The Mirage Campaign

- **Author:** Silas Cutler, Dell SecureWorks Counter Threat Unit(TM) Threat Intelligence
- **Date:** 18 September 2012
- **URL:** http://www.secureworks.com/research/threats/the-mirage-campaign/

Introduction

Since April 2012, the Dell SecureWorks Counter Threat Unit™ (CTU) research team has been tracking a cyber espionage campaign that uses a remote access trojan (RAT) named Mirage (also known as MirageFox). This ongoing attack has targeted a high-profile oil company in the Phillipines, a military organization in Taiwan, an energy company in Canada, and several as yet unidentified entities in Brazil, Israel, Egypt and Nigeria.

Analysis

Distribution vector

Based on the data collected by the CTU research team, the campaign's primary attack vector is spearphishing email that targets mid-level to senior-level executives. These emails contain an attachment that includes a malicious payload that installs a copy of Mirage.

CTU researchers have identified several files that drop and execute a copy of Mirage onto a target system. These "droppers" are designed to look and behave like PDF documents. However, the droppers are stand-alone executable files that open an embedded PDF file and execute the Mirage trojan. In one example, CTU researchers observed an executable file (MD5 hash ce1cdc9c95a6808945f54164b2e4d9d2) that upon execution drops a copy of Mirage and opens an embedded PDF of a news story titled "Yemeni Women can participate in politics just like men, says President Saleh" that was posted on the Yemen Observer's website.

Behavior analysis

The CTU research team has identified two main variants of the Mirage trojan. These variants are based on key evolutionary differences in the execution and encodings used in communication with the command and control (C2) servers.

When Mirage executes, the original file copies itself to a folder under C:\Documents and Settings\<USER>\ or C:\Windows\ and then deletes the original file. After the initial copy, Mirage starts the newly created file and exits the original. The newly started copy creates registry keys to ensure that the system remains infected after every reboot. CTU researchers have observed the following filenames created after execution:

- svchost.exe
- ernel32.dll
- thumb.db
- csrss.exe
- Reader_SL.exe
- MSN.exe

Phone-home and C2 operations

The data sent by Mirage shares attributes with the malware family known as JKDDOS, which was researched by Arbor Networks. In its initial phone-home connection, JKDDOS sends a system profile to the C2 server. This profile contains the CPU speed, memory size, system name and username. Similar information and encoding techniques are seen in the initial phone-home requests of Mirage infections.

Mirage phones home to its C2 servers using a standard HTTP request. From the activity CTU researchers have observed when executing Mirage in a malware sandbox, this communication commonly occurs over ports 80, 443 and 8080, and it can implement SSL for added security.

The earliest variant of Mirage uses an HTTP POST request to transmit the initial phone-home request. This phone-home request contains detailed system information of the infected system to give the C2 server a rough profile of each system that is infected and that is calling home.

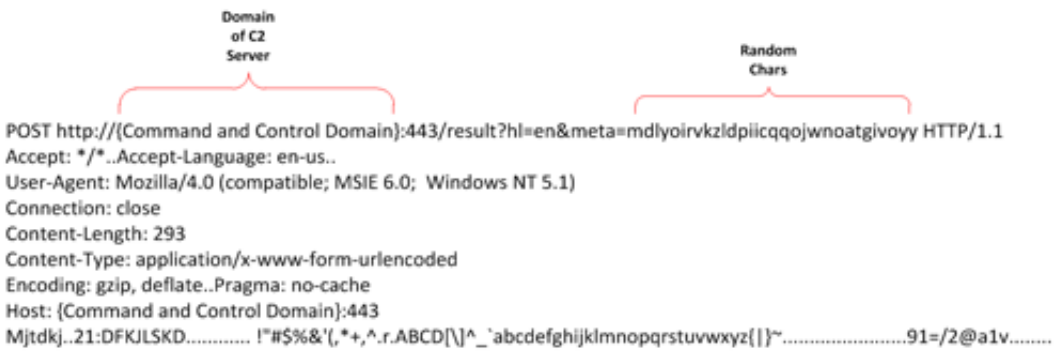

Figure 1. Phone-home request (variant 1).

