Trend Micro Incorporated
Research Paper
2012

The Taidoor Campaign

AN IN-DEPTH ANALYSIS

By: Trend Micro Threat Research Team

CONTENTS

Introduction

Taidoor malware, detected by Trend Micro as BKDR_SIMBOT variants, have been historically documented for their use in targeted attacks. Using techniques developed to match the network traffic Taidoor malware generate when communicating with a command-and-control (C&C) server, we were able to identify victims that these appeared to have compromised. All of the compromise victims we discovered were from Taiwan, the majority of which were government organizations.

Detection

Looking at threat intelligence derived from tracking advanced persistent threat (APT) campaigns over time, we were able to develop indicators of compromise primarily based on the network traffic generated by the malware used in the Taidoor campaign. Using data collected from the Trend Micro™ Smart Protection Network™, we are able to identify victims whose networks communicated with Taidoor C&C servers. While we are unable to determine the exact method by which any of the victims' networks were compromised, the information we collected did indicate which specific Taidoor malware samples contacted which C&C servers. We also obtained email samples associated with the delivery of the Taidoor malware samples. As such, we were able to provide an overview of the Taidoor campaign, including the attack vectors and malware the attackers used, and come up with a remediation strategy.

CONTEXT

The Taidoor attackers have been actively engaging in targeted attacks since at least March 4, 2009. Despite some exceptions, the Taidoor campaign often used Taiwanese IP addresses as C&C servers and email addresses to send out socially engineered emails with malware as attachments. One of the primary targets of the Taidoor campaign appeared to be the Taiwanese government. The attackers spoofed Taiwanese government email addresses to send out socially engineered emails in the Chinese language that typically leveraged Taiwan-themed issues. The attackers actively sent out malicious documents and maintained several IP addresses for command and control.

ATTACK VECTORS

The Taidoor campaign exploits a wide variety of vulnerabilities as attack vectors, old and new alike. Data from the early part of this year shows that the Taidoor attackers rampantly used malicious .DOC files to exploit a *Microsoft Common Controls* vulnerability, *CVE-2012-0158.*[1]

Historical data, on the other hand, shows that the Taidoor attackers also distributed emails with malicious .PDF file attachments that exploited *Adobe Reader, Acrobat,* or *Flash Player* vulnerabilities (e.g., *CVE-2009-4324,* [2] *CVE-2010-1297,*[3] *CVE-2010-2883,*[4] and *CVE-2011-0611).*[5] They also used malicious *Microsoft Excel* and *PowerPoint* files (e.g., *CVE-2011-1269*[6] and *CVE-2009-3129)*[7] to exploit old vulnerabilities in *Microsoft Office.*

Social Engineering Ploy

As part of their social engineering ploy, the Taidoor attackers attach a decoy document to their emails that, when opened, displays the contents of a legitimate document but executes a malicious payload in the background.

---

[1] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158
[2] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4324
[3] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1297
[4] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2883
[5] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0611
[6] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1269
[7] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3129

OPERATIONS

We were only able to gather a limited amount of information regarding the Taidoor attackers' activities after they have compromised a target. We did, however, find that the Taidoor malware allowed attackers to operate an interactive shell on compromised computers and to upload and download files. In order to determine the operational capabilities of the attackers behind the Taidoor campaign, we monitored a compromised honeypot. The attackers issued out some basic commands in an attempt to map out the extent of the network compromise but quickly realized that the honeypot was not an intended targeted and so promptly disabled the Taidoor malware running on it. This indicated that while Taidoor malware were more widely distributed compared with those tied to other targeted campaigns, the attackers could quickly assess their targets and distinguish these from inadvertently compromised computers and honeypots.

TECHNICAL INDICATORS

System Modifications

Opening a malicious document (i.e., .PDF, .DOC, .XLS, or .PPT file) allows the Taidoor malware to create two files in a user's *Temp* folder—*C:\Documents and Settings\[USER]\Local Settings\Temp.* The first file is typically a small executable file (i.e., 17.5KB) named *"[2 characters].tmp."* This is copied to another folder, usually *C:\Documents and Settings\[USER]\Local Settings,* and renamed to *"~dfds3.reg,"* which modifies the *Windows Registry* before being deleted.

