loading Arbitrary Code Execution Vulnerability (BID 48252)

## Prevent back door communications

Block access to the following command-and-control server IP addresses that are associated with this attack.

Table 6
**C&C servers**

| IP | Country | ASN | Registrar |
|---|---|---|---|
| 110.142.12.95 | Australia | 1221 | apnic |
| 203.45.204.239 | Australia | 1221 | apnic |
| 220.245.107.203 | Australia | 7545 | apnic |
| 193.170.111.210 | Austria | 1853 | ripencc |
| 88.117.175.114 | Austria | 8447 | ripencc |
| 81.21.80.40 | Azerbaijan | 39280 | ripencc |
| 203.188.255.117 | Bangladesh | 9832 | apnic |
| 24.79.164.206 | Canada | 6327 | arin |
| 213.41.162.198 | France | 13193 | ripencc |
| 62.38.148.117 | Greece | 3329 | ripencc |
| 212.205.207.42 | Greece | 6799 | ripencc |
| 202.82.162.61 | Hong Kong | 4515 | apnic |
| 218.103.88.197 | Hong Kong | 4515 | apnic |
| 220.246.17.40 | Hong Kong | 4515 | apnic |
| 220.246.5.52 | Hong Kong | 4515 | apnic |
| 219.76.232.33 | Hong Kong | 4515 | apnic |
| 202.65.218.205 | Hong Kong | 9584 | apnic |
| 202.60.254.253 | Hong Kong | 9925 | apnic |
| 203.198.133.15 | Hong Kong | 4760 | apnic |
| 203.198.142.209 | Hong Kong | 4760 | apnic |
| 210.3.235.154 | Hong Kong | 9304 | apnic |
| 210.245.194.241 | Hong Kong | 17444 | apnic |
| 122.160.96.111 | India | 24560 | apnic |

Table 6

## C&C servers

| IP | Country | ASN | Registrar |
|---|---|---|---|
| 61.12.21.84 | India | 17820 | apnic |
| 202.56.122.100 | India | 10077 | apnic |
| 203.92.33.98 | India | 10029 | apnic |
| 59.162.253.38 | India | 17908 | apnic |
| 202.155.109.228 | Indonesia | 4795 | apnic |
| 217.218.246.18 | Iran | 12880 | ripencc |
| 78.39.115.35 | Iran | 12880 | ripencc |
| 78.39.236.6 | Iran | 12880 | ripencc |
| 192.116.205.100 | Israel | 5486 | ripencc |
| 2.116.180.66 | Italy | 3269 | ripencc |
| 83.149.128.190 | Italy | 31319 | ripencc |
| 2.229.10.5 | Italy | 12874 | ripencc |
| 210.20.35.2 | Japan | 9824 | apnic |
| 202.251.249.136 | Japan | 4686 | apnic |
| 61.200.43.129 | Japan | 17676 | apnic |
| 203.179.145.2 | Japan | 4716 | apnic |
| 219.123.85.187 | Japan | 17506 | apnic |
| 61.107.131.147 | South Korea | 9457 | apnic |
| 61.107.29.111 | South Korea | 9457 | apnic |
| 211.177.131.120 | South Korea | 9318 | apnic |
| 211.47.189.41 | South Korea | 38661 | apnic |
| 203.234.132.173 | South Korea | 9979 | apnic |
| 222.101.218.86 | South Korea | 4766 | apnic |
| 61.80.90.113 | South Korea | 4766 | apnic |
| 211.169.248.159 | South Korea | 3786 | apnic |
| 211.233.62.146 | South Korea | 3786 | apnic |
| 211.233.62.147 | South Korea | 3786 | apnic |
| 211.233.62.148 | South Korea | 3786 | apnic |
| 211.234.117.132 | South Korea | 3786 | apnic |
| 211.234.117.185 | South Korea | 3786 | apnic |
| 211.254.153.122 | South Korea | 3786 | apnic |
| 218.208.203.106 | Malaysia | 4788 | apnic |
| 207.248.250.60 | Mexico | 11172 | lacnic |
| 201.158.139.83 | Mexico | 14000 | lacnic |
| 201.175.42.79 | Mexico | 22908 | lacnic |
| 201.116.58.243 | Mexico | 8151 | lacnic |
| 62.231.246.150 | Oman | 28885 | ripencc |
| 203.81.229.89 | Pakistan | 38616 | apnic |
| 200.115.173.102 | Panama | 27956 | lacnic |
| 203.215.80.180 | Philippines | 6648 | apnic |
| 212.33.79.176 | Poland | 8865 | ripencc |
| 62.89.115.229 | Poland | 12968 | ripencc |
| 80.96.120.22 | Romania | 2614 | ripencc |
| 212.76.68.141 | Saudi Arabia | 41176 | ripencc |
| 212.76.68.74 | Saudi Arabia | 41176 | ripencc |
| 212.11.189.124 | Saudi Arabia | 42428 | ripencc |
| 203.126.74.13 | Singapore | 3758 | apnic |