The payload is encoded with a simple cipher to mask the data being sent to the C2 server. The cipher encodes the payload by adding each character's ASCII value by its offset from the start of the payload.

Raw values	M	i	r	a	g	e
Raw hex	0x4d	0x69	0x72	0x61	0x67	0x65
Raw decimal	77	105	114	97	103	101
Encoded decimal	77	106	116	100	107	106
Encoded hex	0x4d	0x6a	0x74	0x64	0x6b	0x6a
Encoded values	M	j	t	d	k	j

Table 1. Payload encoding.

The initial payload starts with the word "Mirage", which in its encoded state is "Mjtdkj". From there, Mirage encodes and sends the MAC address, CPU information, system name and username in the initial request to the C2 server.

If the C2 server successfully receives the request, then it responds with an HTTP response code "200 OK". The word "Mirage" appears in its payload, followed by two null bytes. If there is no response or an invalid response from the C2 server, the infected system continues to send its initial phone-home request at regular intervals.

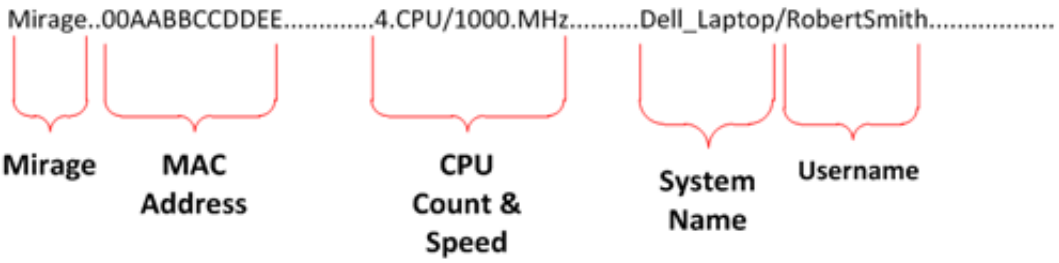

Figure 2. Decoded payload (variant 1).

If the infected system connects successfully to the C2 server, then the infected system continues to send regular check-in updates. These updates are transmitted the same way as the initial phone-home request; however, only the MAC address of the infected system is sent in the payload.

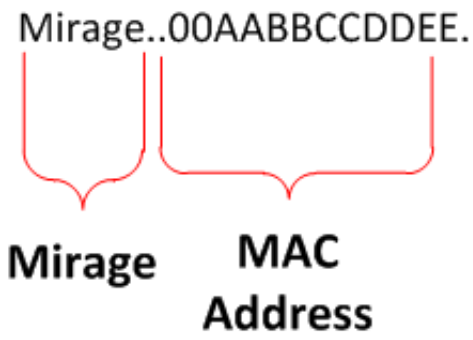

Figure 3. Decoded check-in update (variant 1).

The second variant of Mirage uses HTTP GET requests instead of HTTP POST requests to transmit the phone-home requests' payload. This evolved variant's initial phone-home request's payload is contained in a Base64-encoded string in the initial request. The decoded Base64 payload contains a second level of encoding that has several variations. The data being transmitted in the encoded string contains the same data as the previous variant, as well as some additional data. One change is the text at the beginning of the phone-home payload. Instead of the word "Mirage" used in earlier variants, later variants use the phrase "Neo, welcome to the desert of the real", a quote from the movie *The Matrix*.