Persistence Mechanism

The Taidoor malware uses the file, *~dfds3.reg,* to modify the *Windows Registry* in order to maintain persistence. While the names of the registry entries and the executable files may vary, these consistently modified the key, *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.*

Network Traffic

The Taidoor malware produces identifiable network traffic. These often directly accessed an IP address. Sometimes, however, certain samples made use of domain names for HTTP communication. In such a case, the GET and POST requests contained a URL path such as:

```
aaaaa.php?id=bbbbbbccccccccccc
```

"aaaaa" refers to five random characters that form a file name such as *"qfgkt.php,"* followed by "bbbbbb," six pseudorandomly generated characters that change for each connection. "ccccccccccc" refers to 12 characters that represent the compromised host's MAC address that is obfuscated using a custom algorithm. The compromised host's MAC address is communicated to the Taidoor C&C server this way because it is used as an RC4 encryption key to encrypt the subsequent network communication between the compromised host and the C&C server.

Malware Analysis

Arrival Vectors

The majority of the Taidoor malware samples we have seen in the wild were delivered via email. We also saw considerable variations among the email and IP addresses the senders used.

We listed down some of the emails that were sent via an IP address that also served as a C&C server below. This was one of the IP addresses that some compromised systems accessed. While we do not exactly know how the compromises occurred, we can, based on the attackers' method of operation, determine which email was the most likely attack vector.

- Sample email 1[8]
  - *From:* minaki.yang@yahoo.com
  - *Subject:* US-TAIWAN
  - *Date sent:* October 25, 2011
  - *Sender's IP address:* 60.249.219.82
  - *MD5 hash:* 97ff2338e568fc382d41c30c31f89720
- Sample email 2[9]
  - *From:* [redacted]@wpafb.af.mil
  - *Subject:* 20111012
  - *Sender's IP address:* 60.249.219.82
  - *MD5 hash:* 5fd848000d68f45271a0e1abd5844493
- Sample email 3[10]
  - *From:* 95273503@nccu.edu.tw
  - *Subject:* 稿件 如附檔，請收悉
  - *Sender's IP address:* 60.249.219.82
  - *MD5 hash:* 8406c1ae494add6e4f0e78b476fb4db0

Exploits, Payloads, and Decoy Documents

The shellcode in the exploit document is commonly encrypted. To successfully exploit a vulnerability, the shellcode is first decrypted. It then searches for the filehandle of the exploit document by comparing the file sizes of enumerated handles to a hardcoded file size that is supposed to be that of the exploit document.

Once the handle is found, two buffers are read from the exploit document, which contains the encrypted payload and an encrypted decoy document.

The payload is then decrypted and saved as a file in the *Windows* temporary directory. The payload is then commonly executed using the *WinExec* application programming interface (API).

After the payload is executed, the decoy document is decrypted and also saved in the *Windows* temporary directory. The decoy document is then opened in a new window of the exploited application to convince the victim that nothing is wrong with his/her system. The process that executed the exploit shellcode is then terminated.

Keen observation would also reveal that the document a victim opened was a decoy because its file name differs from the name of the original document that was exploited.

The main purpose of the specially crafted file attachments is to silently drop and install BKDR_SIMBOT variants in the target's computer.[11] These BKDR_SIMBOT variants include BKDR_SIMBOT.SMXA and BKDR_SIMBOT.SME, the generic Trend Micro detection names for SIMBOT malware.

In other instances, the binary poses as an *Adobe Flash Player* installer or uninstaller with a file size of 17,925 bytes. The file was written using Borland's *Delphi,* compiled on a machine whose default language was set to Chinese (Simplified), and did not use any known binary packer.