Table 6

## C&C servers

| IP | Country | ASN | Registrar |
|---|---|---|---|
| 58.185.2.34 | Singapore | 3758 | apnic |
| 202.172.37.145 | Singapore | 17547 | apnic |
| 203.116.203.67 | Singapore | 4657 | apnic |
| 213.81.217.7 | Slovakia | 6855 | ripencc |
| 217.125.43.149 | Spain | 3352 | ripencc |
| 203.64.22.11 | Taiwan | 1659 | apnic |
| 202.39.212.245 | Taiwan | 3462 | apnic |
| 210.242.240.218 | Taiwan | 3462 | apnic |
| 211.20.65.188 | Taiwan | 3462 | apnic |
| 211.21.156.15 | Taiwan | 3462 | apnic |
| 211.22.75.68 | Taiwan | 3462 | apnic |
| 211.72.181.61 | Taiwan | 3462 | apnic |
| 211.72.191.145 | Taiwan | 3462 | apnic |
| 211.72.80.242 | Taiwan | 3462 | apnic |
| 220.130.219.242 | Taiwan | 3462 | apnic |
| 220.133.170.33 | Taiwan | 3462 | apnic |
| 59.120.16.115 | Taiwan | 3462 | apnic |
| 59.120.54.79 | Taiwan | 3462 | apnic |
| 60.248.17.81 | Taiwan | 3462 | apnic |
| 60.249.219.82 | Taiwan | 3462 | apnic |
| 60.251.220.144 | Taiwan | 3462 | apnic |
| 61.218.83.3 | Taiwan | 3462 | apnic |
| 61.220.129.45 | Taiwan | 3462 | apnic |
| 61.220.42.130 | Taiwan | 3462 | apnic |
| 61.221.152.191 | Taiwan | 3462 | apnic |
| 61.221.233.99 | Taiwan | 3462 | apnic |
| 61.222.205.180 | Taiwan | 3462 | apnic |
| 219.84.143.15 | Taiwan | 18182 | apnic |
| 219.87.26.129 | Taiwan | 9924 | apnic |
| 202.3.167.6 | Taiwan | 9831 | apnic |
| 61.19.124.116 | Thailand | 9931 | apnic |
| 61.7.150.118 | Thailand | 131090 | apnic |
| 61.7.158.11 | Thailand | 131090 | apnic |
| 58.137.157.163 | Thailand | 4750 | apnic |
| 58.137.163.166 | Thailand | 4750 | apnic |
| 202.60.203.229 | Thailand | 17887 | apnic |
| 202.183.233.66 | Thailand | 10227 | apnic |
| 113.53.236.67 | Thailand | 9737 | apnic |
| 213.42.74.85 | UAE | 5384 | ripencc |
| 64.118.87.250 | United States | 32742 | arin |
| 98.189.155.145 | United States | 22773 | arin |
| 65.115.139.158 | United States | 209 | arin |
| 209.156.150.178 | United States | 1785 | arin |
| 12.43.95.117 | United States | 7018 | arin |
| 168.8.80.21 | United States | 6389 | arin |
| 68.195.237.234 | United States | 6128 | arin |
| 64.39.73.148 | United States | 27521 | arin |

Table 6

## C&C servers

| IP | Country | ASN | Registrar |
|---|---|---|---|
| 68.82.45.168 | United States | 7922 | arin |
| 65.214.70.122 | United States | 13388 | arin |
| 76.5.157.172 | United States | 13787 | arin |
| 208.40.105.162 | United States | 2707 | arin |
| 184.11.128.172 | United States | 5650 | arin |
| 65.23.153.148 | United States | 22822 | arin |
| 65.23.153.178 | United States | 22822 | arin |
| 216.139.109.156 | United States | 33165 | arin |
| 208.57.226.46 | United States | 18687 | arin |
| 209.123.166.170 | United States | 8001 | arin |
| 64.34.60.218 | United States | 13768 | arin |
| 108.77.146.124 | United States | 7132 | arin |
| 64.167.26.66 | United States | 7132 | arin |
| 65.68.51.49 | United States | 7132 | arin |
| 99.1.23.71 | United States | 7132 | arin |
| 70.63.209.63 | United States | 11426 | arin |
| 216.27.242.38 | United States | 22343 | arin |
| 216.27.242.41 | United States | 22343 | arin |
| 72.9.221.133 | United States | 22343 | arin |
| 174.123.19.84 | United States | 21844 | arin |
| 65.246.9.27 | United States | 701 | arin |
| 65.249.138.102 | United States | 701 | arin |
| 71.246.244.139 | United States | 19262 | arin |
| 96.229.98.180 | United States | 19262 | arin |
| 206.111.214.29 | United States | 2828 | arin |

Symantec
Security Response



**About Symantec**

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Moutain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

**About the authors**

Stephen Doherty is a Security Response Manager and Piotr Krysiuk is a Senior Software Engineer, located in Dublin, Ireland.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com