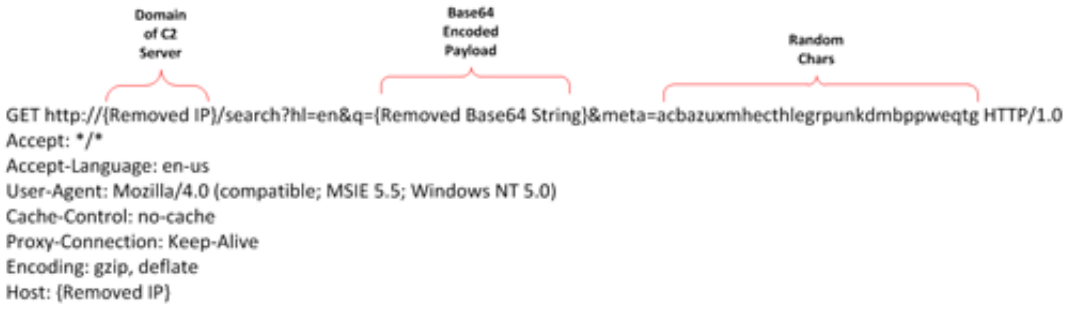

Figure 4. Sample request (variant 2).

The CTU research team has seen the encoding used in variant 2 in other malware families. One such malware family is Lingbo, which uses a similar encoding algorithm but does not contain some of the major characteristics of Mirage. Samples from both malware families have included strange embedded quotes. Instead of Mirage's quote from The Matrix, Lingbo contains the embedded quote "It is the end of the world and I feel Fine", from the REM song "It's the end of the world."

Custom versions and variants

The CTU research team identified several Mirage variants that had unique attributes not designed for widespread targeting. These custom variants were designed to operate under specific conditions and to evade common system defenses. CTU researchers also found several samples that contained debugging information, possibly from early versions.

One of the variants was seen in a subset of samples that had been modified specifically for the environment targeted by the threat actors. These samples had been configured with default credentials for the targeted environment's web proxy servers. The following proxy usernames and password combinations appear in the samples collected by the CTU research team:

- a1:a1
- pagmb:pa
- quickheal:quickheal

In the debugging versions, the CTU research team discovered two strings that identified the source code paths from which the samples were compiled:

- D:\....\MF-v1.2\Server\Debug\Server.pdb (MD5 hash fa26f410d0133f4152ea78df3978c22)
- E:\fox_1.2 20110307\MF-v1.2\Server\Release\MirageFox_Server.pdb (MD5 hash 1045e26819ff782015202838e2c609f7)

The .pdb file extension is commonly used with Microsoft Visual Studio. Its use in these debugging versions coincides with the samples for Mirage, which were written using Microsoft Visual C++. CTU researchers also noted that the original name of the trojan used in the path is MirageFox, which is likely the name used by the threat actors.

This information leads to two potential conclusions:

1. The two variants of MF-v1.2, the debug version and the release version, allow the threat actors to customize variants. CTU researchers have already seen this activity.
2. The use of different drive letters but similar source code paths may indicate that the threat actors are keeping a repository of tools on a central file server for shared use.

Identification of victims

From May to the date of this publication, the CTU research team engaged in a sinkholing operation. During the operation, several of the domains formerly used as part of the C2 infrastructure were taken over, and all activity to the domains was logged. The sinkholed domains were no longer in use and were freely available for registration.

During the operation, CTU researchers were able to identify approximately 80 IP addresses regularly communicating to the sinkhole. After analyzing and decoding the requests, CTU researchers discovered that a subset of the observed systems had usernames such as "admin" or "owner", and the originating IP address resolved to either a residence or an antivirus or security company. Because these requests were most likely from behavioral testing on the malware sample, the CTU research team filtered these connections out of the results.

After decoding the inbound requests, the CTU research team identified approximately 100-120 infected systems attempting to phone home. The majority of the inbound requests came from Taiwan or the Philippines, with several isolated cases in Nigeria, Brazil, Israel, Canada and Egypt. Many of the IP addresses originate from networks owned by the oil company, energy company, and military organization.

Deeper analysis of the phone-home requests and correlation with social networking sites allowed CTU researchers to identify a specific individual infected with Mirage. It was an executive-level finance manager of the Phillipine-based oil company.

Figure 5. Sources of infected hosts.

Threat actors

The threat actors using Mirage have employed several tactics to attempt to hide their identities and their primary C2 servers. One of the common tactics is using dynamic domain name system (dDNS) domains for the callbacks to the C2 servers. dDNS providers (e.g., Dyndns.com) allow anyone to register for a free third-level domain (e.g., Checkip.dyndns.org) and require only a valid email address, which is kept private.