---

[8] http://targetedemailattacks.tumblr.com/post/12137336947/fake-excel-from-ibm111

[9] http://targetedemailattacks.tumblr.com/post/11377987600/malicious-excel

[10] http://contagiodump.blogspot.com/2011/10/sep-28-cve-2010-3333-manuscript-with.html

[11] http://about-threats.trendmicro.com/malware.aspx?language=us&name=BKDR_SIMBOT.SMXA

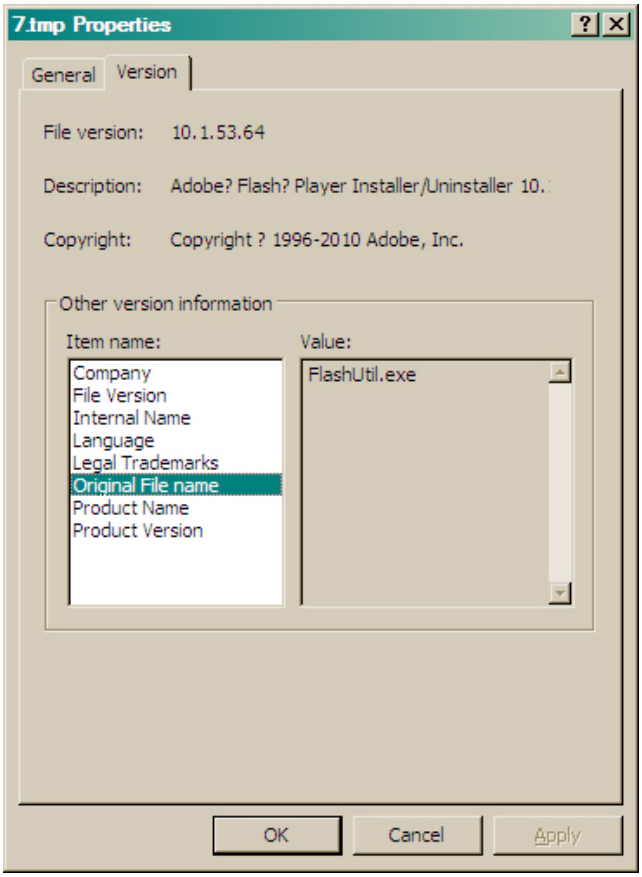

Figure 1. *File properties of the .TMP of the malicious executable file*

The main purpose of the dropped binary file is to install an RC4-encrypted executable file, specifically in the *.data* segment, in the memory space of a known *Windows Service Process.* If the registry, *HKLM|SOFTWARE|McAfee,* is found in the target's machine, the malware injects the executable file in the *services.exe* process. If not, it injects the executable file in *svchost.exe.*

The executable file is written using *C++* and has a file size of about 11,776 bytes. It is not protected nor packed using any known binary protector or packer and has a pretty straightforward code. The code seeks out inactive services and pseudorandomly chooses one, which it then tries to kill. If successful, it uses the service's name as file name for the copy created in the victim's *Temp* folder then creates an autorun registry entry for the binary. If not, "WinHttp" is prepended to the service's name.

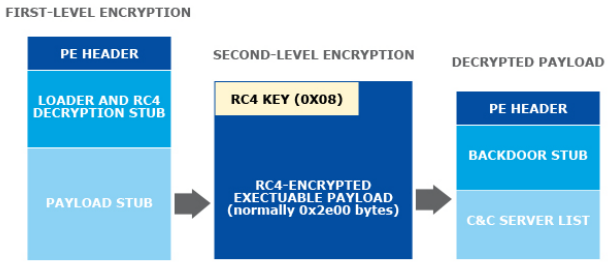

Figure 2. *File structure of encrypted SIMBOT malware variants*

Network Communication

The binary file contacts the C&C server for commands that it then executes on the victim's machine. Communication with the C&C server is done through HTTP and uses RC4 encryption for the data sent and received.

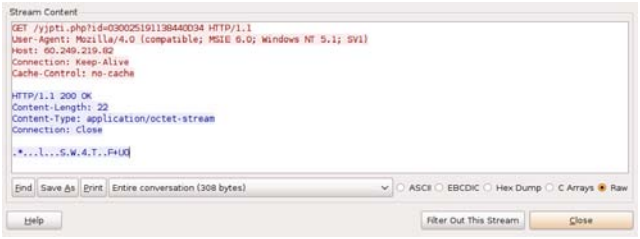

Figure 3. *Network communication between a Taidoor-compromised machine and a Taidoor C&C server*

The initial request to the C&C server is formatted as follows:

```
[C&C]/{5 random characters}.php?id={6 random
numbers}{encrypted victim's MAC address}
```

The victim's MAC address is sent to the C&C server, as this is used as key to encrypt the data exchanged by the victim's machine and the C&C server. The MAC address is encrypted using a custom algorithm, which basically increases the values in the address by 1.

As shown in Figure 4, the C&C server responds with encrypted data. Since we know the encryption algorithm used and that the key is the MAC address, we were able to decrypt it.

```
MAC address of analysis machine: 08-00-27-
33-9C-23
Encrypted data: ?*覿l???S?W 4?T??F+UO
Decrypted data: cmd/c ipconfig/all
Command type: 3
Command string: cmd/c ipconfig/all
```

The decrypted data shows that the C&C server is interested in IP configuration-related data in the victim's machine. The output of the command is then encrypted and sent to the C&C server.

Table 1 shows the full capabilities of the injected binary.

Complete List of C&C Commands

The decrypted C&C command was formatted in the following manner:

```
[command type][command string]
```

Command type refers to a hex digit that can be *[0x2], [0x3], [0x4], [0x5],* or *[0x7],* which identifies what it will do with the command string. Command string, on the other hand, refers to a set of strings relevant to the command type.

Command	*Description*
0x2—sleep command	The binary waits for a specified amount of time before requesting another command from the C&C server.
0x3—execute commands on the system (i.e., *cmd/c ipconfig/all)*	This can be used to explore the data or files in the victim's machine for reporting back to the C&C server. This can also be used to explore the network to which the compromised machine is connected.
0x4—download and execute file	This can be used to install additional files in the victim's machine.
0x5—download files from the C&C server	The binary downloads but does not execute files from the C&C server.
0x7—upload files from infected machine to the C&C server	This can be used to exfiltrate data or files from the victim's network to the C&C server.

TIMELINE

Using the Taidoor C&C servers we found using Trend Micro Smart Protection Network data, we constructed a timeline that indicates related activities as early as October 2010 (see Table 2). While we saw gaps in-between activities, notably between November 2010 and February 2011, we consistently discovered malware samples connect to this infrastructure. The dates when these were discovered may indicate exact dates of compromise.

MD5 HASH	*DETECTION*	*C&C SERVER*	*DATE SEEN*
2d33005a26a9cb2063dde2fa179b453e		*216.139.109.156*	10/12/2010
4b92f9b403fa59a35edf5af2f1aa98fb		*216.139.109.156*	10/12/2010
95bfeb4b7b8edb2517ede938bf9791d9		*216.139.109.156*	10/12/2010
5dd13efe319f0cdfe75346a46c1b791b	TROJ_GEN.R42C3JR	*211.35.222.6*	10/14/2010
1de1a60f51829e5e0d30dfd4b5197a72	TROJ_DLOADE.SMJ	*216.139.109.156*	10/22/2010
608bae3e4a59e4954f9bf43e504e2340	TROJ_GEN.R47E1K9	*211.35.222.6*	10/27/2010
b80da571f2cd7eab4aec12eee8199289	TROJ_DLOADE.SMJ	*60.250.39.73*	11/23/2010
0998743b808b57f6707641be64fa4fcd	TROJ_DLOADR.TDG	*211.35.222.6*	2/25/2011
920a7857da9ee7b403f3077660eddf31	TROJ_DLOADR.TDG	*211.35.222.6*	2/25/2011
d28b1b2824fd26d18f851e7605660f74	TROJ_GEN.R21C3E6	*216.139.109.156*	4/15/2011
265785ccc9503d30465156b90afa2523	TROJ_GEN.R3EC2G4	*216.139.109.156*	4/28/2011
7488ffd5d9c1751d1ceca88a4231304b	TROJ_GEN.R4FCRBC	*216.139.109.156*	7/7/2011
ecd97b7cfb4c8715d7800a9808a1646f	TROJ_INJECT.ZZXX	*216.139.109.156*	8/10/2011
6703dd35f6f56f35d298b9cd4c73e9cb	BKDR_SIMBO.DUKKS	*216.139.109.156*	8/29/2011
8406c1ae494add6e4f0e78b476fb4db0	TROJ_ARTIEF.VTG	*60.249.219.82*	10/6/2011
5fd848000d68f45271a0e1abd5844493	TROJ_MSDROP.ZZXX	*60.249.219.82*	10/12/2011
a0fff659499a4a76af2b89d28d0eafa2	TROJ_GEN.R3EC1J7	*216.139.109.156*	10/14/2011
97ff2338e568fc382d41c30c31f89720	HEUR_OLEXP.A	*60.249.219.82*	10/30/2011
d39981092a2f9a4b40413b38917ca573	TROJ_GEN.R49C7KI	*61.222.205.180*	11/2/2011
f43c9cc84fa7c16321241bb3c0802760		*61.222.190.100*	11/6/2011