When investigating the DNS addresses of the C2 servers, CTU researchers identified several IP addresses of hosting companies based in the United States that are running HTran. HTran software is used to proxy connections from one system to another. In the past, it has been used to disguise the true C2 servers used by malware authors. In the CTU research team's 2011 analysis of HTran, the software's author was identified as a member of the Chinese hacker group HUC, the Honker Union of China.

Despite efforts to operate anonymously, there were several clues that pointed to the true identities of the attackers. During an analysis of the phone-home activity, CTU researchers identified four unique second-level domains that were not connected to a dDNS provider. Two of these domains shared a common owner's email address, and two were previously flagged for suspicious activity.

C2 domain name	Owner name	Owner email
Adobesuit.com	nie min	dnsjacks@yahoo.com
antivirusbar.org	white jacks	dnsjacks@yahoo.com
Echosky.biz	tawnya grilth	jeno_1980@hotmail.com
India-videoer.com	india videoer	king@hotmail.com
Asia-online.us	bkpathak	king_public@hotmail.com / kings@hotmail.com

Table 2. Unique second-level domains.

CTU researchers correlated 86% of the IP addresses the dDNS domains used in the phone-home request to IP addresses of subdomains belonging to domains owned by dnsjacks@yahoo.com. Of the remaining 14% that were not directly associated, CTU researchers correlated 10% to IP ranges that resolved to subdomains owned by dnsjacks@yahoo.com.

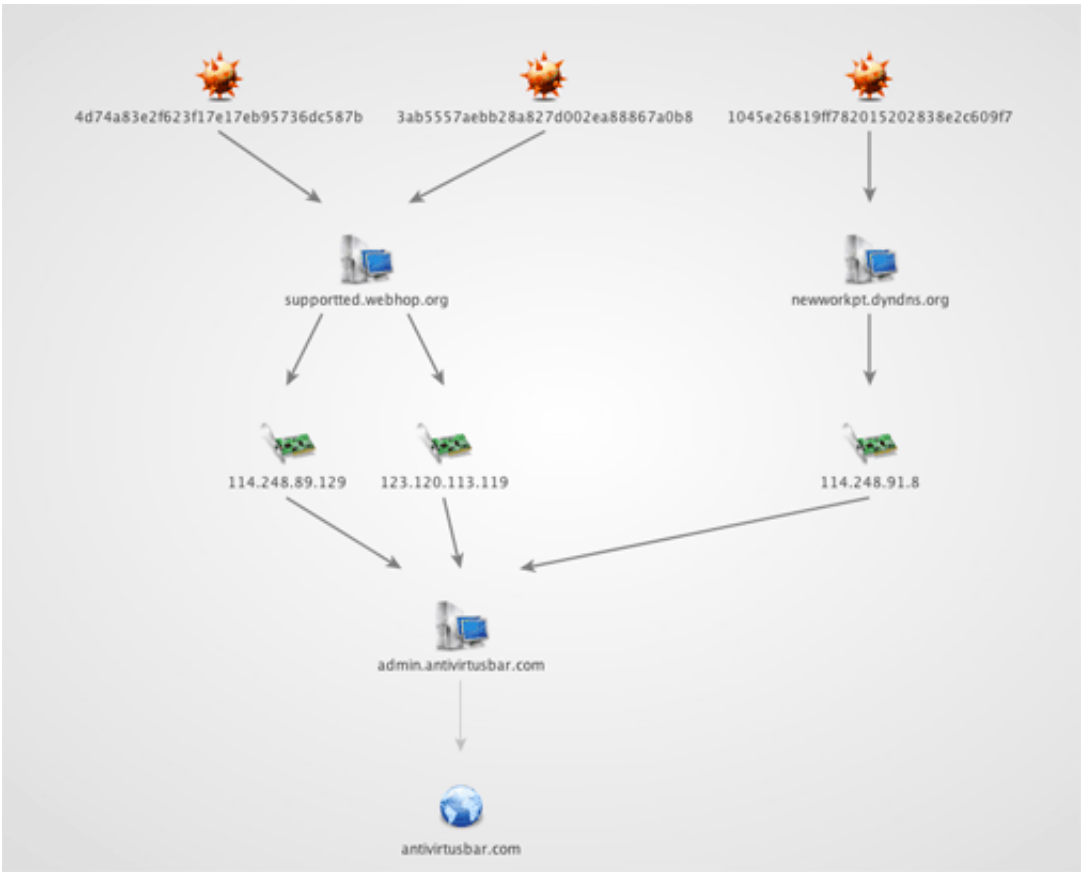

Figure 6. Analysis of IP addresses. (Source: Dell SecureWorks)

This link between the IP addresses and the subdomains indicates that dnsjacks@yahoo.com owns the dDNS domains. Using historical DNS records, CTU researchers were able to map each of the dDNS domains to a subdomain of a domain owned by dnsjacks@yahoo.com.

```
inetnum:        114.240.0.0 - 114.255.255.255
netname:        UNICOM-BJ
descr:          China Unicom Beijing province network
descr:          China Unicom
country:        CN
admin-c:        CH1302-AP
tech-c:         SY21-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-CNCGROUP-BJ
mnt-routes:     MAINT-CNCGROUP-RR
remarks:        service provider
```

Figure 7. Details of IP range.

In the samples CTU researchers analyzed, the other domains associated with the phone-home activity are asia-online.us, india-videoer.com and Echosky.biz. The CTU research team previously flagged these domains in the HTran investigation and later in the Sin Digoo analysis. The analysis of the Sin Digoo affair indicated that jeno_1980@hotmail.com and king@hotmail.com were connected. From the data the CTU research team has collected, indications point to dnsjacks@yahoo.com being either another alias or an associate of the actor referenced in the HTran and Sin Digoo analyses.

Figure 8. A common phone number was found to link india-videoer.com and asia-online.us

Conclusion

Mirage represents only one small piece of malware involved in an ongoing worldwide campaign. Over the past few years, these campaigns have become extremely successful, and a great deal of intellectual property and company secrets has been stolen from the targeted companies.

For companies in the targeted industries, it is important to have a strong perimeter security line in place. Using active intrusion detection and prevention systems as well as DNS monitoring for malicious domains is essential to detecting this activity. Companies that use the Yara malware identification and classification tool for scanning local systems can use the rules provided in the appendix to search for potential infections.

Traditionally, the success of botnets created by threat actor groups has been measured by the quantity of infected systems and the difficulty to defend against in the long term. These targeted attacks show that a successful campaign requires only a small quantity of infected systems to accomplish the attackers' objectives and to yield extremely powerful results.

Appendix

Yara rules

```
rule Mirage_APT_Backdoor : APT Mirage Backdoor Rat MirageRat
{
        meta:
                author = "Silas Cutler (SCutler@SecureWorks.com)"
                version = "1.0"
                description = "Malware related to APT campaign"
                type = "APT Trojan / RAT / Backdoor"
        strings:
                $a1 = "welcome to the desert of the real"
                $a2 = "Mirage"
                $b = "Encoding: gzip"
                $c = /\/[A-Za-z]*\?hl=en/
        condition:
                (($a1 or $a2) or $b) and $c
}
```

MD5 hashes

5efd0d7f52890291599c8562e8ea92db f51fbafc652e10a9ce13795d4cb2d449
eacd03ee55ea7d22b45762c82ae1c0e5 a748ff9663b2d39a35e4c073b73cd7f6
ce1cdc9c95a6808945f54164b2e4d9d2 e7d5ac11903c0217a999a79bc87182d2
5326e4fe9fd10e37d46e81c0f6bbf29a 1b918c8a40dc4a66430cfec7dabeb7f3
b2e821828df59c734c1cc379ef7f3122 c72d7794dc7f2eda6b44b934fe8fff1c
875877eedcd9f2d60bf63937fe22073d ad2dda9241cd6c0e879ab665d77ce13c
02d77cdaa808ded64d09eea732a586cc ccf34d2ba81de856af8167e73d0c8b69
18a5c6e92b962bc6512486db94bb17a7 ebe7699033424b9ef444364bd23ba665
32b33321290ac8011aa218da554b8fa5 7349c7908a672de885fdf9f9cc4547b5
f41896e9f77855842380fd9ed795bc64 eacd14ce8414911546cb027a8cb2fecd
407c291cd5c73da680fa9af9ec017fff 4b9723a4060838114e53d1df3fa2537a
7adb0f22468c10901bd280b2d8a154b0 070ef82a0bded089b6f996a392ca7b9a
abac650ab39c0dd074310710081d715d 286f7b377f5d0ca3505ed1ba6601c947
c9e49c504d5ca953c858d29b7a2acb9d 4d74a83e2f623f17e17eb95736dc587b
aaa9aae486ee7342d29a0a2f9b0ca205 a4b9bfc5aa5e37cc613112b9a9dcdb3e
7ad79f9a0efde6f4673585e400f29f18 fb17ffc7495880a7c19df0ebe5c97ad7
e29ab99be392bb7012f516a2dbfdc00c 3bfa7b806ff540cc1c264ec75048fbc4
8caf2a96e4d7bb83156c260ccc8f47e7 05a02e08cce99d3821574d8612f757fd

a4ff66224a0967763e1d079c99482577	d60cfe03bce8647cce723991e2cd2f8c
f0b93bf7273cbeaed69ed55b5169daf7	6ed270da7450945a3a5a05eda8312732
3be6fea2bf35c3c3be860622c68ff369	a1083968b78c081135268b6e4e12b1e5
5fa26f410d0133f4152ea78df3978c22	0fce05e2cea6bd9c217373f2ab962d82
3d10e68dec16b1a4bf949e3e403f2dda	85ef19fab3951d4dd56e42b5a9ccdeea
5c371a6dfb45f188fe8e6da4fee9300d	422f1ffe7e5bda7062f005be92fba36e
9ff3a9ef192453ecec26cf567c579bff	346aa61b5739e616482a1bc8bb548871
65445b138d80954cc912a6e43fe5b66d	c2661e45ec2198b04b29ec3fd1e120b2
685805936d8744225f8c11965202de8e	e04e5eb4aefeb326246d7f41d1b50759
80e978d0eea713812f1dd6b4e9b7daf2	eb1aa241b4a482ac44b27ce38eabccb7
921c724ccb04b9f672b294ffff83ce7b	418fb9ba2a61bccab3e54ebe0698c4b6
072877b961e31e8792a296c63b9c7b56	590e68aaaa5c2353b7288f64cc87d9bb
1a8bc862ceaa7e05189345065145842a	1f9894e730c0f5ba085baae409aa963a
6794cc6f5e463ee7432b9e718d8c1b8e	11b76423f450ba610f073e7522eeb56b
fdb949112cc72c68fc7c1ea0c65344bc	54d37fb1f624c798f0b400b4f50f3635
f4a6114fce22eb18b0ccf19cfa68ddba	7fda0451e4d320cc34efcaaabedd6824
1045e26819ff782015202838e2c609f7	84fc624f9f5f8de6980497058db1e8e1
5640beb540bef2e97ec4366713d533b8	964eec615f977b05bc87943ce0942cf9
0f93d28964b440c241ca126a7f94dae2	5069057b799636c012eec38147fb96e6
075df4723073ff08cd3e90d2b1f11722	a4a1670c537861f7d5b0db115a7aa5fa
240627a306f32483378e44ff13e12169	00b9619613bc82f5fe117c2ca394a328
5f2a4d865e6e94f7f15571faab5128d6	2219bef789ff73efc0a01f87be03188d

Printed from http://www.secureworks.com

For more information call (877) 838-7947 or email info@secureworks.com.