MD5 HASH	*DETECTION*	*C&C SERVER*	*DATE SEEN*
c2cb594246942c328d8b11d4696a05c0	BKDR_SIMBOT.SMC	*61.218.233.51*	4/30/2012
		63.135.55.13	4/30/2012
65a0716af402727247296649abda7be6	BKDR_SIMBOT.SMC	*203.146.189.160*	4/7/2012
		203.150.231.236	4/7/2012
4a1365bdef0773aa0d3d33877d5a5334	BKDR_SIMBOT.SMC	*222.101.218.86*	5/29/2012
		64.34.60.218	5/29/2012
		203.90.100.21	5/29/2012
7f82c77a1f1b36f392f2f1763e2cc119	BKDR_SIMBOT.SMC	*203.146.189.141*	4/30/2012
ac75e62b36f4e845c1a095c9bcc43896	TROJ_DLOADR.WKJ	*62.13.61.173*	4/2/2012
		61.218.233.51	4/2/2012
		63.135.55.13	4/2/2012
5eb86d098a5ab48c7173545829008636	BKDR_SIMBOT.SMC	*112.217.74.188*	6/13/2012
		203.114.103.58	6/13/2012
85c64f43de8cb83234ee21fb0234f256	BKDR_SIMBOT.SMC	*203.146.189.141*	5/14/2012
7f82c77a1f1b36f392f2f1763e2cc119	BKDR_SIMBOT.SMC	*85.43.157.110*	4/30/2012
		203.116.147.94	4/30/2012
		58.40.20.165	4/30/2012
85c64f43de8cb83234ee21fb0234f256	BKDR_SIMBOT.SMC	*213.50.91.196*	5/14/2012
		211.22.72.193	5/14/2012
ffe76a043871638ec5e953084af1a2d8	BKDR_SIMBOT.SME	*69.178.171.135*	5/17/2012
		202.40.188.10	5/17/2012
20db3ff24701f4adac3cc61b591b6c98	BKDR_SIMBOT.SME	*60.248.216.194*	5/7/2012
85c64f43de8cb83234ee21fb0234f256	BKDR_SIMBOT.SMC	*201.159.226.189*	5/14/2012
		202.251.249.222	5/14/2012
20db3ff24701f4adac3cc61b591b6c98	BKDR_SIMBOT.SME	*222.101.218.86*	5/7/2012
		64.34.60.218	5/7/2012

MD5 HASH	*DETECTION*	*C&C SERVER*	*DATE SEEN*
		203.90.100.21	5/7/2012
6b5ca357066b40def382a1e130fb87cb	BKDR_SIMBOT.SME	*210.65.11.11*	4/25/2012

Damage

After analyzing of the Taidoor campaign, we saw that the malware the attackers used had the functionality normally seen in a Remote Access Trojan (RAT). Based on the command capabilities of the Taidoor malware, we were able to determine that data theft and data destruction was possible. The malware also had the ability to remotely and sometimes randomly terminate processes on victims' machines. This can lead to the termination of a critical process that results in denial of service (DoS). If this happens on a critical server, this can cause loss of business revenue or critical data.

Defending Against APTs

Sufficiently motivated threat actors can penetrate even networks that use moderately advanced security measures. As such, apart from standard and relevant attack prevention measures and mechanisms such as solid patch management; endpoint and network security; firewall use; and the like, enterprises should also focus on detecting and mitigating attacks. Moreover, data loss prevention (DLP) strategies such as identifying exactly what an organization is protecting and taking into account the context of data use should be employed.

Local and External Threat Intelligence

Threat intelligence refers to indicators that can be used to identify the tools, tactics, and procedures threat actors engaging in targeted attacks utilize. Both external and local threat intelligence is crucial for developing the ability to detect attacks early. The following are the core components of this defense strategy:

- *Enhanced visibility:* Logs from endpoint, server, and network monitoring are an important and often underused resource that can be aggregated to provide a view of the activities within an organization that can be processed for anomalous behaviors that can indicate a targeted attack.
- *Integrity checks:* In order to maintain persistence, malware will make modifications to the file system and registry. Monitoring such changes can indicate the presence of malware.
- *Empowering the human analyst:* Humans are best positioned to identify anomalous behaviors when presented with a view of aggregated logs from across a network. This information is used in conjunction with custom alerts based on the local and external threat intelligence available.

Technologies available today such as *Trend Micro™ Deep Discovery* provide visibility, insight, and control over networks to defend against targeted threats.[12] *Deep Discovery* uniquely detects and identifies evasive threats in real time and provides in-depth analysis and actionable intelligence to prevent, discover, and reduce risks.

Mitigation and Cleanup Strategy

Once an attack is identified, the cleanup strategy should focus on the following objectives:

- Determine the attack vector and cut off communications with the C&C server.
- Determine the scope of the compromise.
- Assess the damage by analyzing the data and forensic artifacts available on compromised machines.

Remediation should be applied soon afterward, which includes steps to fortify affected servers, machines, or devices into secure states, informed in part by how the compromised machines were infiltrated.

Educating Employees Against Social Engineering

Security-related policies and procedures combined with education and training programs are essential components of defense. Traditional training methods can be fortified by simulations and exercises using real spear-phishing attempts sent to test employees. Employees trained to expect targeted attacks are better positioned to report potential threats and constitute an important source of threat intelligence.

Data-Centric Protection Strategy

The ultimate objective of targeted attacks is to acquire sensitive data. As such, DLP strategies that focus on identifying and protecting confidential information are critical. Enhanced data protection and visibility across an enterprise provides the ability to control access to sensitive data as well as monitor and log successful and unsuccessful attempts to access it. Enhanced access control and logging capabilities allow security analysts to locate and investigate anomalies, respond to incidents, and initiate remediation strategies and damage assessment.

[12] http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/index.html

TREND MICRO THREAT PROTECTION AGAINST TAIDOOR CAMPAIGN COMPONENTS

Table 3 summarizes the Trend Micro solutions for the components of the Taidoor campaign. Trend Micro recommends a comprehensive security risk management strategy that goes further than advanced protection to meet the real-time threat management requirements of dealing with targeted attacks.

Attack Component	*Protection Technology*	*Trend Micro Solution*
Initial C&C server request format: `[C&C]/{5 random characters}.php?id={6 random numbers}{encrypted victim's MAC address}`	Web Reputation	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*
BKDR_SIMBO.DUKKS BKDR_SIMBOT.SMC BKDR_SIMBOT.SME HEUR_OLEXP.A TROJ_ARTIEF.VTG TROJ_DLOADE.SMJ TROJ_DLOADR.TDG TROJ_DLOADR.WKJ TROJ_GEN.R21C3E6 TROJ_GEN.R3EC1J7 TROJ_GEN.R3EC2G4 TROJ_GEN.R3EC7JC	File Reputation (Antivirus/Anti-malware)	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*

Attack Component	*Protection Technology*	*Trend Micro Solution*
TROJ_GEN.R42C3JR TROJ_GEN.R47E1K9 TROJ_GEN.R49C7KI TROJ_GEN.R4FCRBC TROJ_INJECT.ZZXX TROJ_MSDROP.ZZXX		
CVE-2009-3129 *CVE-2009-4324* *CVE-2010-1297* *CVE-2010-2883* *CVE-2011-0611* *CVE-2011-1269* *CVE-2012-0158*	Vulnerability Shielding/Virtual Patching	Server *(Deep Security)* Endpoint *(OfficeScan with Intrusion Defense Firewall Plug-In)* For *CVE-2009-3129:* • Rule #1003817 *(Excel* Featheader Record Memory Corruption Vulnerability) For *CVE-2009-4324:* • Rule #1004008 *(Adobe Reader* and *Acrobat* 'newplayer()' JavaScript Method Code Execution) For *CVE-2010-1297:* • Rule #1004202 (Adobe Products *authplay.dll* Remote Code Execution Vulnerability) For *CVE-2010-2883:* • Rule #1004393 *(Adobe Reader* SING Table Parsing Vulnerability) • Rule #1004113 (Identified Malicious Adobe PDF Document) • Rule #1004315 (Identified Malicious Adobe PDF Document) For *CVE-2011-0611:* • Rule #1004647 (Restrict *Microsoft Office* File with Embedded SWF)

Attack Component	*Protection Technology*	*Trend Micro Solution*
		For *CVE-2011-1269:* • Rule #1004661 *(Microsoft PowerPoint* Remote Code Execution Vulnerability) For *CVE-2012-0158:* • Rule #1004973 (MSCOMCTL.OCX RCE Vulnerability for Rich Text File) • Rule #1004977 (Restrict *Microsoft Windows* Common ListView and TreeView ActiveX Controls) • Rule#1004978 (MSCOMCTL.OCX RCE Vulnerability for *Office* Binary File)
58.40.20.165 *60.248.216.194* *60.249.219.82* *60.250.39.73* *61.222.190.100* *61.222.205.180* *61.218.233.51* *62.13.61.173* *63.135.55.13* *64.34.60.218* *69.178.171.135* *85.43.157.110* *112.217.74.188* *201.159.226.189* *202.40.188.10* *202.251.249.222*	Web, Domain, and IP Reputation	Endpoint *(Titanium, Worry-Free Business Security, OfficeScan)* Server *(Deep Security)* Messaging *(InterScan Messaging Security, ScanMail Suite for Microsoft Exchange)* Network *(Deep Discovery)* Gateway *(InterScan Web Security, InterScan Messaging Security)* Mobile *(Mobile Security)*

Attack Component	*Protection Technology*	*Trend Micro Solution*
203.90.100.21 *203.114.103.58* *203.116.147.94* *203.146.189.141* *203.146.189.160* *203.150.231.236* *210.65.11.11* *211.35.222.6* *211.22.72.193* *213.50.91.196* *216.139.109.156* *222.101.218.86*		

Advanced persistent threats (APTs) refer to a category of threats that aggressively pursue and compromise specific targets to maintain persistent presence within the victim's network so they can move laterally and exfiltrate data. Unlike indiscriminate cybercrime attacks, spam, web threats, and the like, APTs are much harder to detect because of the targeted nature of related components and techniques. Also, while cybercrime focuses on stealing credit card and banking information to gain profit, APTs are better thought of as cyber espionage.

TAIDOOR

First Seen

Individual targeted attacks are not one-off attempts. Attackers continually try to get inside the target's network.

Based on Trend Micro™ Smart Protection Network™ data, the earliest Taidoor campaign-related activities were seen as far back as October 2010.

Victims and Targets

APT campaigns target specific industries or communities of interest in specific regions.

This campaign primarily targeted government organizations located in Taiwan.

Operations

The first-stage computer intrusions often use social engineering. Attackers custom-fit attacks to their targets.

In this campaign, attackers sent an email to targets. The email came with specially created file attachments that exploited vulnerabilities such as *CVE-2012-0158, CVE-2009-4324, CVE-2010-1297, CVE-2010-2883, CVE-2011-0611, CVE-2011-1269,* and *CVE-2009-3129.* The purpose of the file attachment is to drop and install SIMBOT malware variants, which had functionalities normally seen in Remote Access Trojans (RATs).

Possible Indicators of Compromise

Attackers want to remain undetected as long as possible. A key characteristic of these attacks is stealth.

The GET and POST requests from compromised computers contained a URL path in the following format, *aaaaa.php?id=bbbbbbccccccccccc,* where *"aaaaa"* refers to five random characters that form a file name, *"bbbbbb,"* refers to six pseudorandomly generated characters that change for each connection, and *"ccccccccccc"* refers to 12 characters that represent the compromised host's MAC address that is obfuscated using a custom algorithm.

In addition, the initial command-and-control (C&C) server request typically uses the following format:

```
[C&C]/{5 random characters}.php?id={6 random numbers}{encrypted victim's MAC address}
```

* The full technical details of this attack can be read in the Trend Micro research paper, "The Taidoor Campaign: An In-Depth Analysis." The characteristics highlighted in this APT campaign profile reflect the results of our investigation as of August 2012.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud