THE MsnMM CAMPAIGNS

The Earliest Naikon APT Campaigns

Kurt Baumgartner, Maxim Golovkin

May, 2015

CONTENTS

INTRODUCTION

Over time, the Naikon APT appears to have used specific toolsets against organizations within a designated country, as though each campaign was focused on one country. There is sometimes crossover between campaigns in several ways: the backdoors they deliver, the infiltration techniques, and the overall infrastructure. Backdoor functionality can also cross campaigns and tools. For example, sometimes we see an "inject" variant dropping a "sys10" backdoor. Or a naikon backdoor dropping a rarstone backdoor. Again, this particular actor is responsible for the MsnMM and Naikon campaigns deploying the following backdoors and tools:

- sslMM
- winMM
- exe_exchange
- wininetMM/sakto
- inject
- sys10
- xsControl/naikon and plugins
- rarstone
- second stage tools

The Naikon group also deployed a lesser-known set of second stage tools. They mixed together legitimate system administration tools with offensive network reconnaissance tools, including a custom network and service scanner and an attack codeset based on old Honker Union codebase shared on Chinese-speaking forums. See "**Second Stage Tools**".

For years, Naikon downloaders/backdoors were delivered to victim systems with kit-produced CVE-2012-0158 spear-phish. This exploit builder kit was shared amongst multiple APTs, because we see the same exploits dropping tools from various groups. Many of these exploit attachments were blocked by our advanced exploit protection (AEP) on customer systems in Vietnam, Myanmar, the Philippines, and organizations related to the energy sector in these and other ASEAN nations. Some of these backdoors and spear-phish activities also showed up in the Hardore Charlie CEIEC dump. In Jan 2014, we observed in some targets the increase of "right-to-left-override" (RTLO) naming schemes for initial payload delivery. In addition to its custom toolset, it appears to test freely-distributed tools – in December 2013, it pushed out

"Everything32" to victim systems, and TeamViewer was used as well. It is likely that the group faced difficulties when it came up against anti-malware products and tried abusing legitimate tools for anti-malware evasion. Finally, this threat actor deploys a custom pdf binding tool, to add to its effective but low-tech toolset.

The Naikon attackers can be, and in fact have been precise in social-engineering their targets. Data collection prior to an attack may have included the following data points:

- full names
- email addresses and status (active or inactive)
- date of birth and age
- interests in current events
- nationality
- gender
- previous email and social network communications to and from a target
- language spoken

Victims of the early campaigns were located mostly throughout Myanmar, Vietnam, Singapore, Laos, Malaysia, and the Philippines. There are other locations where Naikon's victims can be found, but these countries stand out.

To get in to target networks, the Naikon APT relied on email as an attack vector. It first compromised victim systems using common spear-phishing techniques, such as cve-2012-0158 exploit attachments, attachments altered with RTLO techniques, and a combination of icon-spoofing and name padding for executables. The MsnMM campaigns featured ripped images and documents re-used for spear-phish decoys, and we see that technique reapplied throughout other Naikon APT campaigns. The winMM components were also delivered to Myanmar victims throughout mid-2013 using RTLO and icon-spoofing techniques and sometimes even simpler icon spoofing+double extension+extra spacing in attachment filenames. For example, many of the Backdoor.Win32.MsnMM.i (winMM) executable filenames maintained almost 200 spaces, looking like this:

"letter to Gov office.doc .exe"

The Naikon APT used multiple backdoors presenting a variety of behaviors over time, but clusters of indicators were fairly consistent into 2015.

SHARED EXPLOIT GENERATION KIT

It's interesting that what appear to be multiple campaigns and crews all use a kit that generates CVE-2012-0158 exploits embedded with arbitrary backdoors for spear-phishing. One of the interesting characteristics of the Naikon APT's kit-produced shell-code is its runtime function offset calculations and control flow are built to jump past behavior-based protection and sandbox analysis. Each of the win32 api shellcode calls are carefully executed to land just past function hot patch space and prologues, evading user mode trampolines and hooks.

MsnMM, Naikon and Rarstone backdoors were generally delivered with stock 0158 exploits. Some dropped iph.bat and an "iExplorer.exe" that began with a "WMcal" parameter and profile.dat executable blob loaded into a running IE process. Other APTs use this kit as well. We found Stone Panda Poison Ivy samples delivered with the same CVE-2012-0158 exploits, dropping iph.bat and iExplorer.exe, and running the "iExplorer.exe WMcal" executable filename and parameter.

Finally, we found another exploit builder's template used to attack Korean-speaking targets. It was used across this group and others for building CVE-2012-0158 files, sharing the common author "Tran Duy Linh".

SHARED STRINGS, FUNCTIONALITY, TARGETS, AND INFRASTRUCTURE ACROSS CAMPAIGNS

Multiple Naikon tools used in multiple campaigns shared strings, functionality, a deployment and content focus on ASEAN organizations and other organizations doing business with them, and the infrastructure itself. Let's examine some of the toolset's shared strings and functionality, then move on to shared infrastructure.

Similar strings

While the Naikon backdoor maintained the user-agent string "NOKIAN95/WEB", it also maintained a debug path

```
f:\MyProjects\xServer\Release\xServer.pdb
```

Also, the Naikon backdoor's matching management software is called "xsControl". Plugins for the Naikon backdoor included a screenshot grabber named xsAdv.dll, and a single export "XS_Screencap".

This debug path in Naikon backdoors is very similar to the debug path maintained in Rarstone backdoors:

```
g:\MyProjects\xsFunction\Release\DLL.pdb
```

The MsnMM campaign backdoors all maintain an "MM" internal name, and the functionality changes when comparing them:

- WinMM
- WininetMM
- SslMM

A more recent oddity from this group includes a WinMM dropper with the internal name "Zhixin", creating a recently compiled Sys10 backdoor.

Some "MM" executables maintained debug strings across versions and families:

```
J:\chong\new\Release\SslMM.exe
```

and

```
J:\chong\nod\Release\SslMM.exe
```

Shared infrastructure

Now, let’s take a look at some of the shared infrastructure that helps to tie all of these campaigns together. MsnMM backdoors and naikon backdoors share portions of infrastructure across campaigns. For a quick example, early msnMM backdoors like sslMM, and one of the later tools, exe_exchange, share some domains with the nokian95 (naikon) and sys10 backdoors. There is much crossover.

Here, you can see a table recording domains that are shared across the backdoors for command and control infrastructure.

	exe_exchange	sys10	winMM	sslMM	wininetMM/ sakto	xsPlus/naikon
ahzx.eicp.net	yes	yes	yes			
mncgn.51vip.biz	yes	yes	yes			
bkav.imshop.in		yes				yes
ubaoyouxiang.gicp.net	yes			yes	yes	yes
googlemm.vicp.net			yes		yes	
myanmartech.vicp.net			yes	yes		yes

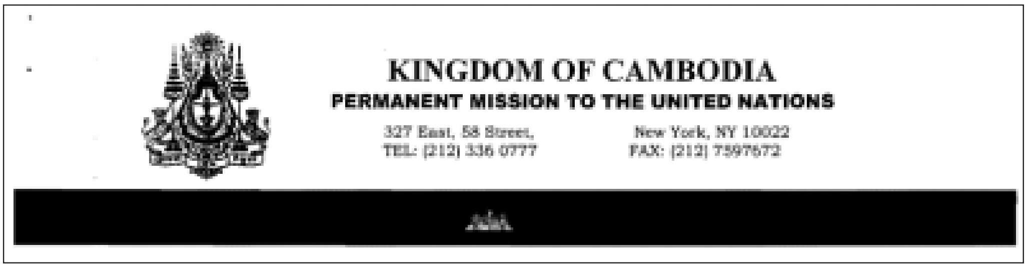
Correlating target profiles with spear-phish and decoy content

One of the most striking characteristics of this APT is that its targeting interest is revealed by its spear-phish and decoy content. Malicious actors of all stripes, including cybercriminals, have for at least the last ten years abused “hot topics” in their social-engineering content to better attract and mass-exploit victim systems. It’s a pretty worn-out discussion. What is different about the Naikon APT’s use of hot topics in spear-phish and decoy content is that reveals its specific victims and how these change over time. Precision social engineering seems to be an elevated skill set for the group.

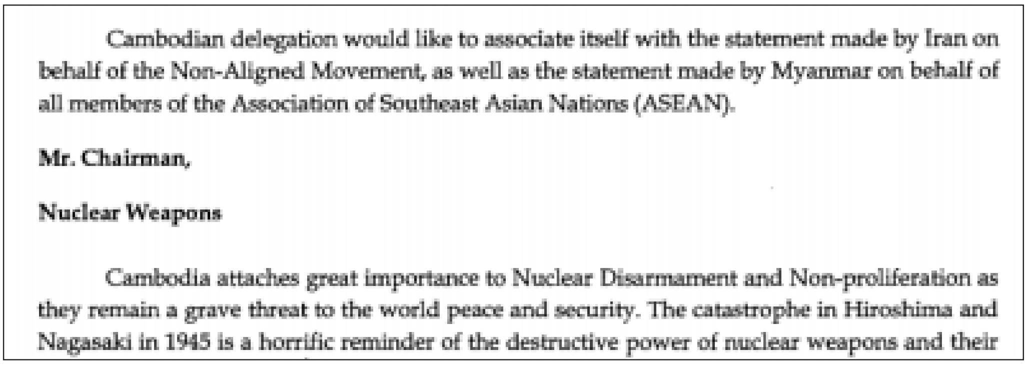
A few of the most interesting examples of such content include: a UN discussion and vote on nuclear proliferation and disarmament, the MH370 flight, and construction on the Raytheon-built National Coast Watch Center in PH.

For example, in the second week of October 2012, during the gang’s intense ongoing focus on SE Asian countries like Cambodia and its diplomats, we find a winMM backdoor detected as "Trojan.Win32.Agent.udtc" in New York City. This verdict identified the Naikon

APT's backdoor on the victim system. The timing is uncanny because, in that same week speeches and views on nuclear disarmament and non-proliferation were presented by SE Asian country delegates to the United Nations in New York City. An example of such a talk is here; a naikon decoy's content was strikingly similar:



KINGDOM OF CAMBODIA
PERMANENT MISSION TO THE UNITED NATIONS
327 East, 58 Street, New York, NY 10022
TEL: (212) 336 0777 FAX: (212) 7597672



Cambodian delegation would like to associate itself with the statement made by Iran on behalf of the Non-Aligned Movement, as well as the statement made by Myanmar on behalf of all members of the Association of Southeast Asian Nations (ASEAN).

Mr. Chairman,

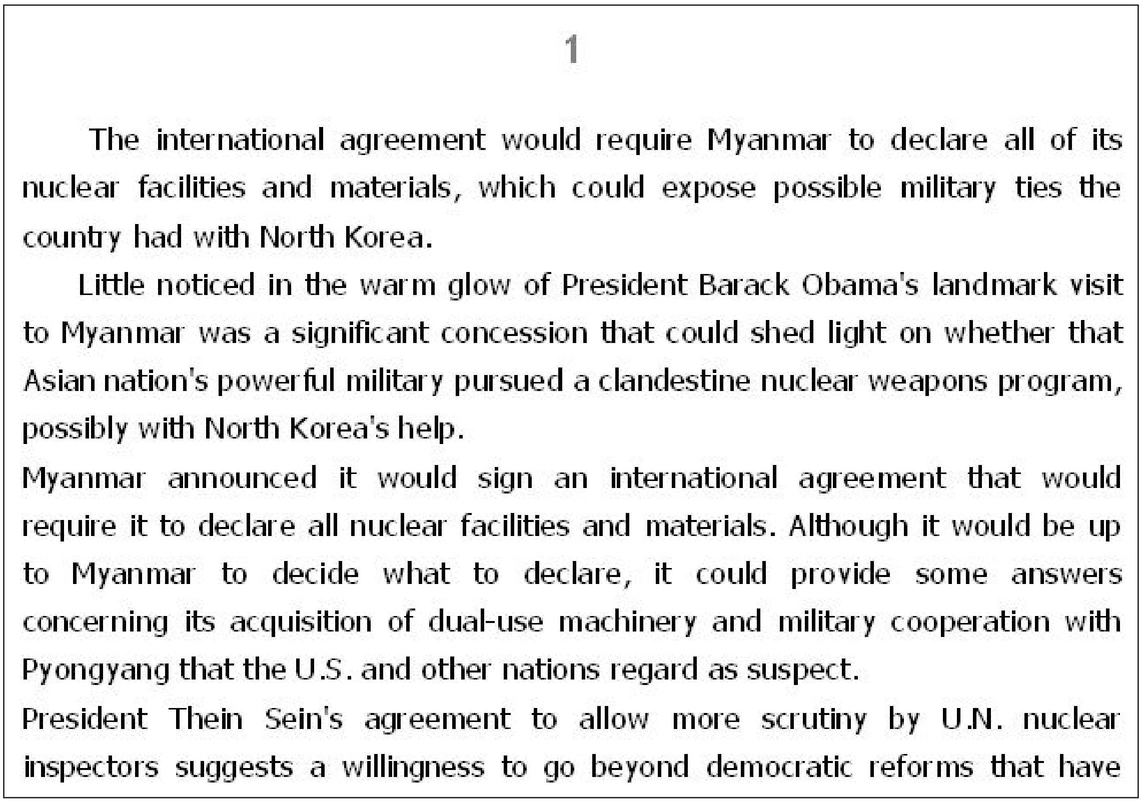
Nuclear Weapons

Cambodia attaches great importance to Nuclear Disarmament and Non-proliferation as they remain a grave threat to the world peace and security. The catastrophe in Hiroshima and Nagasaki in 1945 is a horrific reminder of the destructive power of nuclear weapons and their

MsnMM campaigns most commonly presented spear-phish exploits targeting CVE-2012-0158. A listing of screenshots in Appendix A reveals the variety of content and themes, all related to events and topics in the ASEAN region. Example titles include:

Letpadaung copper mine.doc	Myanmar Wanbao to commence construction of Letpadaung project	December 2014
nuclear agreement burma.doc	Burma Signs New Nuclear Deal With IAEA	September 2013
ALP Statement on Present Illegal Bangali Problem inside Arakan.doc	ALP statement on present illegal Bangali problems inside Arakan [pdf]	December 2012
Calendar Misslao 2013 Free.doc	Miss Lao Calendars	January 2014
ASEAN and Partners Firmly Committed to Narrowing the Development Gap.doc	ASEAN and Partners Firmly Committed to Narrowing the Development Gap	April 2013
refer to the 11th ACD Ministerial Meeting.doc	Asia Co-operation Dialogue eyes peace	December 2013
Asia's Military Developments.doc	Asia's military developments	November 2013

The following example's content was crafted to appear like a legitimate international agreement discussion. After the malicious document is opened and successfully exploits CVE-2012-0158 on the victim workstation, the exploit code drops and opens this decoy Word document:



1

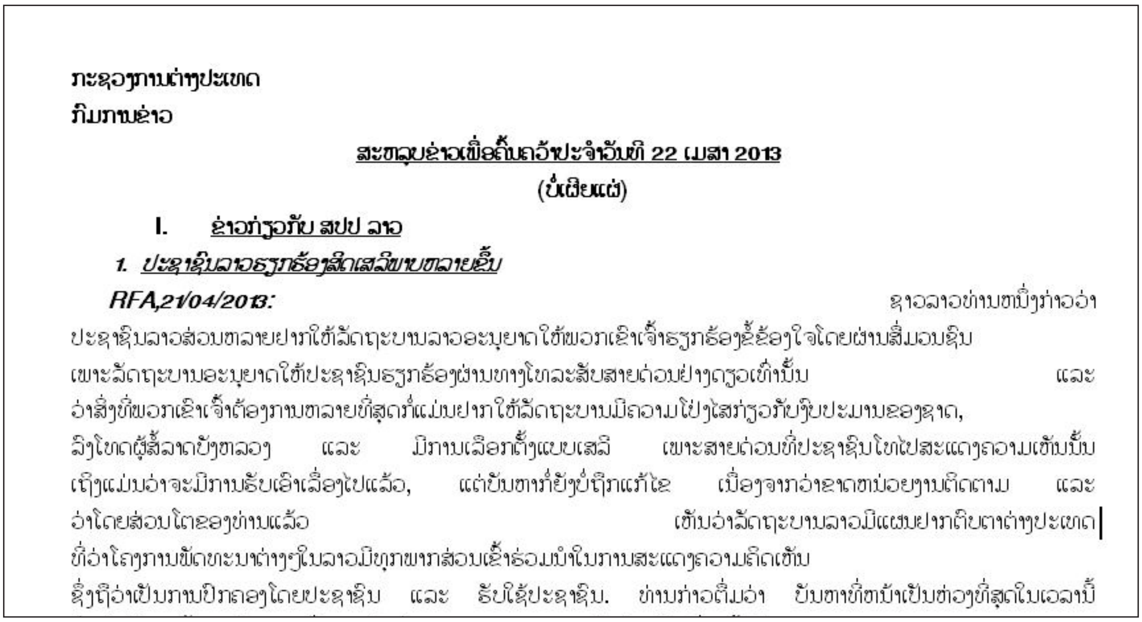
The international agreement would require Myanmar to declare all of its nuclear facilities and materials, which could expose possible military ties the country had with North Korea.

Little noticed in the warm glow of President Barack Obama's landmark visit to Myanmar was a significant concession that could shed light on whether that Asian nation's powerful military pursued a clandestine nuclear weapons program, possibly with North Korea's help.

Myanmar announced it would sign an international agreement that would require it to declare all nuclear facilities and materials. Although it would be up to Myanmar to decide what to declare, it could provide some answers concerning its acquisition of dual-use machinery and military cooperation with Pyongyang that the U.S. and other nations regard as suspect.

President Thein Sein's agreement to allow more scrutiny by U.N. nuclear inspectors suggests a willingness to go beyond democratic reforms that have

This next example is written with the Laotian Phetsarath OT font, a decoy attempt to be a legitimate Daily News Brief from the Laotian Foreign Ministry of Affairs.
It demonstrates the group's intentions to hit targets in Laos:



ກະຊວງການຕ່າງປະເທດ
ກົມການຂ່າວ

ສະຫລຸບຂ່າວເພື່ອຄົ້ນຄວ້າປະຈໍາວັນທີ 22 ເມສາ 2013

(ບໍ່ເຜີຍແຜ່)

I. ຂ່າວກ່ຽວກັບ ສປປ ລາວ

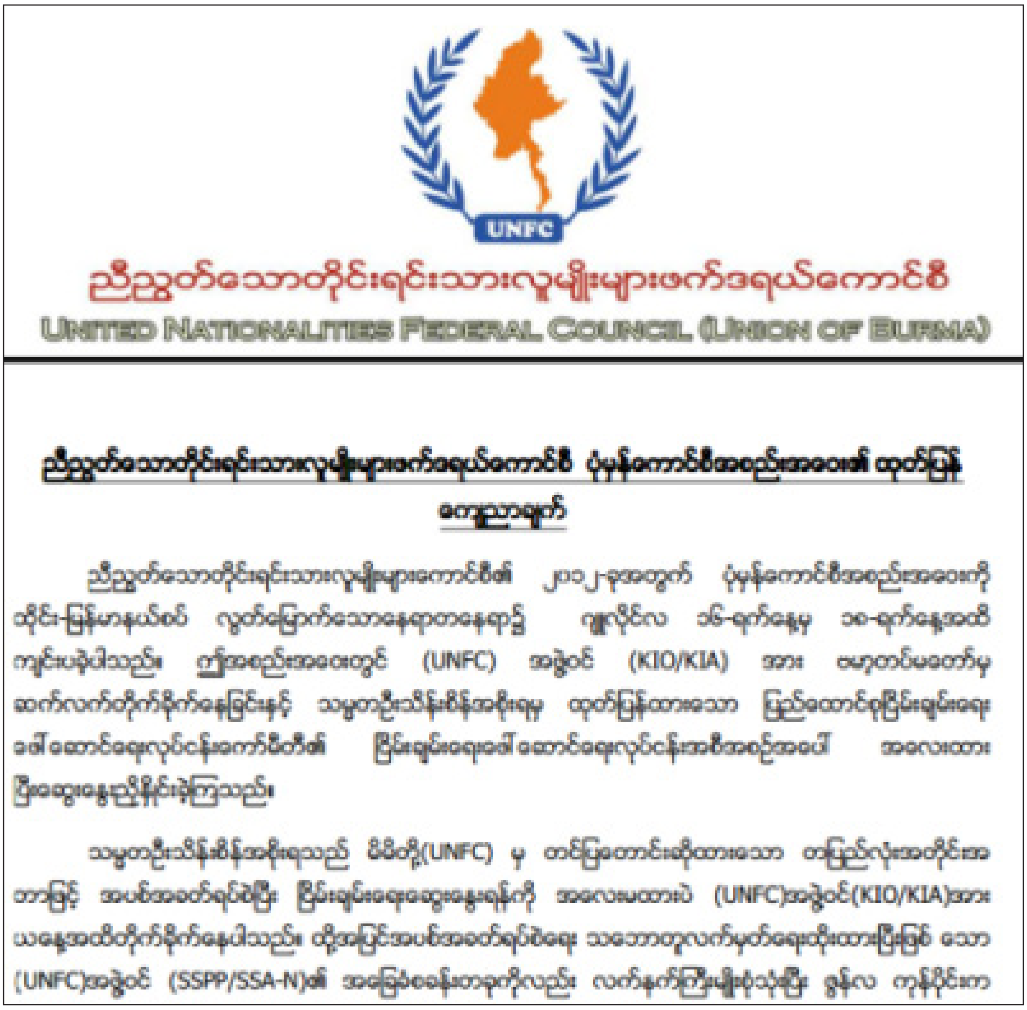
1. ປະຊາຊົນລາວຮຽກຮ້ອງສິດເສລີພາບຫລາຍຂຶ້ນ

RFA,21/04/2013: ຊາວລາວທ່ານໜຶ່ງກ່າວວ່າ ປະຊາຊົນລາວສ່ວນຫລາຍຢາກໃຫ້ລັດຖະບານລາວອະນຸຍາດໃຫ້ພວກເຂົາເຈົ້າຮຽກຮ້ອງຂໍ້ຂ້ອງໃຈໂດຍຜ່ານສື່ມວນຊົນ ເພາະລັດຖະບານອະນຸຍາດໃຫ້ປະຊາຊົນຮຽກຮ້ອງຜ່ານທາງໂທລະສັບສາຍດ່ວນຢ່າງດຽວເທົ່ານັ້ນ ແລະ ວ່າສິ່ງທີ່ພວກເຂົາເຈົ້າຕ້ອງການຫລາຍທີ່ສຸດກໍ່ແມ່ນຢາກໃຫ້ລັດຖະບານມີຄວາມໂປ່ງໃສກ່ຽວກັບງົບປະມານຂອງຊາດ, ລົງໂທດຜູ້ສໍ້ລາດບັງຫລວງ ແລະ ມີການເລືອກຕັ້ງແບບເສລີ ເພາະສາຍດ່ວນທີ່ປະຊາຊົນໂທໄປສະແດງຄວາມເຫັນນັ້ນ ເຖິງແມ່ນວ່າຈະມີການຮັບເອົາເລື່ອງໄປແລ້ວ, ແຕ່ບັນຫາກໍ່ຍັງບໍ່ຖືກແກ້ໄຂ ເນື່ອງຈາກວ່າຂາດໜ່ວຍງານຕິດຕາມ ແລະ ວ່າໂດຍສ່ວນໂຕຂອງທ່ານແລ້ວ ເຫັນວ່າລັດຖະບານລາວມີແຜນຢາກຕົບຕາຕ່າງປະເທດ ທີ່ວ່າໂຄງການພັດທະນາຕ່າງໆໃນລາວມີທຸກພາກສ່ວນເຂົ້າຮ່ວມນໍາໃນການສະແດງຄວາມຄິດເຫັນ ຊຶ່ງຖືວ່າເປັນການປົກຄອງໂດຍປະຊາຊົນ ແລະ ຮັບໃຊ້ປະຊາຊົນ. ທ່ານກ່າວຕື່ມວ່າ ບັນຫາທີ່ໜ້າເປັນຫ່ວງທີ່ສຸດໃນເວລານີ້

Appendix A contains many more example document titles and screenshots. The themes and content that would appeal to politically-interested individuals in various parts of the world quickly become obvious.

In addition to a high volume of files exploiting CVE-2012-0158, the MsnMM attackers for a brief period used RTLO (right to left override) techniques, and then attachments exploiting CVE-2010-3333. An example of RTLO that creates and opens this decoy document to camouflage its malicious background activity, then dropping and executing MsnMM backdoors on its victim system:

UNFC_Statement_final_rcs.pdf



UNFC

ညီညွတ်သောတိုင်းရင်းသားလူမျိုးများဖက်ဒရယ်ကောင်စီ

UNITED NATIONALITIES FEDERAL COUNCIL (UNION OF BURMA)

ညီညွတ်သောတိုင်းရင်းသားလူမျိုးများဖက်ဒရယ်ကောင်စီ ပုံမှန်ကောင်စီအစည်းအဝေး၏ ထုတ်ပြန်ကြေညာချက်

ညီညွတ်သောတိုင်းရင်းသားလူမျိုးများကောင်စီ၏ ၂၀၁၂-ခုအတွက် ပုံမှန်ကောင်စီအစည်းအဝေးကို ထိုင်း-မြန်မာနယ်စပ် လွတ်မြောက်သောနေရာတနေရာ၌ ဇူလိုင်လ ၁၆-ရက်နေ့မှ ၁၈-ရက်နေ့အထိ ကျင်းပခဲ့ပါသည်။ ဤအစည်းအဝေးတွင် (UNFC) အဖွဲ့ဝင် (KIO/KIA) အား ဗမာ့တပ်မတော်မှ ဆက်လက်တိုက်ခိုက်နေခြင်းနှင့် သမ္မတဦးသိန်းစိန်အစိုးရမှ ထုတ်ပြန်ထားသော ပြည်ထောင်စုငြိမ်းချမ်းရေး ဖေါ်ဆောင်ရေးလုပ်ငန်းကော်မီတီ၏ ငြိမ်းချမ်းရေးဖေါ်ဆောင်ရေးလုပ်ငန်းအစီအစဉ်အပေါ် အလေးထား ပြီးဆွေးနွေးညှိနှိုင်းခဲ့ကြသည်။

သမ္မတဦးသိန်းစိန်အစိုးရသည် မိမိတို့(UNFC) မှ တင်ပြတောင်းဆိုထားသော တပြည်လုံးအတိုင်းအတာဖြင့် အပစ်အခတ်ရပ်စဲပြီး ငြိမ်းချမ်းရေးဆွေးနွေးရန်ကို အလေးမထားပဲ (UNFC)အဖွဲ့ဝင်(KIO/KIA)အား ယနေ့အထိတိုက်ခိုက်နေပါသည်။ ထို့အပြင်အပစ်အခတ်ရပ်စဲရေး သဘောတူလက်မှတ်ရေးထိုးထားပြီးဖြစ် သော (UNFC)အဖွဲ့ဝင် (SSPP/SSA-N)၏ အခြေစိုက်စခန်းတခုကိုလည်း လက်နက်ကြီးများပစ်သုံးပြီး ဇွန်လ ကုန်ပိုင်းက

NAIKON APT MSNMM CAMPAIGN BACKDOORS AND LATERAL MOVEMENT TOOLSET

SslMM

MD5 – Filename	File Size	Compilation date	Linker version
7b1199523a662a3844ba590f83b56dae - %temp%\conime.exe	77,824 bytes	2013:01:31 01:25:38+00:00	6.0

The MsnMM gang built and released many more variants of their sslMM creation. The code is a full-featured backdoor. Each variant of this tool starts by attempting to create a socket, and then creates a new thread implementing a fairly complicated keylogging facility not often seen, using Windows Keyboard Accelerators. Online code demonstrates the technique here:

http://thronic.com/Win32%20Keylogging/

The backdoor retrieves a large number of victim system data points, which it then uses to check in to its hardcoded C2. The backdoor reports system identification information both to present the victim's identifying information and to fingerprint the system for asset management:

- OS version
- Service pack information
- Processor speed
- System name
- Logged-on user name
- OS install date

One of its more interesting features is the ability to fetch and use certificates from the "My" store on Windows systems. The "My" certificate store is created on a per-user basis, and this is where users' certificates are stored. It is reserved for each user for signing and decrypting data and encrypting network communications.

Feature list:

- Victim fingerprinting and performance sensitivity – system configuration collection
- Persistence – immediately identifying the Start Menu Startup directory and dropping a LNK to its own executable disguised as a “Office Start”, “Yahoo Talk”, “MSN Gaming Z0ne”, or “MSN Talk” shortcut
- Configurable network settings – both a primary and backup C2 string is hard-coded in each backdoor. At this point, we are aware of almost 50 domains and unique IP addresses used to host C2
- Keylogging facility – Windows Accelerators with hidden window and lengthy Accelerator table
- Flexible network connectivity – proxy support for use with victim systems situated behind isolated networks
- GET and POST network code for exfiltrating system information
- Log file capabilities
- File search and file write primitives – identifying and collecting sensitive ondisk information
- Download and execute further arbitrary downloads
- Arbitrary inter-process launch and communication through named pipes
- Process privilege and token adjustments
- Anti-malware kill-process identification and termination
- Digital Certificate stealing and reuse for stealth SSL communications
- Network server listener

WinMM

MD5 – Filename	File Size	Compilation date	Linker version
c8c81cca4645e71213f2310cec6c277d - %temp%\wuauc1t.exe	118,784 bytes	2012.11.01 00:53:49	6.0

WinMM is a full-featured, simple backdoor. Its first actions upon installation are to collect user and system data and report them back to the C2 over http. It uses NetUserGetInfo to identify that it is running under an "Admin" account on the local system, then retrieves the system name and the version of the operating system that is running, including its service pack, and collects the system install date from the registry:

```
\\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\InstallDate
```

These values are built into a single string for reporting.

SslMM also maintains this code chunk and functionality but does not immediately invoke it like winMM. Also interesting and different from sslMM, are the decoy Word documents dropped by many of the winMM droppers. Images of these documents are shown in the Appendix. The documents are all written and formatted with a specially developed Myanmar2 True Type font, demonstrating the focus on politically-connected, native Myanmar speakers as targets. This font is not delivered by default with Microsoft Office. Instead, it must have been specifically installed by the attackers and then by the victims, otherwise the documents would not have displayed properly.

The backdoor maintains multiple primitive functionalities.

Setting a WH_CBT Windows hook for full activity spying (sslMM does not maintain this hooking functionality):

- File search and capture
- Process creation
- Keystroke capture

The backdoor is usually configured with primary and backup domains for C2 communications, although there are multiple known samples that maintain an IP address or only a single domain for communications with no backup. Communication is built to appear as though a web browser is simply making a request to a remote web server. Some of these backdoors are configured to use an unusual port for encrypted communications.

exe_exchange (used in attacks prior to ~2012)

MD5 – Filename	File Size	Compilation date	Linker version
6a82c153bd370250cc2fed89f1bb5c91 - %temp%\services.exe	69,632 bytes	2012-03-13 07:54:19	6.0

INJECTv1/INJECTRESOURCE

MD5 – Filename	File Size	Compilation date	Linker version
b295274423c91ad9e254475bf8edd459 - wmiprive.exe	159,744 bytes	May 27, 2013	

The xsPlus/nokian backdoor and keylogger

MD5 – Filename	File Size	Compilation date	Linker version
d86106faaa398b8d83437176bf5e39c4	281,624 bytes	2011.12.19 08:06:30	6.0

In 2014 the Naikon gang was found to be using another tool that maintains an internal name “xsPlus” and “xsControl”. This builder and its backdoors produce components with the “NOKIAN95/WEBx” user-agent strings, for which there are multiple versions. It’s functionality is covered in our previous Naikon APT post.

NAIKON AND MINOR LINKS WITH APT30

Another interesting aspect of the backdoor builder is that it also provides a keylogger plugin that is used on specific victim systems. And here there are minor, but striking, similarities with the APT30 tools.

Callback sessions for stolen data include these URLs:

POST /**stonehoof**.rar/user=xxx&password=xxx
GET /**stonehoof**.rar/user=xxx&password=xxx

Some of the collector components upload data in SQLite3 format, while earlier versions of the tool upload xml formatted data. Presenting a similarity with the APT30 artifacts, their callback domains included stonehoof.com, hosted on several IPs during the naikon campaigns. This name is very unusual, and it is an odd coincidence that it is shared by two geopolitically-focused cyber-espionage groups, both targeting the South China Sea region.

APT30 - **stonehoof**.com

2012-10-07	208.77.46.251	174.36.159.165
2013-04-03	174.36.159.165	219.90.115.251
2013-04-14	219.90.115.251	174.36.159.164

While the Msn**MM** components include the unusual "**MM**" in internal names ssl**MM**, win**MM**, and wininet**MM**, some of the strings in the APT30 GEMSTONE software include the same – search and retrieval of the registry key "Software\Microsoft\Get**MM**", and three function names "MicrosoftG**MM**Exit, MicrosoftG**MM**HaveExit, MicrosoftGMMZJ". The APT30 BACKSPACE backdoor also contains a similar potential target reference, as discussed in the FireEye paper.

"BACKSPACE Variant	Path	Possible Target
ZJ Auto (version 1.4)	/auto**MM**/	Myanmar"

So, the "**MM**" shared by both of these may be a simple reference to Myanmar, the starting target for these Naikon APT attacks.

APT30 backdoors also add "MSN.lnk" shortcuts to the Start Menu Startup location for persistence, just like the MsnMM components spoof "Msn Gaming Zone.lnk" and "Msn Talk.lnk" for persistence.

Sys10

MD5 – Filename	File Size	Compilation date	Linker version
c58df5892700ac3f467524f86bf325c0 - update.exe	116.5 kb	2013.02.01 07:39:12	9.0

Yet another backdoor was used throughout 2013 by Naikon. Several of the C2 domains are shared with either Naikon or MsnMM infrastructure. This backdoor is a very basic initial component. To give an idea of the sophistication of its development, one of the decryption schemes it uses is an xor 0x1 loop on the very beginning of its .data section to decrypt its C2 domain. In this case, 6C 6C 6A 62 66 2F 74 68 62 71 2F 6F 64 75 01 (lljbf/thbq/odu) → mmkcg.uicp.net.

This weak level of encryption is odd, because other strings, like the unicode version of the callback url "s.y.s.t.e.n.&.c.p.=.%.s.&.l.o.g.=.%.s.&.i.n.d.e.x.=.%.d.", are maintained in plaintext in the .rdata section. Perhaps the authors thought xor'ing the domains would hide their infrastructure for as long as needed, or they were working with others who didn't understand automated sandboxes and tracing but didn't want the dns strings present in the binary. It doesn't seem to make sense, but it appears to have been effective enough to leave in the executables.

For all of the "Sys10" backdoors, URL parameters were used consistently for the initial C2 callback:

systen&cp=&log=&index=

where: **cp** = system computername
log = signed decimal integer representation of the OS InstallDate
index = simply the return value from a GetTickCount call

The backdoor collects several bits of identifying information to send to the C2:

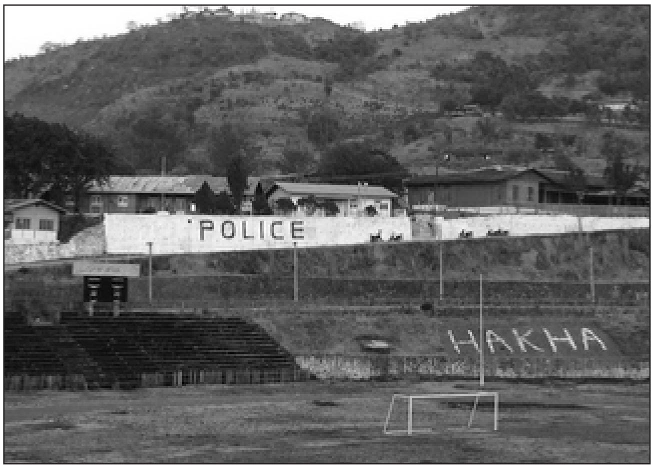
- computer name
- account name of logged-in user
- group name of logged-in user
- local IP address
- OS versioning information
- OS install date

The backdoor maintains a simple set of primitives:

- http-based communications with hardcoded C2
- download additional components
- start a new process
- terminate a running process
- find files and copy them
- delete files
- create files

We detected this backdoor on multiple victim workstations with the following verdicts:

```
Trojan.Win32.Agentb.hyb
Trojan.Win32.Agentb.iqj
Backdoor.Win32.MsnMM.p
UDS:DangerousObject.Multi.Generic
Trojan.Win32.Agentb.jwp
```



According to KSN (Kaspersky Security Network) data, almost all of the victims attacked with this backdoor are based in Myanmar, or were Myanmar delegates travelling through the other countries like the US, for example. Some of the victims were located in Vietnam and Singapore. Victim profiles range from global political representatives and local IT service companies, to government ministries controlling media and news content, university students, and local law enforcement agencies.

WininetMM/Sakto

MD5 – Filename	File Size	Compilation date	Linker version
516f64dd4fce3b9a325ea8501f97a88a	95,744 bytes	2014.11.03 07:59:14	9.0

SECOND STAGE TOOLS

Most of the Naikon APT's second stage tools detected on victim networks are publicly-available. Some are very common system administration tools and utilities, and some are less publicly-available custom written scanners and tools available through Chinese hacking forums. Their ability to move through networks undisturbed appears to have matured over time, demonstrating that they are a seasoned team:

- Windows system utilities: ftp.exe, systeminfo.exe, ipconfig, net view, ping, netstat -ano, net use, quser, tasklist, netsh interface ip, netsh interface show, netsh advfirewall firewall, reg export, AT
- Sysinternals: procmon.exe, tcpview.exe, procexep.exe, psexec
- Prosolve: winscan.exe
- Rarlabs: rar.exe
- Other: procex.exe, nc.exe, xscan.exe, winscanx.exe, hscan120.rar package (includes mysql.exe and sqlcmd.exe), cutfile.exe, tftp.exe, Win7 elevation of privilege and UAC bypass, ReadPSW.exe (password stealer)

The Naikon APT frequently used a custom backdoor that appears to be an HDoor variant, based on old "Honker Union" code like "hscan v120". For example, once on a victim network, one of the first steps is to run the hdoor -hbs scan to identify target local network hosts. Alternatively, it may show up on victim networks and be run with a long list of parameters:

```
"lms.dat -hscan 192.168.0.1-192.168.0.254 /a"
```

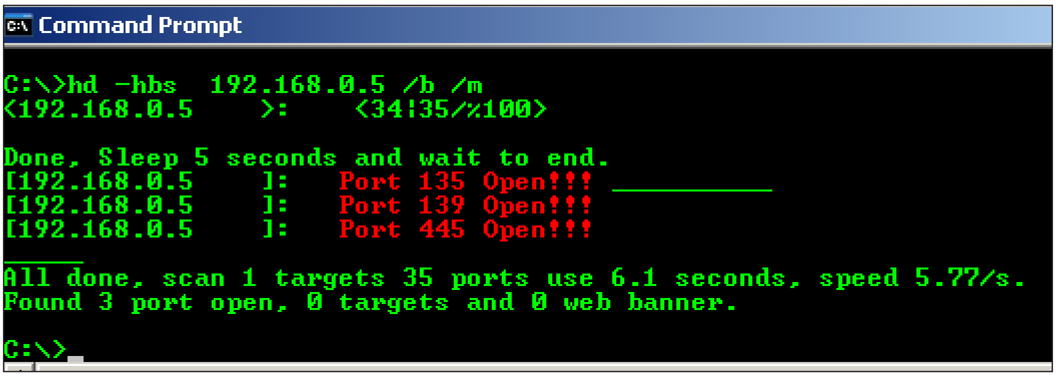
CUSTOM HDOOR

MD5 – Filename	File Size	Compilation date	Detection Name
bf6d3f52ab8176122be858ddccc22148 - lms.dat	56 kb	2015.05.20	HackTool.Win32.Agent.whj

The Naikon APT's custom-built HDoor tool is a robust reconnaissance tool for lateral movement, supporting the identification of, interfacing with and attacking of multiple technologies and resources:

- host, user, group, and related authentication resources and cracking/brute forcing capabilities
- network asset scanning and identification, including SQL database, embedded network devices like home or SMB routers, and other common network services
- fake service listener to sniff traffic
- disk wiping – safe delete with multiple overwrites
- process management
- local filetime modifier
- SQL administration toolset
- SOCKS5 proxy service
- banner-based scanner
- AV killer

Publicly-available hd.exe (40138f3db14e6e137f8d0bdcbb5851d8), as posted by NCPH:

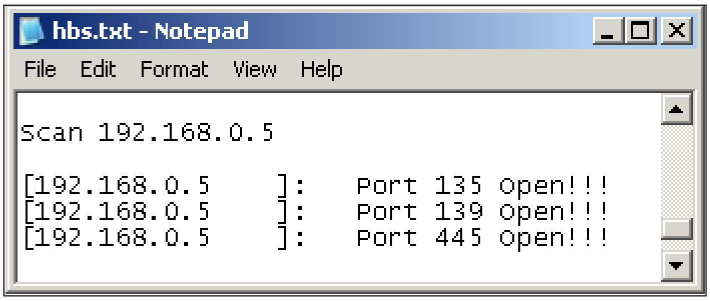


```
C:\>hd -hbs  192.168.0.5 /b /m
<192.168.0.5    >:    <34!35/%100>

Done, Sleep 5 seconds and wait to end.
[192.168.0.5    ]:    Port 135 Open!!! __________
[192.168.0.5    ]:    Port 139 Open!!!
[192.168.0.5    ]:    Port 445 Open!!!
_____
All done, scan 1 targets 35 ports use 6.1 seconds, speed 5.77/s.
Found 3 port open, 0 targets and 0 web banner.

C:\>_
```

The corresponding hbs.txt output file content that is sometimes left behind on victim systems:



```
Scan 192.168.0.5

[192.168.0.5     ]:    Port 135 Open!!!
[192.168.0.5     ]:    Port 139 Open!!!
[192.168.0.5     ]:    Port 445 Open!!!
```

The operator’s scanning is somewhat inconsistent. They will scan for a specific set of ports that include 21,22,80,3389,1433,3306, and 389. Sometimes, they add 139 and 445 to the end of that list. Often, they check for a “PortString”, or banner, which is output to a txt file:

```
[10.1.1.2 ]: Port 22 Open!!! SSH-1.99-Cisco-1.25
[10.1.1.3 ]: Port 21 Open!!! 220-FileZilla Server version 0.9.41 beta
[10.1.1.4 ]: Port 21 Open!!! 220 Lexmark X860de FTP Server NP.APS.N332a ready.
[10.1.1.5 ]: Port 22 Open!!! SSH-2.0-OpenSSH_5.8
[10.1.1.6 ]: Port 22 Open!!! SSH-2.0-dropbear_0.48
[10.1.1.7 ]: Port 21 Open!!! 220 Service ready for new user
[10.1.1.8 ]: Port 21 Open!!! 220 Microsoft FTP Service (Version 5.0).
[10.1.1.8 ]: Port 80 Open!!!
[10.1.1.8 ]: Port 3389 Open!!!
[10.1.1.8 ]: Port 139 Open!!!
[10.1.1.9 ]: Port 21 Open!!! 220 fima FTP server (SunOS 5.8) ready.
[10.1.1.10 ]: Port 21 Open!!! 220 (vsFTPd 2.0.5)
[10.1.1.13 ]: Port 21 Open!!! 220 EthernetBoard OkiLAN 8100e Ver 02.15 FTP server.
[10.1.1.15 ]: Port 22 Open!!! SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
[10.1.1.21 ]: Port 80 Open!!! http://10.1.1.21/cgi-bin/webproc Dlink WIRELESS AP
```

TARGET AND VICTIM PROFILES

Target profiles included high profile government and military agencies around the South China Sea:

- Law enforcement
- Government – executive, administrative, regulatory
- Military – operations centers
- Economic administration
- State media
- Public/Private energy
- Shared Victims with Cycldek and Comparing Lateral Movement with Cycldek

The Cycldek APT appeared to follow an operational script across victim systems. It created or used c:\intel on the victim hard disk to unpack tools and compress/archive stolen victim files and data with Winrar, like "c:\intel\1.rar". Some of these victim systems were occupied by both the Cycldec and Naikon attackers.

The Cycldek attackers maintained this c:\intel directory and its subdirectories as a sort of staging point. This mirrors what we have seen with Naikon directory setup on some victims.

- a set of subdirectories
- stolen files for exfiltration
- operational logs
- process logs
- Cycldek tools and their config files

The Naikon APT and Cycldek APT also share a common attraction to Honker Union codebase.

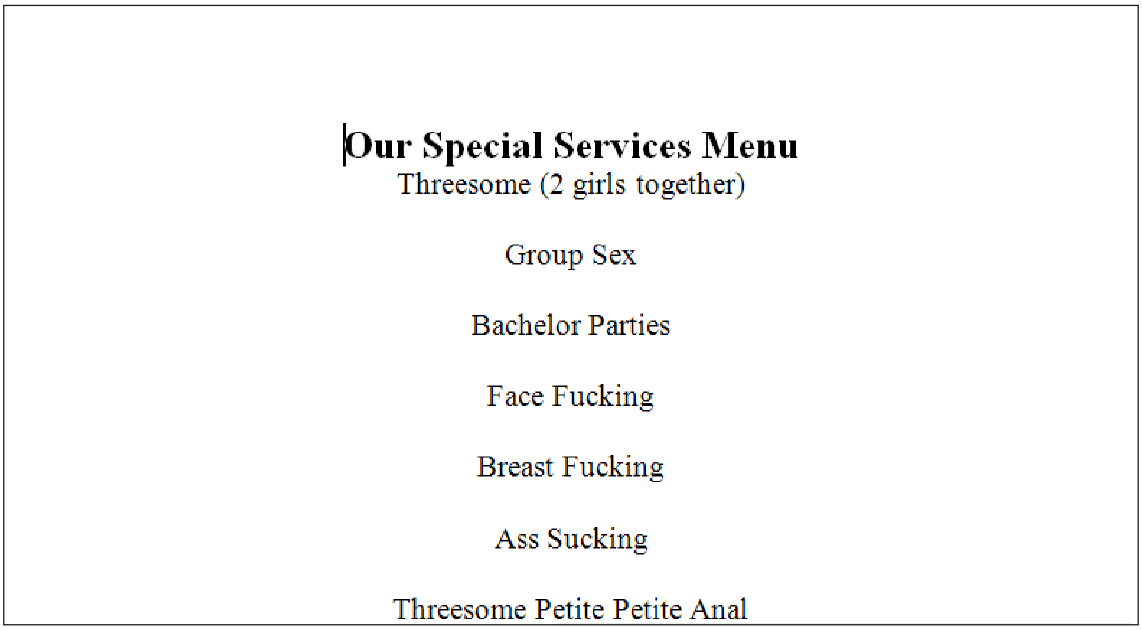
SPEAR-PHISH, DROPPED FILES, WEB BROWSER INJECTION

The common sequence of events on a vulnerable system falling for related spear-phish attacks led to a newly-created Internet Explorer process running with execution transferred to additionally loaded executable code, usually profile.dat, maintaining the connectback C2 communication code and data.

In this instance, a "naikon backdoor" was delivered initially as a part of a small package of objects. The exploit attachment dropped iph.bat, iExplorer.exe, and a clean decoy document. The exploit executed this batch file, which in turn executed iExplorer.exe and opened a decoy document from %temp%. The iExplorer.exe process wrote out a profile.dat file, launched the legitimate Internet Explorer, and injected the .dat file into this newly created browser process. It transfered control to the injected .dat code and terminated itself. The .dat code then connected with a hardcoded C2 from within Internet Explorer, a common technique for evading any outbound traffic firewall issues.

The full email spear-phish and other decoy documents' content presented here display the campaigns' focus on ASEAN targets that line up with the MsnMM campaigns.

Example spear-phish and dropped sequence for NOKIAN95/WEB sent to web email service provider users in the US and Southeastern Asian region:



Our Special Services Menu
Threesome (2 girls together)

Group Sex

Bachelor Parties

Face Fucking

Breast Fucking

Ass Sucking

Threesome Petite Petite Anal

Example Word document decoy

Example details, exhibiting the “common” sequence of events on systems:

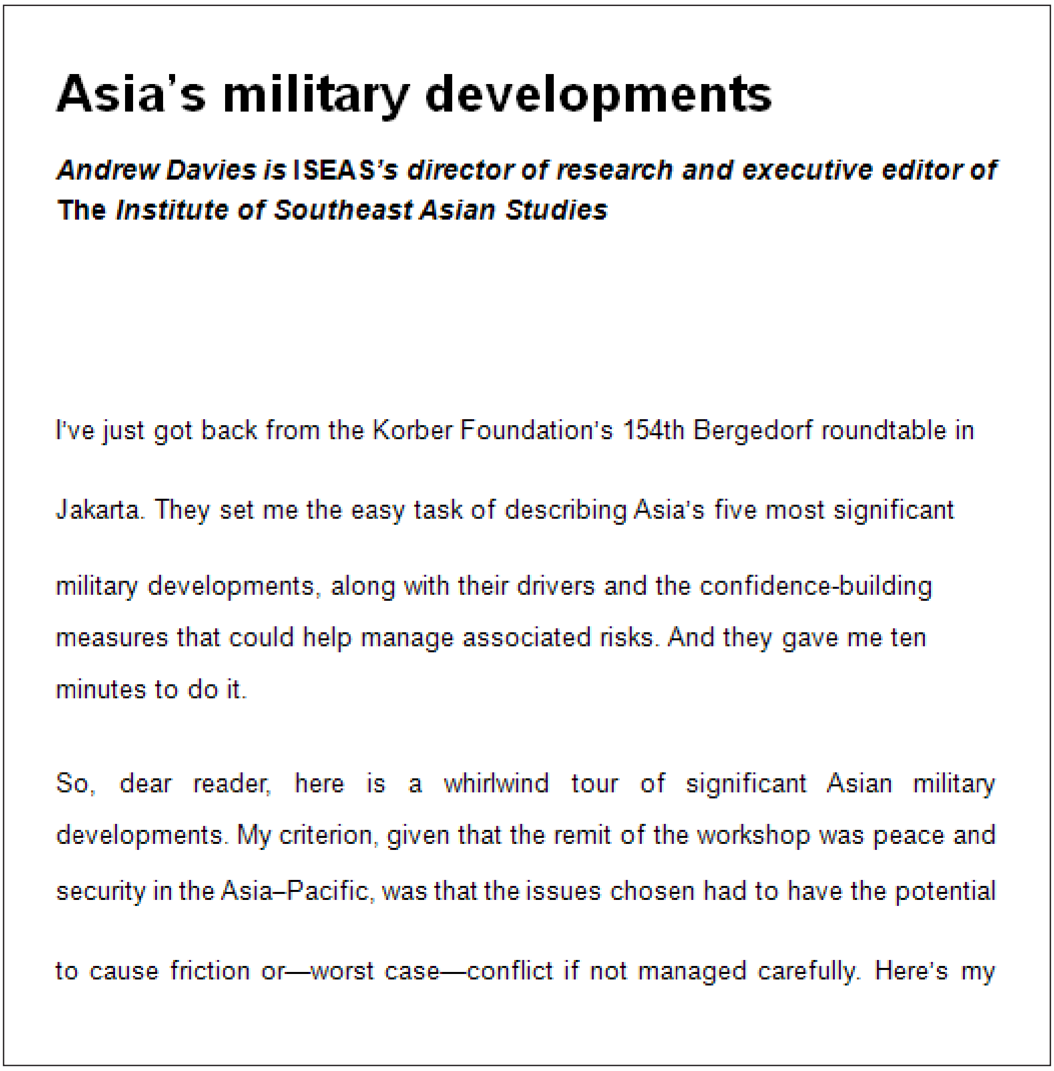
c334737ea5e8f74567bfdc2fce6717b9,2 SpecialServices.doc

Drops → %temp%\iph.bat
c8ed40879e1e3352692fe8c765294955,%temp%\svchost.exe
c8ed40879e1e3352692fe8c765294955,C:\WINDOWS\system32\ymsgr_tray.exe

C2: frankhere.oicp.net:443

1b37457632840b04bf03e0745e51e573,readme.rtf

Drops → %temp%\iph.bat → %temp%\iExplorer.exe WMcal
6cbc73fae7118dbd0fae328ce8ee6050,iExplorer.exe,Trojan-Downloader.Win32.Cordmix.cu
C2: phsenator.vicp.net
C2: goihang.vicp.net:443



Asia's military developments

Andrew Davies is ISEAS's director of research and executive editor of The Institute of Southeast Asian Studies

I've just got back from the Korber Foundation's 154th Bergedorf roundtable in Jakarta. They set me the easy task of describing Asia's five most significant military developments, along with their drivers and the confidence-building measures that could help manage associated risks. And they gave me ten minutes to do it.

So, dear reader, here is a whirlwind tour of significant Asian military developments. My criterion, given that the remit of the workshop was peace and security in the Asia–Pacific, was that the issues chosen had to have the potential to cause friction or—worst case—conflict if not managed carefully. Here's my

Example decoy Word document

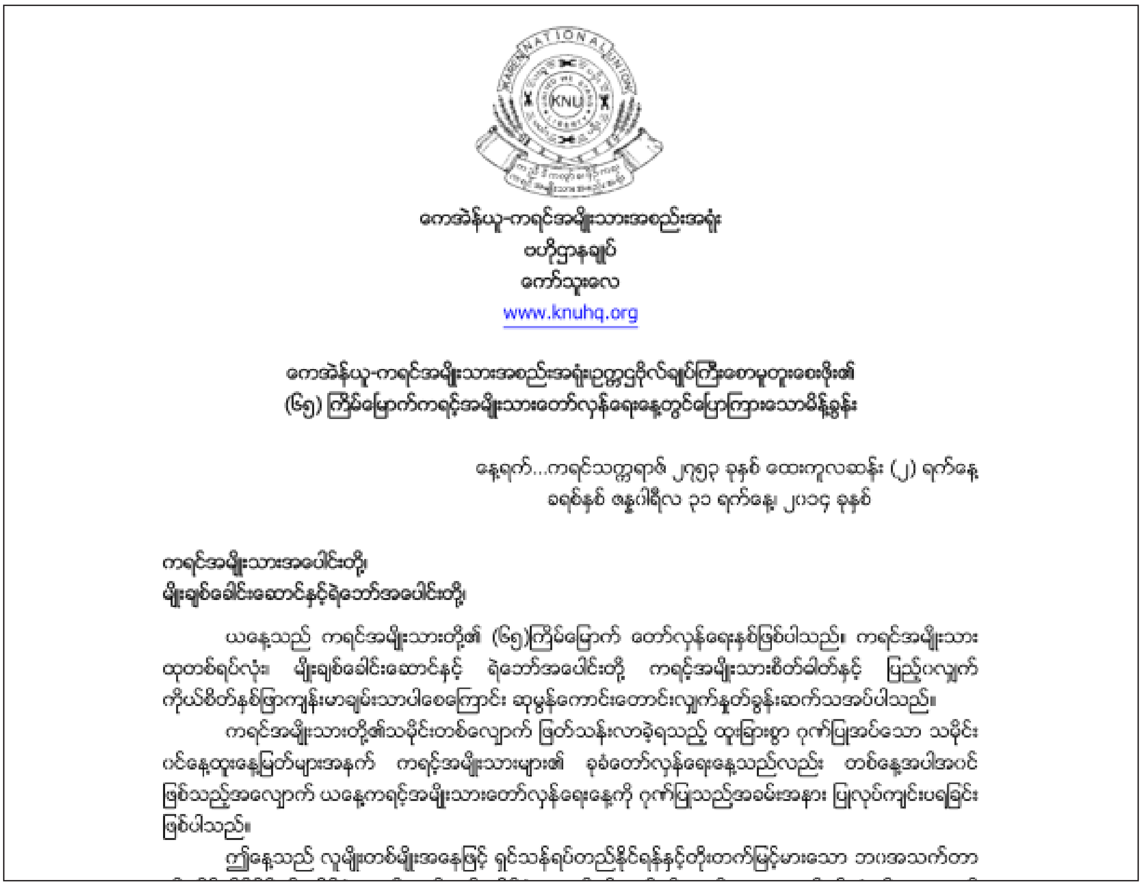
cb72e70378755f1e8ab744a5b5e692bd,Asia's Military Developments.doc (ripped from "Australian Strategic Policy Institute" blog post located here – http://www.aspistrategist.org.au/asias-military-developments/)

638c119a82a1b1d470e42e2e9712f3fb,iph.bat
79de618615e139053ad92ca1e7bb7456,C:\Documents and Settings\user\Local Settings\Temp\mshtml.dat

4299846c34fddda2f5a75239f8aca424,C:\DOCUME~1\user\LOCALS~1\Temp\upd.exe
Rpcss

a3b3a32b6f67e4629133cc4578230efe,C:\WINDOWS\system32\msictl.exe

C2: us.googlereader.pw:443



ကေအဲန်ယူ-ကရင်အမျိုးသားအစည်းအရုံး
ဗဟိုဌာနချုပ်
ကော်သူးလေ
www.knuhq.org

ကေအဲန်ယူ-ကရင်အမျိုးသားအစည်းအရုံးဉက္ကဌဗိုလ်ချုပ်ကြီးစောမူတူးစေးဖိုး၏
(၆၅) ကြိမ်မြောက်ကရင့်အမျိုးသားတော်လှန်ရေးနေ့တွင်ပြောကြားသောမိန့်ခွန်း

နေ့ရက်...ကရင်သက္ကရာဇ် ၂၇၅၃ ခုနှစ် ထေးကူလဆန်း (၂) ရက်နေ့
ခရစ်နှစ် ဇန်နဝါရီလ ၃၁ ရက်နေ့၊ ၂၀၁၄ ခုနှစ်

ကရင်အမျိုးသားအပေါင်းတို့၊
မျိုးချစ်ခေါင်းဆောင်နှင့်ရဲဘော်အပေါင်းတို့၊

ယနေ့သည် ကရင်အမျိုးသားတို့၏ (၆၅)ကြိမ်မြောက် တော်လှန်ရေးနေ့ဖြစ်ပါသည်။ ကရင်အမျိုးသားထုတစ်ရပ်လုံး၊ မျိုးချစ်ခေါင်းဆောင်နှင့် ရဲဘော်အပေါင်းတို့ ကရင့်အမျိုးသားစိတ်ဓါတ်နှင့် ပြည့်ဝလျက် ကိုယ်စိတ်နှစ်ဖြာကျန်းမာချမ်းသာပါစေကြောင်း ဆုမွန်ကောင်းတောင်းလျက်နှုတ်ခွန်းဆက်သအပ်ပါသည်။

ကရင်အမျိုးသားတို့၏သမိုင်းတစ်လျှောက် ဖြတ်သန်းလာခဲ့ရသည့် ထူးခြားစွာ ဂုဏ်ပြုအပ်သော သမိုင်းဝင်နေ့ထူးနေ့မြတ်များအနက် ကရင့်အမျိုးသားများ၏ ခုခံတော်လှန်ရေးနေ့သည်လည်း တစ်နေ့အပါအဝင်ဖြစ်သည့်အလျောက် ယနေ့ကရင့်အမျိုးသားတော်လှန်ရေးနေ့ကို ဂုဏ်ပြုသည့်အခမ်းအနား ပြုလုပ်ကျင်းပခြင်းဖြစ်ပါသည်။

ဤနေ့သည် လူမျိုးတစ်မျိုးအနေဖြင့် ရှင်သန်ရပ်တည်နိုင်ရန်နှင့်တိုးတက်မြင့်မားသော ဘဝအသက်တာ

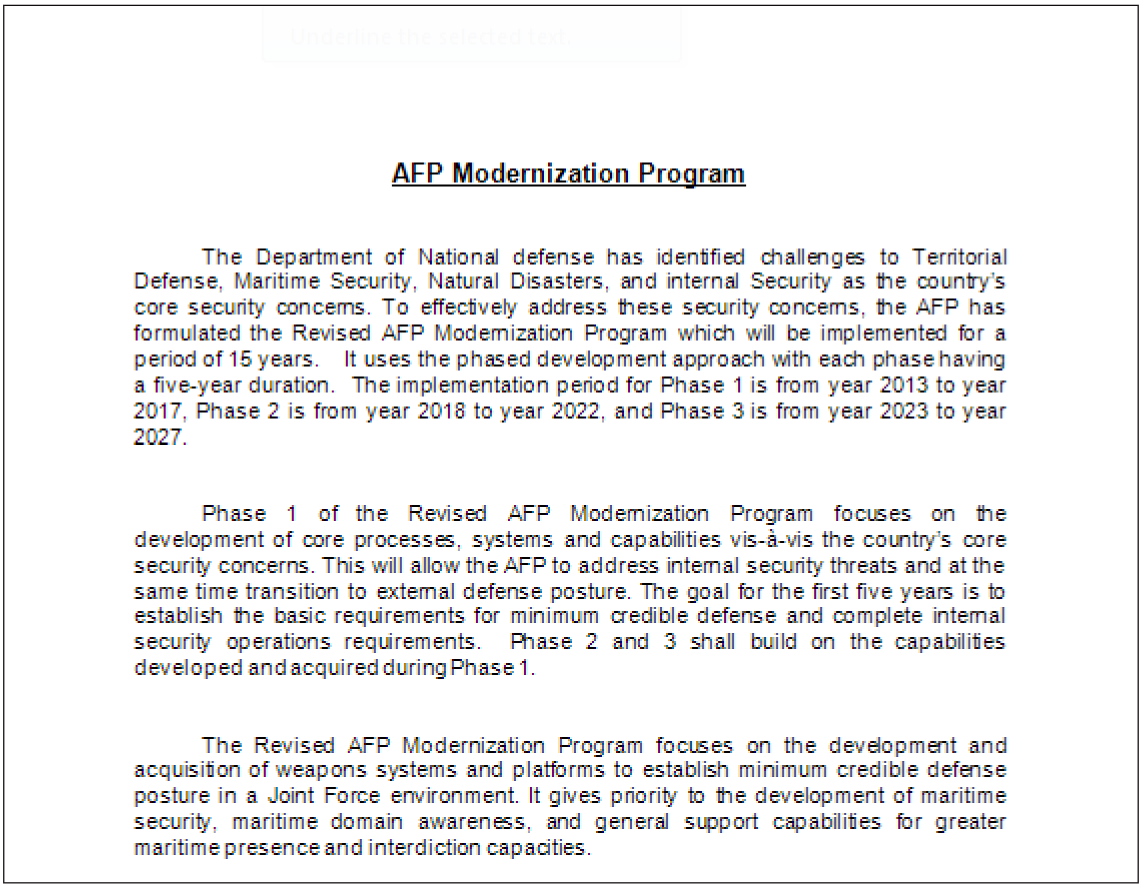
Example decoy pdf targeting Myanmar government

5f1f6fb3cea3e9c3bd84909b7d37aa8d, ”knu president speech on 65th anniversary of karen resistance day _burmese language_?fdp.scr” ← indicates RTLO naming, appeared to the target as pdf “knu president speech on 65th anniversary of karen resistance day _burmese language_rcs.pdf”

55b8b8779001b7e78a6adc55fb546401,C:\DOCUME~1\user\LOCALS~1\Temp\update.exe

8660193a90e70f19a4419ae09306761f,C:\DOCUME~1\user\LOCALS~1\Temp\adobe.pdf

C2: ubaoyouxiang.gicp.net



Underline the selected text.

AFP Modernization Program

The Department of National defense has identified challenges to Territorial Defense, Maritime Security, Natural Disasters, and internal Security as the country's core security concerns. To effectively address these security concerns, the AFP has formulated the Revised AFP Modernization Program which will be implemented for a period of 15 years. It uses the phased development approach with each phase having a five-year duration. The implementation period for Phase 1 is from year 2013 to year 2017, Phase 2 is from year 2018 to year 2022, and Phase 3 is from year 2023 to year 2027.

Phase 1 of the Revised AFP Modernization Program focuses on the development of core processes, systems and capabilities vis-à-vis the country's core security concerns. This will allow the AFP to address internal security threats and at the same time transition to external defense posture. The goal for the first five years is to establish the basic requirements for minimum credible defense and complete internal security operations requirements. Phase 2 and 3 shall build on the capabilities developed and acquired during Phase 1.

The Revised AFP Modernization Program focuses on the development and acquisition of weapons systems and platforms to establish minimum credible defense posture in a Joint Force environment. It gives priority to the development of maritime security, maritime domain awareness, and general support capabilities for greater maritime presence and interdiction capacities.

Example decoy Word document targeting PH gov

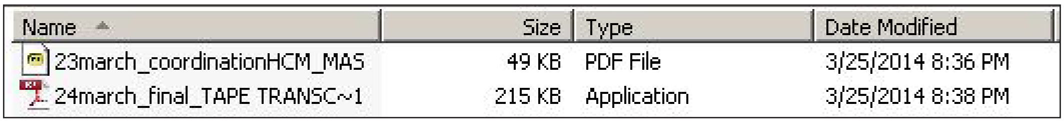
27ed7c7dd840ff7936418cf029d56603,
AFP Summary.doc à → temp%\iph.bat

ceb6e4499cfd8650f3e94fbcf7de48f6,%temp%\iExplorer.exe WMcal
b6424852dd0187ea554a1cbc4e3490f3,%temp%\profile.dat

C2: ttteco.vicp.net

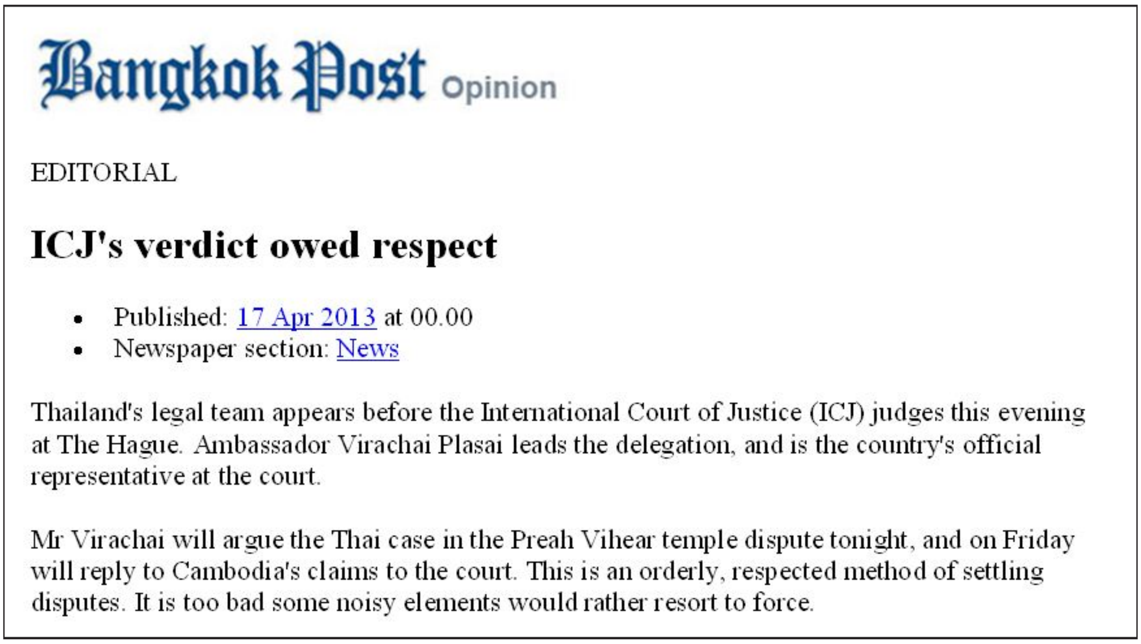
Many of these backdoors were delivered by simply binding decoy pdfs to a Naikon backdoor and sending this bundle to target addresses. Here is a March 2014 spear-phish email with the subject line "Fw: Fw: tape transcript for mh370" (3bed6788753690762c7d15a3247d8301):

The "tape transcript.zip" (5de5aa40eb3d30df2053a38bc26963b5) file contains both a pdf file and a Naikon dropper name "24march_final_TAPE TRANSC~1" detected as "Trojan-Dropper.Win32.Injector.kasl" (4972c7205e3279322637f609b9199e97). The dropper maintains a clean copy of this decoy pdf that opens on execution, [as well as?] the Naikon backdoor (ab0185f3dc730af754559297f6f47492) and accompanying mshtml.dat component (03A3251BDE74DF30AB5BF0B730E08C8D) that communicates with C2 xl.findmy.pw. This dropper is built with the attackers' "pdfBind 2012" tool. Once extracted to disk, you can see that the icon was replaced for the executable with an Adobe pdf icon. Lots of users fall for this sort of trick when file extensions are not visible:



Name	Size	Type	Date Modified
23march_coordinationHCM_MAS	49 KB	PDF File	3/25/2014 8:36 PM
24march_final_TAPE TRANSC~1	215 KB	Application	3/25/2014 8:38 PM

APPENDIX A: MsnMM SPEAR-PHISH AND DECOY CONTENT



Bangkok Post Opinion

EDITORIAL

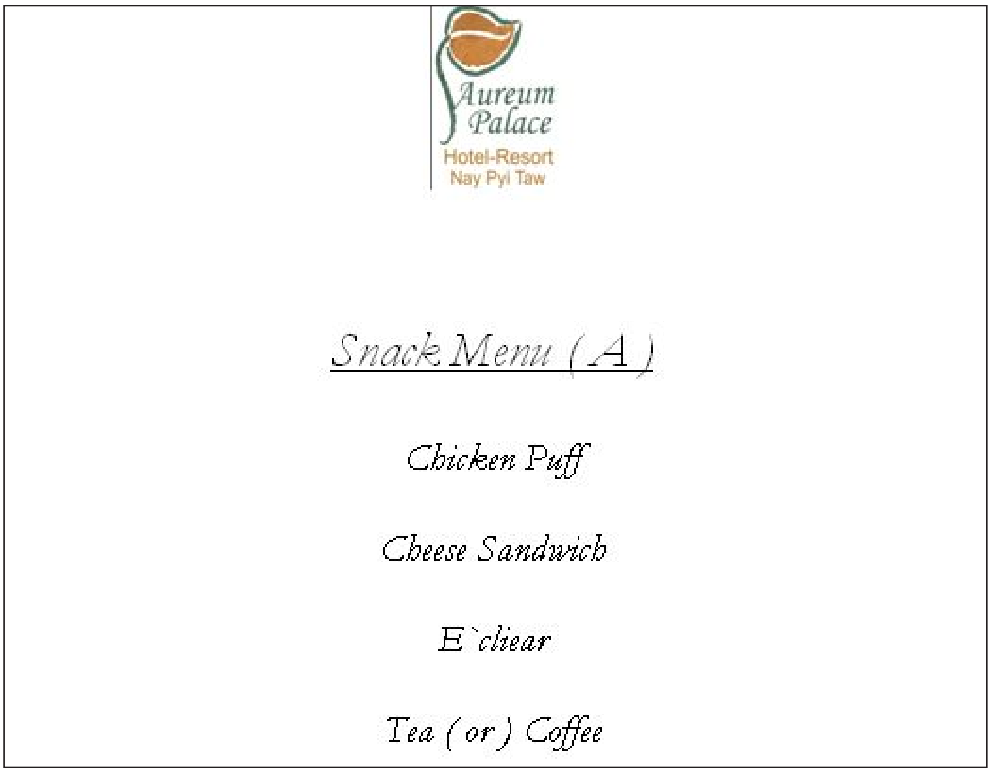
ICJ's verdict owed respect

- Published: 17 Apr 2013 at 00.00
- Newspaper section: News

Thailand's legal team appears before the International Court of Justice (ICJ) judges this evening at The Hague. Ambassador Virachai Plasai leads the delegation, and is the country's official representative at the court.

Mr Virachai will argue the Thai case in the Preah Vihear temple dispute tonight, and on Friday will reply to Cambodia's claims to the court. This is an orderly, respected method of settling disputes. It is too bad some noisy elements would rather resort to force.

Image 1. "ICJ's verdict owed respect 17 Apr 2013.doc"



Aureum Palace
Hotel-Resort
Nay Pyi Taw

Snack Menu (A)

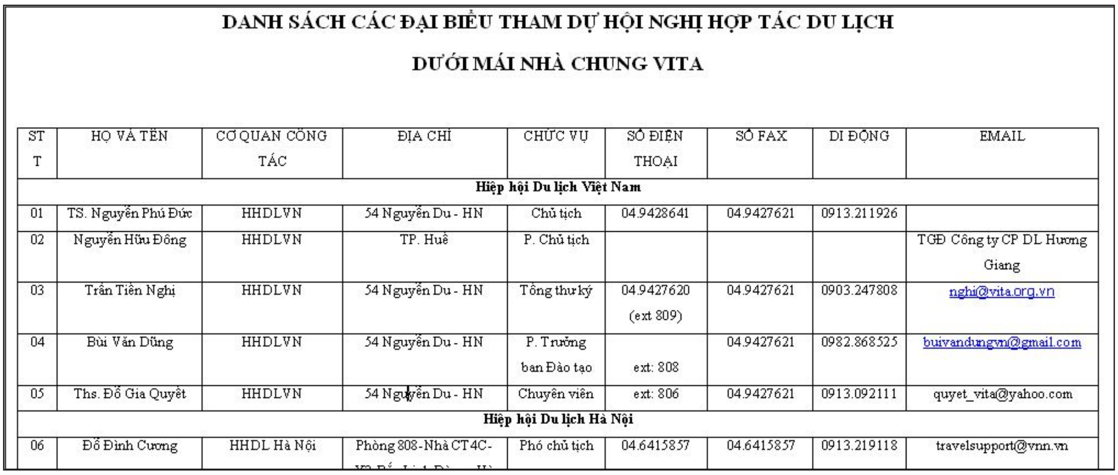
Chicken Puff

Cheese Sandwich

E`cliear

Tea (or) Coffee

Image 2. "FDI Law Weeding Menu.doc"

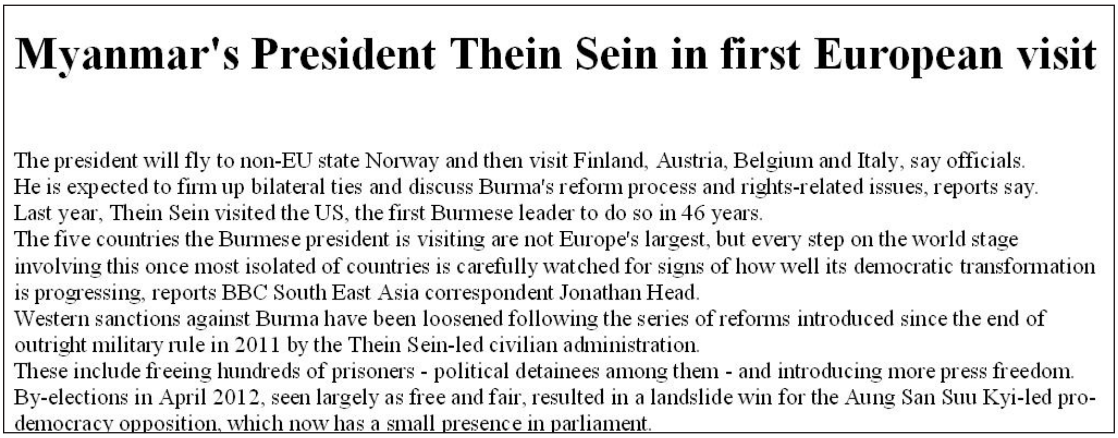


DANH SÁCH CÁC ĐẠI BIỂU THAM DỰ HỘI NGHỊ HỢP TÁC DU LỊCH

DƯỚI MÁI NHÀ CHUNG VITA

STT	HỌ VÀ TÊN	CƠ QUAN CÔNG TÁC	ĐỊA CHỈ	CHỨC VỤ	SỐ ĐIỆN THOẠI	SỐ FAX	DI ĐỘNG	EMAIL
Hiệp hội Du lịch Việt Nam								
01	TS. Nguyễn Phú Đức	HHDLVN	54 Nguyễn Du - HN	Chủ tịch	04.9428641	04.9427621	0913.211926	
02	Nguyễn Hữu Đông	HHDLVN	TP. Huế	P. Chủ tịch				TGĐ Công ty CP DL Hương Giang
03	Trần Tiến Nghị	HHDLVN	54 Nguyễn Du - HN	Tổng thư ký	04.9427620 (ext 809)	04.9427621	0903.247808	nghi@vita.org.vn
04	Bùi Văn Dũng	HHDLVN	54 Nguyễn Du - HN	P. Trưởng ban Đào tạo	ext: 808	04.9427621	0982.868525	buivandungvn@gmail.com
05	Ths. Đỗ Gia Quyết	HHDLVN	54 Nguyễn Du - HN	Chuyên viên	ext: 806	04.9427621	0913.092111	quyet_vita@yahoo.com
Hiệp hội Du lịch Hà Nội								
06	Đỗ Đình Cương	HHDL Hà Nội	Phòng 808-Nhà CT4C-	Phó chủ tịch	04.6415857	04.6415857	0913.219118	travelsupport@vnn.vn

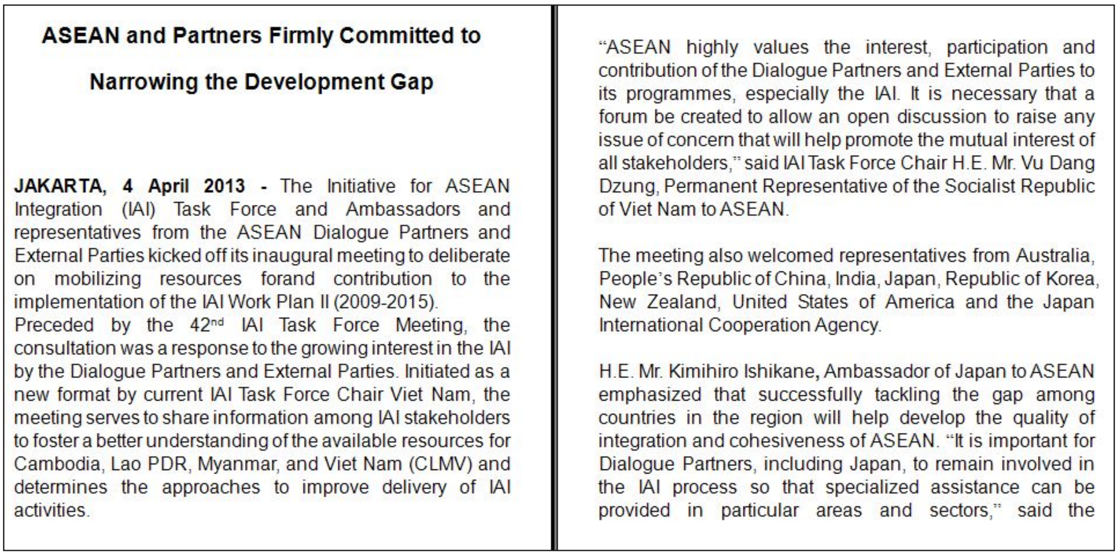
Image 3. “Danh sach dai bieu HNHTDMNC tai TPHCM.doc”



Myanmar's President Thein Sein in first European visit

The president will fly to non-EU state Norway and then visit Finland, Austria, Belgium and Italy, say officials.
He is expected to firm up bilateral ties and discuss Burma's reform process and rights-related issues, reports say.
Last year, Thein Sein visited the US, the first Burmese leader to do so in 46 years.
The five countries the Burmese president is visiting are not Europe's largest, but every step on the world stage involving this once most isolated of countries is carefully watched for signs of how well its democratic transformation is progressing, reports BBC South East Asia correspondent Jonathan Head.
Western sanctions against Burma have been loosened following the series of reforms introduced since the end of outright military rule in 2011 by the Thein Sein-led civilian administration.
These include freeing hundreds of prisoners - political detainees among them - and introducing more press freedom.
By-elections in April 2012, seen largely as free and fair, resulted in a landslide win for the Aung San Suu Kyi-led pro-democracy opposition, which now has a small presence in parliament.

Image 4. “Thein Sein first European tour.doc”



ASEAN and Partners Firmly Committed to Narrowing the Development Gap

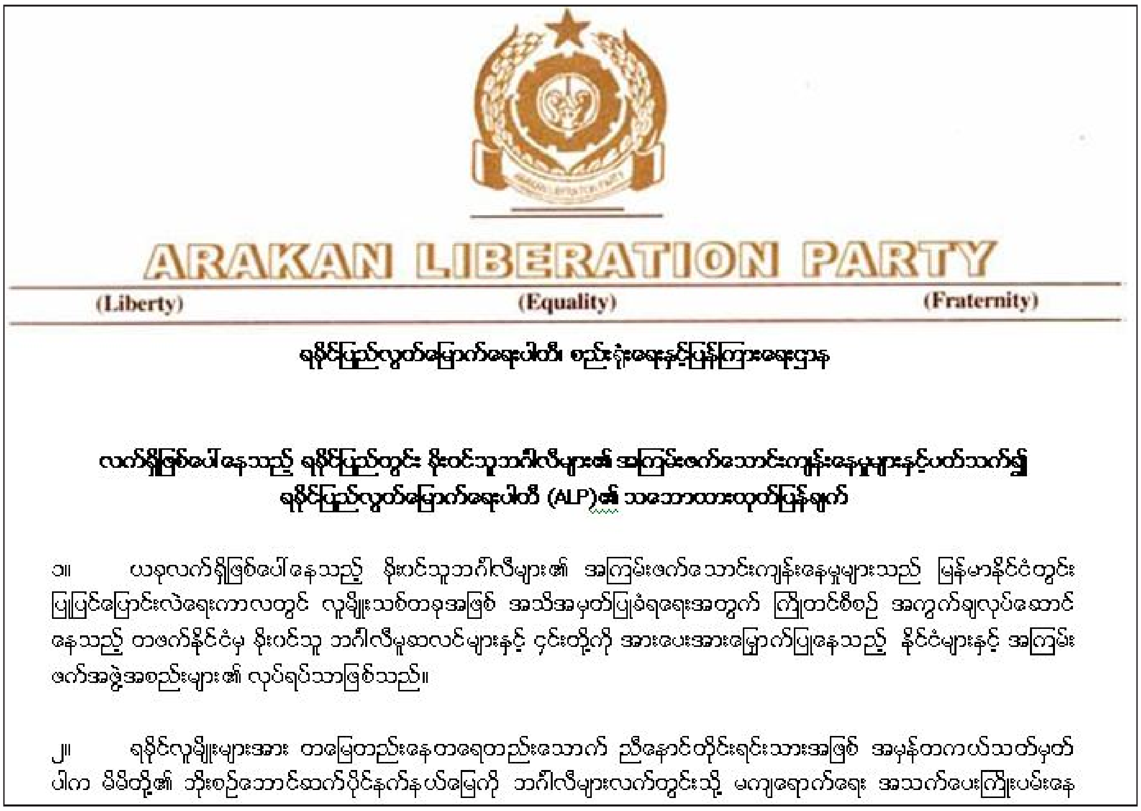
JAKARTA, 4 April 2013 - The Initiative for ASEAN Integration (IAI) Task Force and Ambassadors and representatives from the ASEAN Dialogue Partners and External Parties kicked off its inaugural meeting to deliberate on mobilizing resources forand contribution to the implementation of the IAI Work Plan II (2009-2015).
Preceded by the 42nd IAI Task Force Meeting, the consultation was a response to the growing interest in the IAI by the Dialogue Partners and External Parties. Initiated as a new format by current IAI Task Force Chair Viet Nam, the meeting serves to share information among IAI stakeholders to foster a better understanding of the available resources for Cambodia, Lao PDR, Myanmar, and Viet Nam (CLMV) and determines the approaches to improve delivery of IAI activities.

“ASEAN highly values the interest, participation and contribution of the Dialogue Partners and External Parties to its programmes, especially the IAI. It is necessary that a forum be created to allow an open discussion to raise any issue of concern that will help promote the mutual interest of all stakeholders,” said IAI Task Force Chair H.E. Mr. Vu Dang Dzung, Permanent Representative of the Socialist Republic of Viet Nam to ASEAN.

The meeting also welcomed representatives from Australia, People’s Republic of China, India, Japan, Republic of Korea, New Zealand, United States of America and the Japan International Cooperation Agency.

H.E. Mr. Kimihiro Ishikane, Ambassador of Japan to ASEAN emphasized that successfully tackling the gap among countries in the region will help develop the quality of integration and cohesiveness of ASEAN. “It is important for Dialogue Partners, including Japan, to remain involved in the IAI process so that specialized assistance can be provided in particular areas and sectors,” said the

Image 5. “ASEAN and Partners Firmly Committed To Narrowing Development Gap.doc”



ARAKAN LIBERATION PARTY

(Liberty) (Equality) (Fraternity)

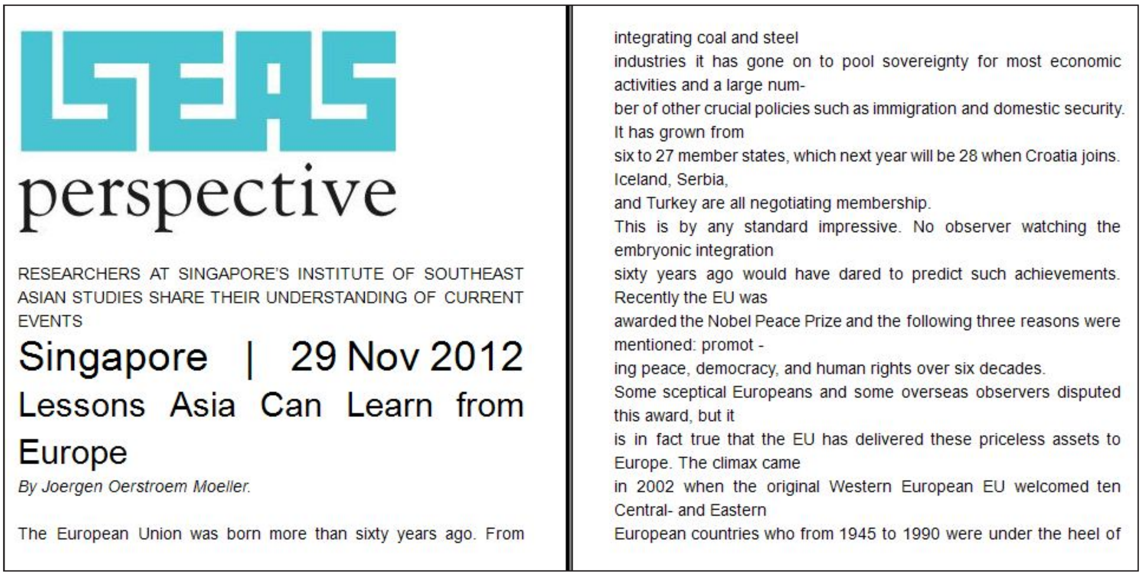
ရခိုင်ပြည်လွတ်မြောက်ရေးပါတီ၊ စည်းရုံးရေးနှင့်ပြန်ကြားရေးဌာန

လက်ရှိဖြစ်ပေါ်နေသည့် ရခိုင်ပြည်တွင်း ခိုးဝင်သူဘင်္ဂါလီများ၏ အကြမ်းဖက်သောင်းကျန်းနေမှုများနှင့်ပတ်သက်၍
ရခိုင်ပြည်လွတ်မြောက်ရေးပါတီ (ALP)၏ သဘောထားထုတ်ပြန်ချက်

၁။ ယခုလက်ရှိဖြစ်ပေါ်နေသည့် ခိုးဝင်သူဘင်္ဂါလီများ၏ အကြမ်းဖက်သောင်းကျန်းနေမှုများသည် မြန်မာနိုင်ငံတွင်း ပြုပြင်ပြောင်းလဲရေးကာလတွင် လူမျိုးသစ်တခုအဖြစ် အသိအမှတ်ပြုခံရရေးအတွက် ကြိုတင်စီစဉ် အကွက်ချလုပ်ဆောင် နေသည့် တဖက်နိုင်ငံမှ ခိုးဝင်သူ ဘင်္ဂါလီမူဆလင်များနှင့် ၎င်းတို့ကို အားပေးအားမြှောက်ပြုနေသည့် နိုင်ငံများနှင့် အကြမ်းဖက်အဖွဲ့အစည်းများ၏ လုပ်ရပ်သာဖြစ်သည်။

၂။ ရခိုင်လူမျိုးများအား တမြေတည်းနေတရေတည်းသောက် ညီနောင်တိုင်းရင်းသားအဖြစ် အမှန်တကယ်သတ်မှတ် ပါက မိမိတို့၏ ဘိုးစဉ်ဘောင်ဆက်ပိုင်နက်နယ်မြေကို ဘင်္ဂါလီများလက်တွင်းသို့ မကျရောက်ရေး အသက်ပေးကြိုးပမ်းနေ

Image 6. "ALP Statement on Present Illegal Bangali Problem inside Arakan.doc"



ISEAS perspective

RESEARCHERS AT SINGAPORE'S INSTITUTE OF SOUTHEAST ASIAN STUDIES SHARE THEIR UNDERSTANDING OF CURRENT EVENTS

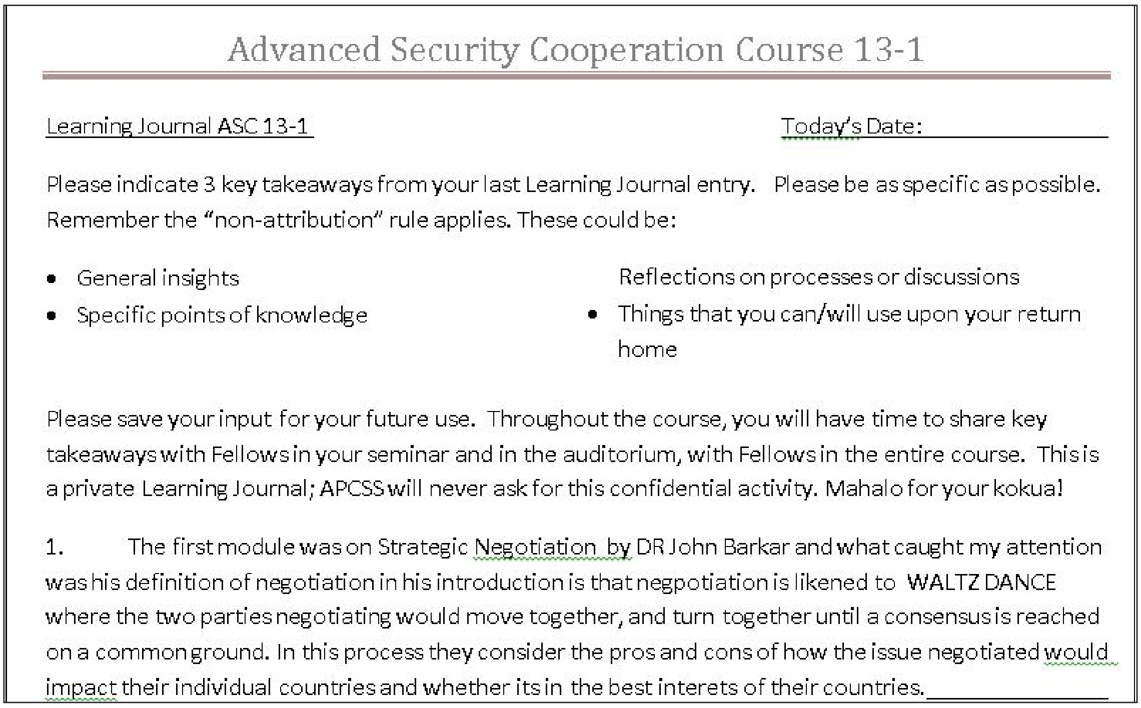
Singapore | 29 Nov 2012

Lessons Asia Can Learn from Europe

By Joergen Oerstroem Moeller.

The European Union was born more than sixty years ago. From integrating coal and steel
industries it has gone on to pool sovereignty for most economic activities and a large num-
ber of other crucial policies such as immigration and domestic security.
It has grown from
six to 27 member states, which next year will be 28 when Croatia joins.
Iceland, Serbia,
and Turkey are all negotiating membership.
This is by any standard impressive. No observer watching the embryonic integration
sixty years ago would have dared to predict such achievements.
Recently the EU was
awarded the Nobel Peace Prize and the following three reasons were mentioned: promot -
ing peace, democracy, and human rights over six decades.
Some sceptical Europeans and some overseas observers disputed this award, but it
is in fact true that the EU has delivered these priceless assets to Europe. The climax came
in 2002 when the original Western European EU welcomed ten Central- and Eastern
European countries who from 1945 to 1990 were under the heel of

Image 7. "ISEAS Perspective 29nov12.doc"



Advanced Security Cooperation Course 13-1

Learning Journal ASC 13-1 Today's Date:

Please indicate 3 key takeaways from your last Learning Journal entry. Please be as specific as possible. Remember the "non-attribution" rule applies. These could be:

- General insights
- Specific points of knowledge

Reflections on processes or discussions

- Things that you can/will use upon your return home

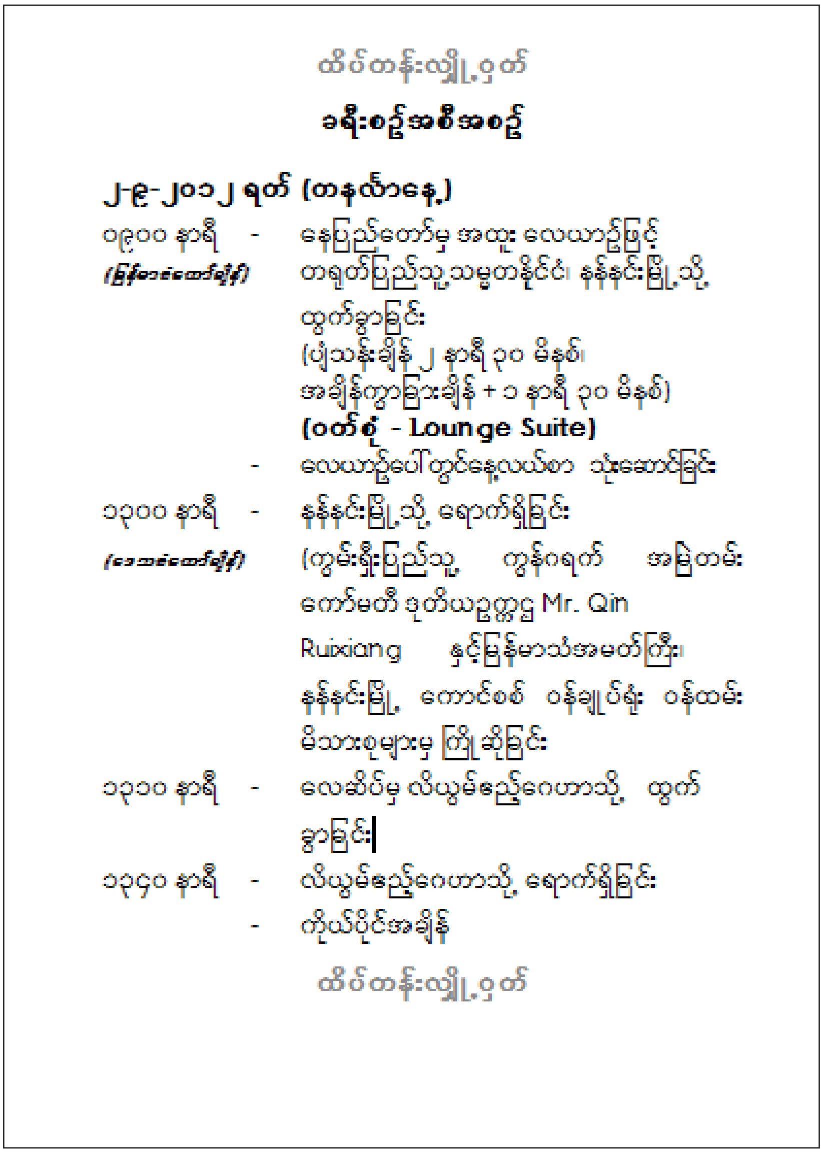
Please save your input for your future use. Throughout the course, you will have time to share key takeaways with Fellows in your seminar and in the auditorium, with Fellows in the entire course. This is a private Learning Journal; APCSS will never ask for this confidential activity. Mahalo for your kokua!

1. The first module was on Strategic Negotiation by DR John Barkar and what caught my attention was his definition of negotiation in his introduction is that negpotiation is likened to WALTZ DANCE where the two parties negotiating would move together, and turn together until a consensus is reached on a common ground. In this process they consider the pros and cons of how the issue negotiated would impact their individual countries and whether its in the best interests of their countries.

Image 8. "Learning Journal ASC 13-1_1.doc"
(related to http://www.apcss.org/wp-content/uploads/2013/01/finalfinalhandbookJan13.pdf, http://www.apcss.org/)

Image 9. unnamed.jpg
48c2d02c443d70fe004a2d6fb9439f76, cve-2012-0158,
"mau van ban.doc" or "2013_ thong tin gia dinh.doc", delivered to VN targets

winMM-related Dropped Decoy Documents



ထိပ်တန်းလျှို့ဝှက်

ခရီးစဉ်အစီအစဉ်

၂-၉-၂၀၁၂ ရက် (တနင်္လာနေ့)

၀၉၀၀ နာရီ - နေပြည်တော်မှ အထူး လေယာဉ်ဖြင့်
(မြန်မာစံတော်ချိန်) တရုတ်ပြည်သူ့သမ္မတနိုင်ငံ၊ နန်နင်းမြို့သို့
ထွက်ခွာခြင်း
(ပျံသန်းချိန် ၂ နာရီ ၃၀ မိနစ်၊
အချိန်ကွာခြားချိန် + ၁ နာရီ ၃၀ မိနစ်)
(ဝတ်စုံ - Lounge Suite)
- လေယာဉ်ပေါ်တွင်နေ့လယ်စာ သုံးဆောင်ခြင်း

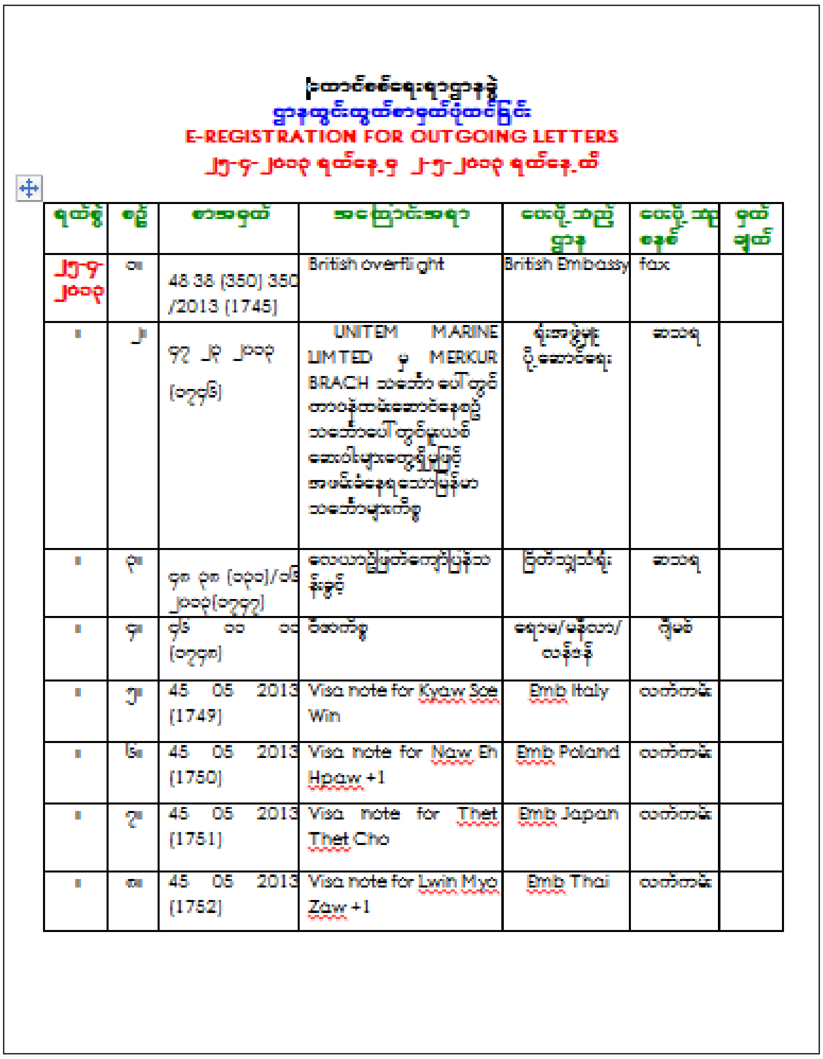
၁၃၀၀ နာရီ - နန်နင်းမြို့သို့ ရောက်ရှိခြင်း
(ဒေသစံတော်ချိန်) (ကွမ်းရှီးပြည်သူ့ ကွန်ဂရက် အမြဲတမ်း
ကော်မတီ ဒုတိယဥက္ကဋ္ဌ Mr. Qin
Ruixiang နှင့်မြန်မာသံအမတ်ကြီး၊
နန်နင်းမြို့ ကောင်စစ် ဝန်ချုပ်ရုံး ဝန်ထမ်း
မိသားစုများမှ ကြိုဆိုခြင်း

၁၃၁၀ နာရီ - လေဆိပ်မှ လိယွမ်ဧည့်ဂေဟာသို့ ထွက်
ခွာခြင်း

၁၃၄၀ နာရီ - လိယွမ်ဧည့်ဂေဟာသို့ ရောက်ရှိခြင်း
- ကိုယ်ပိုင်အချိန်

ထိပ်တန်းလျှို့ဝှက်

Image 1. “book form for naning 30-8.doc” (dropped by 448cd7c3ae0ae445d805a4849fe5e120)



ကြောင်စစ်ရေးရာဌာနခွဲ

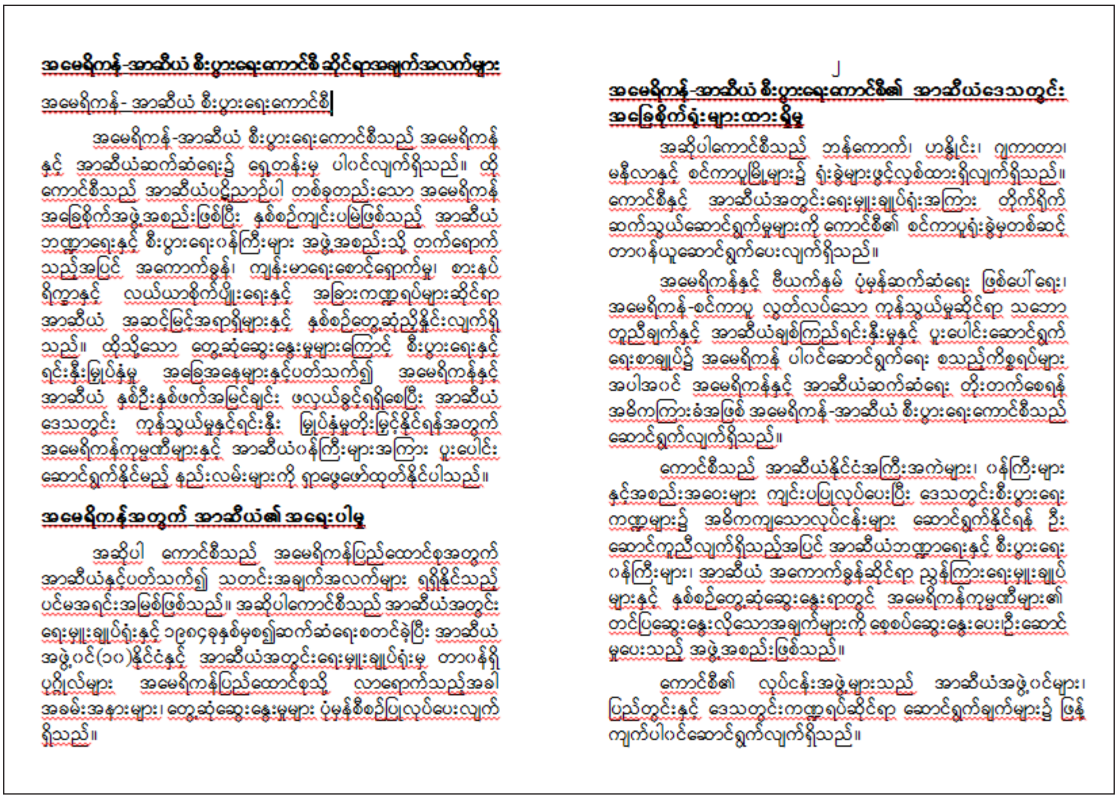
ဌာနထွင်းထွက်စာမှတ်ပုံတင်ခြင်း

E-REGISTRATION FOR OUTGOING LETTERS

၂၅-၄-၂၀၁၃ ရက်နေ့မှ ၂-၅-၂၀၁၃ ရက်နေ့ထိ

ရက်စွဲ	စဥ်	စာအမှတ်	အကြောင်းအရာ	ပေးပို့သည့်ဌာန	ပေးပို့သည့်နည်း	မှတ်ချက်
၂၅-၄-၂၀၁၃	၁။	48 38 (350) 350 /2013 (1745)	British overfli ght	British Embassy	fax	
။	၂။	၄၇ ၂၇ ၂၀၁၃ (၁၇၄၆)	UNITEM MARINE LIMTED မှ MERKUR BRACH သင်္ဘော ပေါ်တွင် တာဝန်ထမ်းဆောင်နေစဥ် သင်္ဘောပေါ်တွင်မူးယစ် ဆေးဝါးများတွေ့ရှိမှုဖြင့် အဖမ်းခံနေရသောမြန်မာ သင်္ဘောသားများကိစ္စ	ရုံးအဖွဲ့မှူး ပို့ဆောင်ရေး	ဆာသရ	
။	၃။	၄၈ ၄၈ (၁၃၀)/၀၆ ၂၀၁၃(၁၇၄၇)	လေယာဥ်ဖြတ်ကျော်ပျံသန်းခွင့်	ဗြိတိသျှသံရုံး	ဆာသရ	
။	၄။	၄၆ ၀၀ ၀၀ (၁၇၄၈)	ဗီဇာကိစ္စ	ရောမ/မနီလာ/ ထန်ဇန်	ဂျိမစ်	
။	၅။	45 05 2013 (1749)	Visa note for Kyaw Soe Win	Emb Italy	လက်ကမ်း	
။	၆။	45 05 2013 (1750)	Visa note for Naw Eh Hpaw +1	Emb Poland	လက်ကမ်း	
။	၇။	45 05 2013 (1751)	Visa note for Thet Thet Cho	Emb Japan	လက်ကမ်း	
။	၈။	45 05 2013 (1752)	Visa note for Lwin Myo Zaw +1	Emb Thai	လက်ကမ်း	

Image 2. Unknown. Dropped by 748c4761822dc7076399922df58551ae



အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီ ဆိုင်ရာအချက်အလက်များ

အမေရိကန်- အာဆီယံ စီးပွားရေးကောင်စီ

အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီသည် အမေရိကန်နှင့် အာဆီယံဆက်ဆံရေး၌ ရှေ့တန်းမှ ပါဝင်လျက်ရှိသည်။ ထိုကောင်စီသည် အာဆီယံပဋိညာဉ်ပါ တစ်ခုတည်းသော အမေရိကန် အခြေစိုက်အဖွဲ့အစည်းဖြစ်ပြီး နှစ်စဉ်ကျင်းပမြဲဖြစ်သည့် အာဆီယံ ဘဏ္ဍာရေးနှင့် စီးပွားရေးဝန်ကြီးများ အဖွဲ့အစည်းသို့ တက်ရောက်သည့်အပြင် အကောက်ခွန်၊ ကျန်းမာရေးစောင့်ရှောက်မှု၊ စားနပ်ရိက္ခာနှင့် လယ်ယာစိုက်ပျိုးရေးနှင့် အခြားကဏ္ဍရပ်များဆိုင်ရာ အာဆီယံ အဆင့်မြင့်အရာရှိများနှင့် နှစ်စဉ်တွေ့ဆုံညှိနှိုင်းလျက်ရှိသည်။ ထိုသို့သော တွေ့ဆုံဆွေးနွေးမှုများကြောင့် စီးပွားရေးနှင့် ရင်းနှီးမြှုပ်နှံမှု အခြေအနေများနှင့်ပတ်သက်၍ အမေရိကန်နှင့် အာဆီယံ နှစ်ဦးနှစ်ဖက်အမြင်ချင်း ဖလှယ်ခွင့်ရရှိစေပြီး အာဆီယံ ဒေသတွင်း ကုန်သွယ်မှုနှင့်ရင်းနှီး မြှုပ်နှံမှုတိုးမြှင့်နိုင်ရန်အတွက် အမေရိကန်ကုမ္ပဏီများနှင့် အာဆီယံဝန်ကြီးများအကြား ပူးပေါင်းဆောင်ရွက်နိုင်မည့် နည်းလမ်းများကို ရှာဖွေဖော်ထုတ်နိုင်ပါသည်။

အမေရိကန်အတွက် အာဆီယံ၏ အရေးပါမှု

အဆိုပါ ကောင်စီသည် အမေရိကန်ပြည်ထောင်စုအတွက် အာဆီယံနှင့်ပတ်သက်၍ သတင်းအချက်အလက်များ ရရှိနိုင်သည့် ပင်မအရင်းအမြစ်ဖြစ်သည်။ အဆိုပါကောင်စီသည် အာဆီယံအတွင်းရေးမှူးချုပ်ရုံးနှင့် ၁၉၈၄ခုနှစ်မှစ၍ဆက်ဆံရေးစတင်ခဲ့ပြီး အာဆီယံ အဖွဲ့ဝင်(၁၀)နိုင်ငံနှင့် အာဆီယံအတွင်းရေးမှူးချုပ်ရုံးမှ တာဝန်ရှိပုဂ္ဂိုလ်များ အမေရိကန်ပြည်ထောင်စုသို့ လာရောက်သည့်အခါ အခမ်းအနားများ၊ တွေ့ဆုံဆွေးနွေးမှုများ ပုံမှန်စီစဉ်ပြုလုပ်ပေးလျက်ရှိသည်။

၂

အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီ၏ အာဆီယံဒေသတွင်း အခြေစိုက်ရုံးများထားရှိမှု

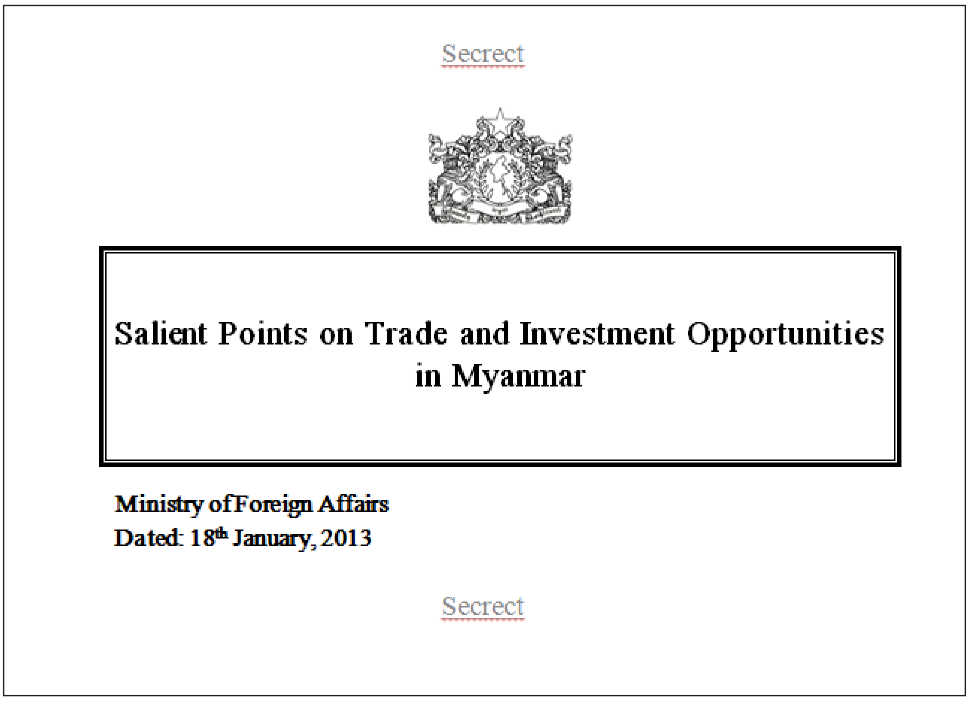
အဆိုပါကောင်စီသည် ဘန်ကောက်၊ ဟနွိုင်း၊ ဂျကာတာ၊ မနီလာနှင့် စင်ကာပူမြို့များ၌ ရုံးခွဲများဖွင့်လှစ်ထားရှိလျက်ရှိသည်။ ကောင်စီနှင့် အာဆီယံအတွင်းရေးမှူးချုပ်ရုံးအကြား တိုက်ရိုက်ဆက်သွယ်ဆောင်ရွက်မှုများကို ကောင်စီ၏ စင်ကာပူရုံးခွဲမှတစ်ဆင့် တာဝန်ယူဆောင်ရွက်ပေးလျက်ရှိသည်။

အမေရိကန်နှင့် ဗီယက်နမ် ပုံမှန်ဆက်ဆံရေး ဖြစ်ပေါ်ရေး၊ အမေရိကန်-စင်ကာပူ လွတ်လပ်သော ကုန်သွယ်မှုဆိုင်ရာ သဘောတူညီချက်နှင့် အာဆီယံချစ်ကြည်ရင်းနှီးမှုနှင့် ပူးပေါင်းဆောင်ရွက်ရေးစာချုပ်၌ အမေရိကန် ပါဝင်ဆောင်ရွက်ရေး စသည့်ကိစ္စရပ်များ အပါအဝင် အမေရိကန်နှင့် အာဆီယံဆက်ဆံရေး တိုးတက်စေရန် အဓိကကြားခံအဖြစ် အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီသည် ဆောင်ရွက်လျက်ရှိသည်။

ကောင်စီသည် အာဆီယံနိုင်ငံအကြီးအကဲများ၊ ဝန်ကြီးများနှင့်အစည်းအဝေးများ ကျင်းပပြုလုပ်ပေးပြီး ဒေသတွင်းစီးပွားရေးကဏ္ဍများ၌ အဓိကကျသောလုပ်ငန်းများ ဆောင်ရွက်နိုင်ရန် ဦးဆောင်ကူညီလျက်ရှိသည့်အပြင် အာဆီယံဘဏ္ဍာရေးနှင့် စီးပွားရေးဝန်ကြီးများ၊ အာဆီယံ အကောက်ခွန်ဆိုင်ရာ ညွှန်ကြားရေးမှူးချုပ်များနှင့် နှစ်စဉ်တွေ့ဆုံဆွေးနွေးရာတွင် အမေရိကန်ကုမ္ပဏီများ၏ တင်ပြဆွေးနွေးလိုသောအချက်များကို စေ့စပ်ဆွေးနွေးပေးပြီးဆောင်မှုပေးသည့် အဖွဲ့အစည်းဖြစ်သည်။

ကောင်စီ၏ လုပ်ငန်းအဖွဲ့များသည် အာဆီယံအဖွဲ့ဝင်များ၊ ပြည်တွင်းနှင့် ဒေသတွင်းကဏ္ဍရပ်ဆိုင်ရာ ဆောင်ရွက်ချက်များ၌ ဖြန့်ကျက်ပါဝင်ဆောင်ရွက်လျက်ရှိသည်။

Image 3. “fact sheet asean-us (president office format).doc”
Dropped by “fact sheet asean-us (president office format).doc .exe”
6803bd509d36d2b99049fcc9d975a21c



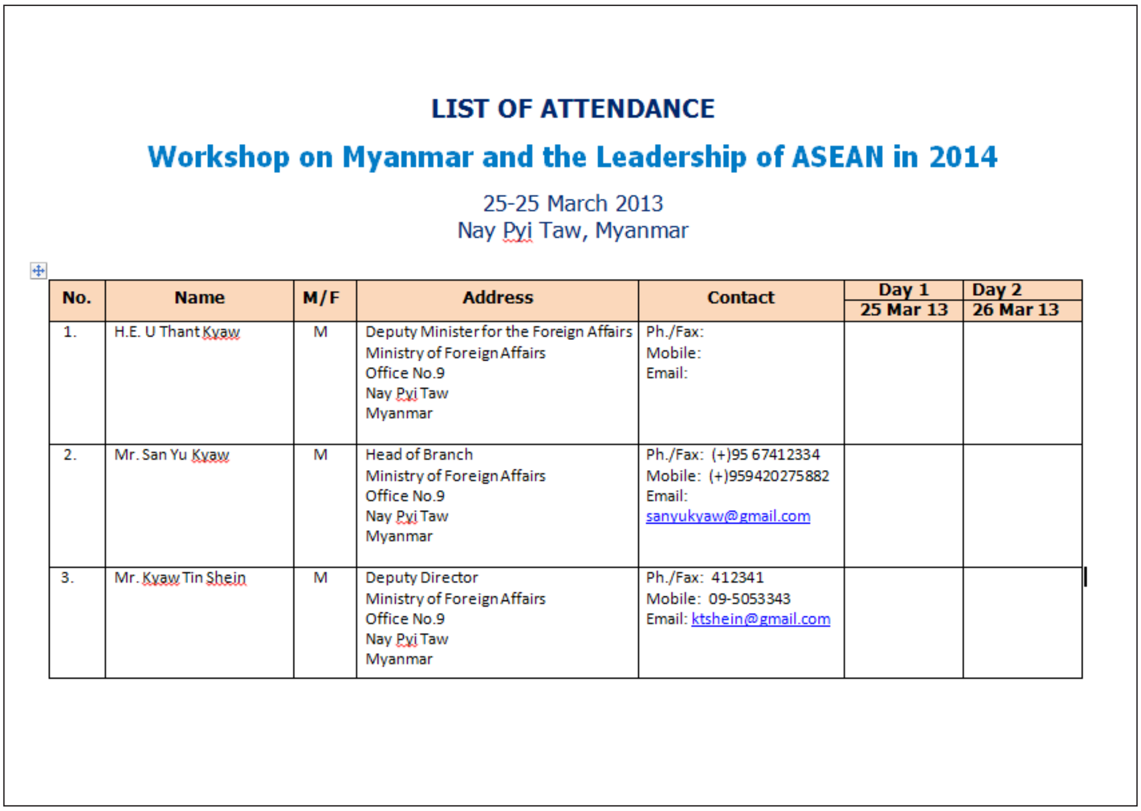
Secrect

Salient Points on Trade and Investment Opportunities in Myanmar

Ministry of Foreign Affairs
Dated: 18th January, 2013

Secrect

Image 4. Trade and Investment (english).doc
Dropped by b049fdeeb707e86e5e334f72cd50ffd8 “trade and investment (english).doc .exe”



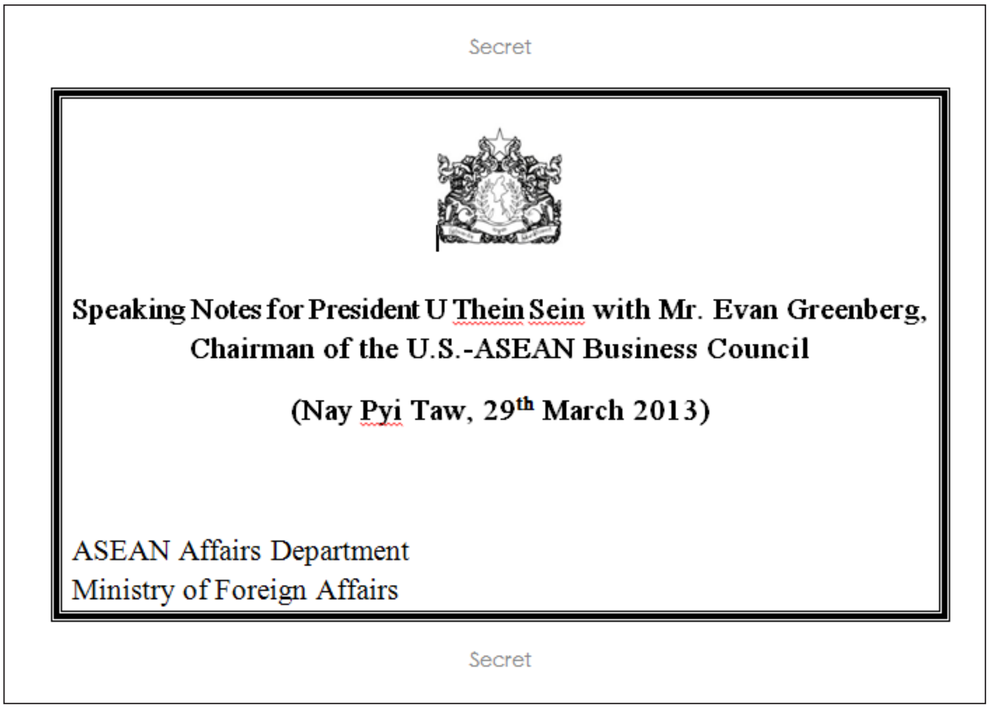
LIST OF ATTENDANCE

Workshop on Myanmar and the Leadership of ASEAN in 2014

25-25 March 2013
Nay Pyi Taw, Myanmar

No.	Name	M/F	Address	Contact	Day 1	Day 2
					25 Mar 13	26 Mar 13
1.	H.E. U Thant Kyaw	M	Deputy Minister for the Foreign Affairs Ministry of Foreign Affairs Office No.9 Nay Pyi Taw Myanmar	Ph./Fax: Mobile: Email:		
2.	Mr. San Yu Kyaw	M	Head of Branch Ministry of Foreign Affairs Office No.9 Nay Pyi Taw Myanmar	Ph./Fax: (+)95 67412334 Mobile: (+)959420275882 Email: sanyukyaw@gmail.com		
3.	Mr. Kyaw Tin Shein	M	Deputy Director Ministry of Foreign Affairs Office No.9 Nay Pyi Taw Myanmar	Ph./Fax: 412341 Mobile: 09-5053343 Email: ktshein@gmail.com		

Image 5. List of Attendance.doc
Dropped by F14C42765F130EE6DEC3A87DC50A47E1



Secret

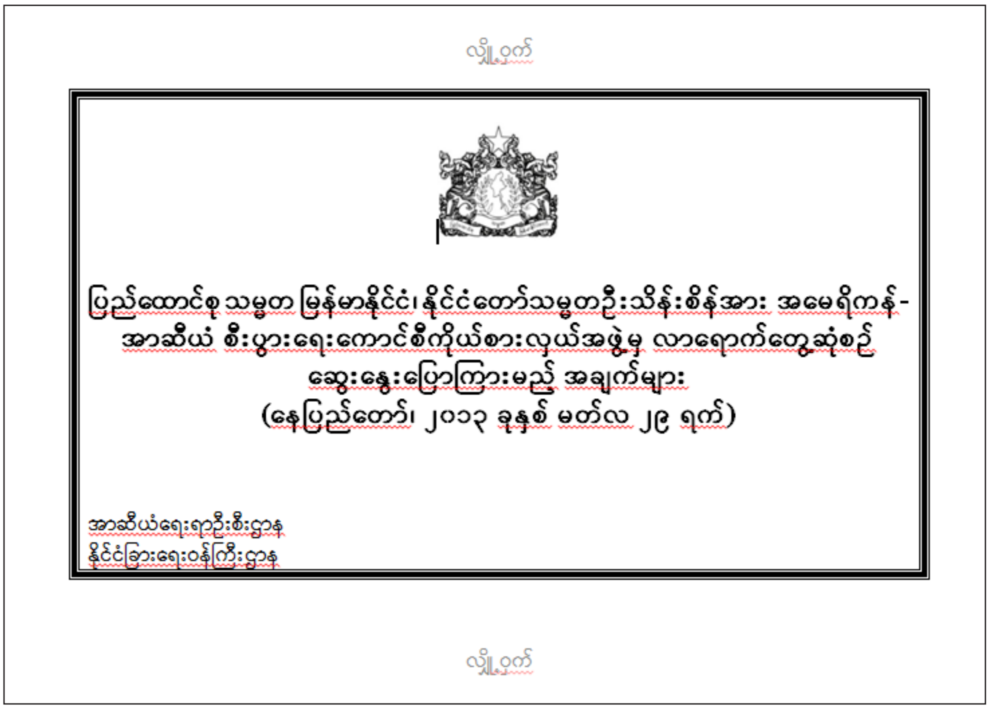
Speaking Notes for President U Thein Sein with Mr. Evan Greenberg, Chairman of the U.S.-ASEAN Business Council

(Nay Pyi Taw, 29th March 2013)

ASEAN Affairs Department
Ministry of Foreign Affairs

Secret

Image 6. "talking point english(english).doc"
Dropped by "talking point english(english).doc .exe", 800116c4fe842768a0e1acbc72c8cd62



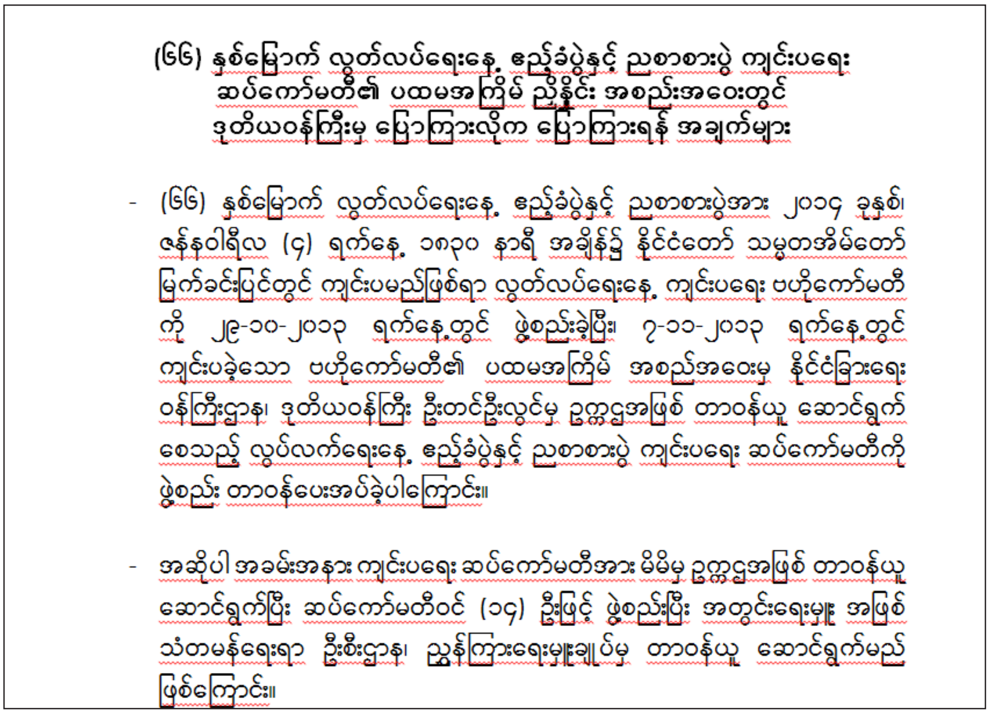
လျှို့ဝှက်

ပြည်ထောင်စု သမ္မတ မြန်မာနိုင်ငံ၊ နိုင်ငံတော်သမ္မတဦးသိန်းစိန်အား အမေရိကန်-
အာဆီယံ စီးပွားရေးကောင်စီကိုယ်စားလှယ်အဖွဲ့မှ လာရောက်တွေ့ဆုံစဉ်
ဆွေးနွေးပြောကြားမည့် အချက်များ
(နေပြည်တော်၊ ၂၀၁၃ ခုနှစ် မတ်လ ၂၉ ရက်)

အာဆီယံရေးရာဦးစီးဌာန
နိုင်ငံခြားရေးဝန်ကြီးဌာန

လျှို့ဝှက်

Image 7. talking point myanmar (21-3-2013).docx
Dropped by “talking point myanmar (21-3-2013).docx .exe” 416e6c9105139080310984ed06f6a57b

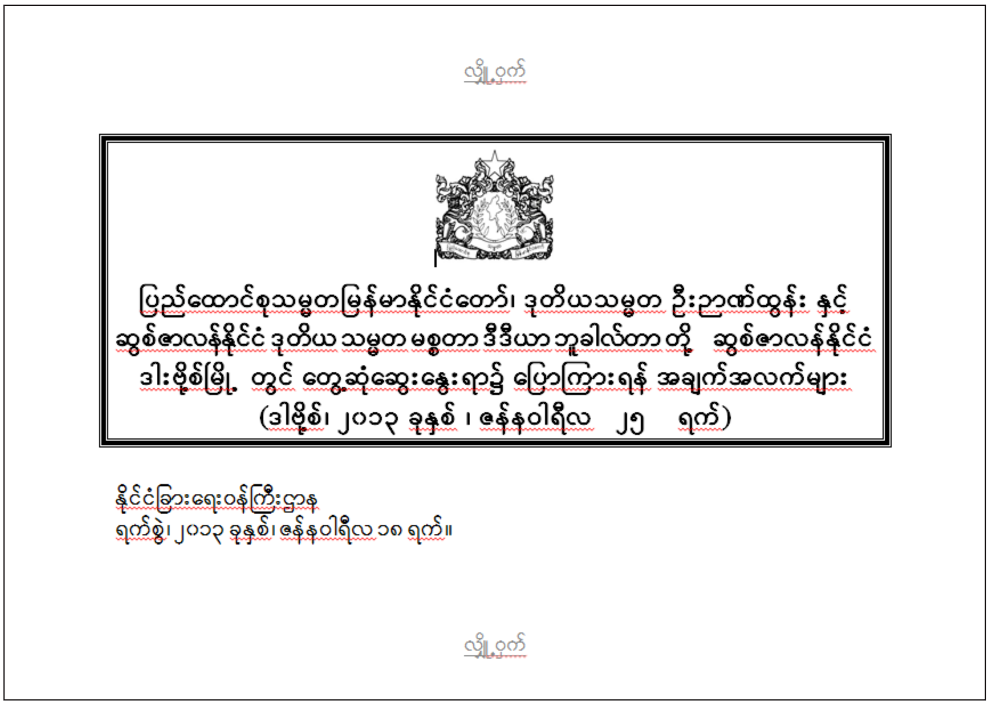


(၆၆) နှစ်မြောက် လွတ်လပ်ရေးနေ့ ဧည့်ခံပွဲနှင့် ညစာစားပွဲ ကျင်းပရေး
ဆပ်ကော်မတီ၏ ပထမအကြိမ် ညှိနှိုင်း အစည်းအဝေးတွင်
ဒုတိယဝန်ကြီးမှ ပြောကြားလိုက ပြောကြားရန် အချက်များ

- (၆၆) နှစ်မြောက် လွတ်လပ်ရေးနေ့ ဧည့်ခံပွဲနှင့် ညစာစားပွဲအား ၂၀၁၄ ခုနှစ်၊ ဇန်နဝါရီလ (၄) ရက်နေ့ ၁၈၃၀ နာရီ အချိန်၌ နိုင်ငံတော် သမ္မတအိမ်တော် မြက်ခင်းပြင်တွင် ကျင်းပမည်ဖြစ်ရာ လွတ်လပ်ရေးနေ့ ကျင်းပရေး ဗဟိုကော်မတီကို ၂၉-၁၀-၂၀၁၃ ရက်နေ့တွင် ဖွဲ့စည်းခဲ့ပြီး၊ ၇-၁၁-၂၀၁၃ ရက်နေ့တွင် ကျင်းပခဲ့သော ဗဟိုကော်မတီ၏ ပထမအကြိမ် အစည်းအဝေးမှ နိုင်ငံခြားရေး ဝန်ကြီးဌာန၊ ဒုတိယဝန်ကြီး ဦးတင်ဦးလွင်မှ ဥက္ကဋ္ဌအဖြစ် တာဝန်ယူ ဆောင်ရွက်စေသည့် လွပ်လက်ရေးနေ့ ဧည့်ခံပွဲနှင့် ညစာစားပွဲ ကျင်းပရေး ဆပ်ကော်မတီကို ဖွဲ့စည်း တာဝန်ပေးအပ်ခဲ့ပါကြောင်း။

- အဆိုပါ အခမ်းအနား ကျင်းပရေး ဆပ်ကော်မတီအား မိမိမှ ဥက္ကဋ္ဌအဖြစ် တာဝန်ယူ ဆောင်ရွက်ပြီး ဆပ်ကော်မတီဝင် (၁၄) ဦးဖြင့် ဖွဲ့စည်းပြီး အတွင်းရေးမှူး အဖြစ် သံတမန်ရေးရာ ဦးစီးဌာန၊ ညွှန်ကြားရေးမှူးချုပ်မှ တာဝန်ယူ ဆောင်ရွက်မည် ဖြစ်ကြောင်း။

Image 8. Unknown.
Dropped by 6758fc7e483ad9cd6280bcc3f4d85222



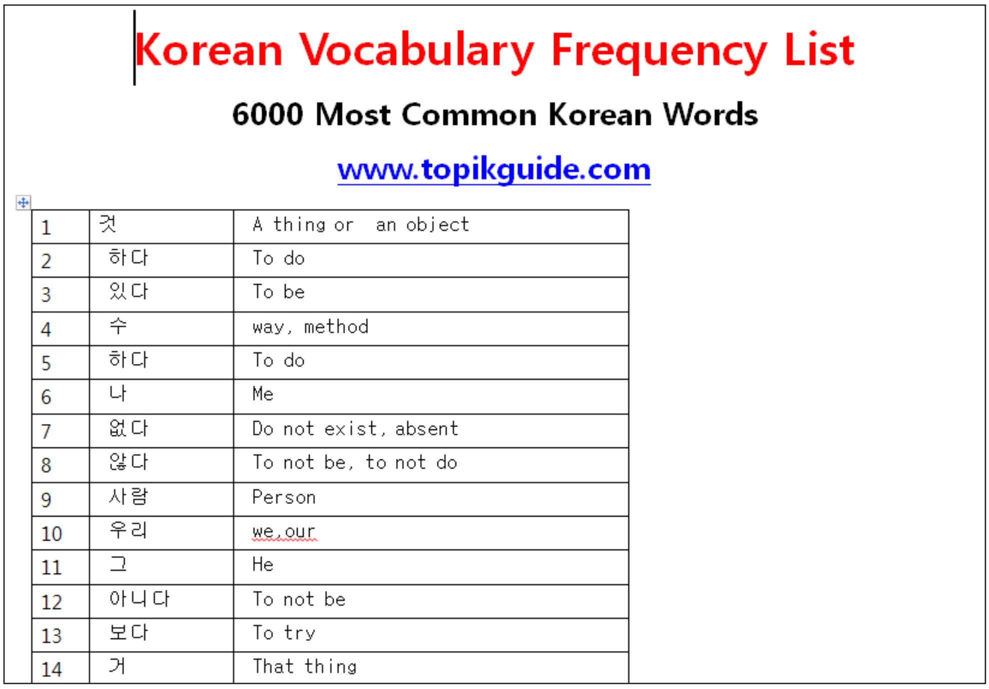
လျှို့ဝှက်

ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်၊ ဒုတိယသမ္မတ ဦးဉာဏ်ထွန်း နှင့်
ဆွစ်ဇာလန်နိုင်ငံ ဒုတိယ သမ္မတ မစ္စတာ ဒီဒီယာ ဘူခါလ်တာ တို့ ဆွစ်ဇာလန်နိုင်ငံ
ဒါးဗိုစ်မြို့ တွင် တွေ့ဆုံဆွေးနွေးရာ၌ ပြောကြားရန် အချက်အလက်များ
(ဒါဗိုစ်၊ ၂၀၁၃ ခုနှစ် ၊ ဇန်နဝါရီလ ၂၅ ရက်)

နိုင်ငံခြားရေးဝန်ကြီးဌာန
ရက်စွဲ၊ ၂၀၁၃ ခုနှစ်၊ ဇန်နဝါရီလ ၁၈ ရက်။

လျှို့ဝှက်

Image 9. tp for vp with swiss_myanmar[1].doc
Dropped by "tp for vp with swiss_myanmar[1].doc .exe" 90E9BDFC1FC6FE5999B047880C7445AE



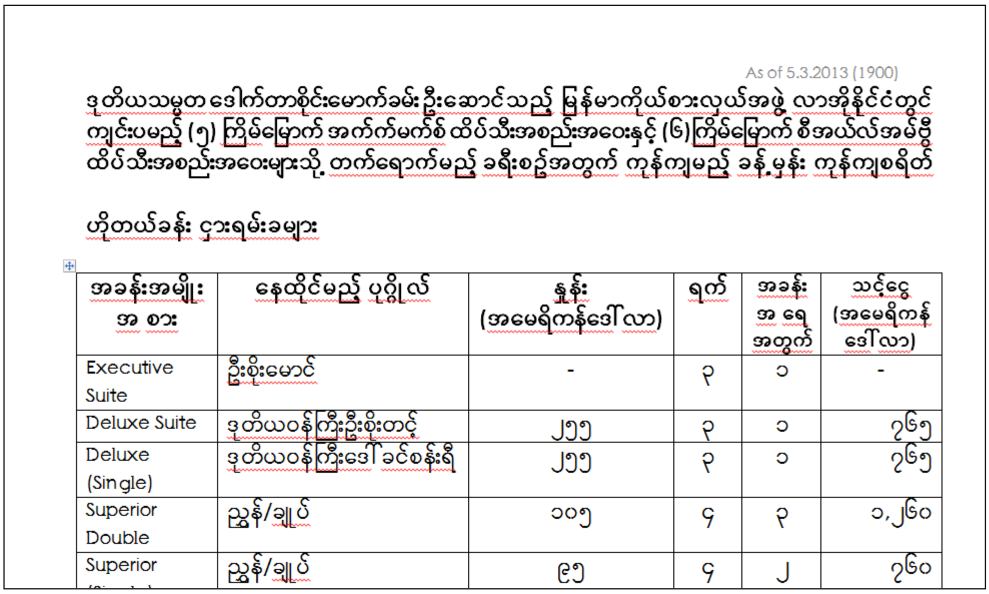
Korean Vocabulary Frequency List

6000 Most Common Korean Words

www.topikguide.com

1	것	A thing or an object
2	하다	To do
3	있다	To be
4	수	way, method
5	하다	To do
6	나	Me
7	없다	Do not exist, absent
8	않다	To not be, to not do
9	사람	Person
10	우리	we,our
11	그	He
12	아니다	To not be
13	보다	To try
14	거	That thing

Image 10. Unknown.
Dropped by 7F422B43EEB93B230FF7553C841C4785



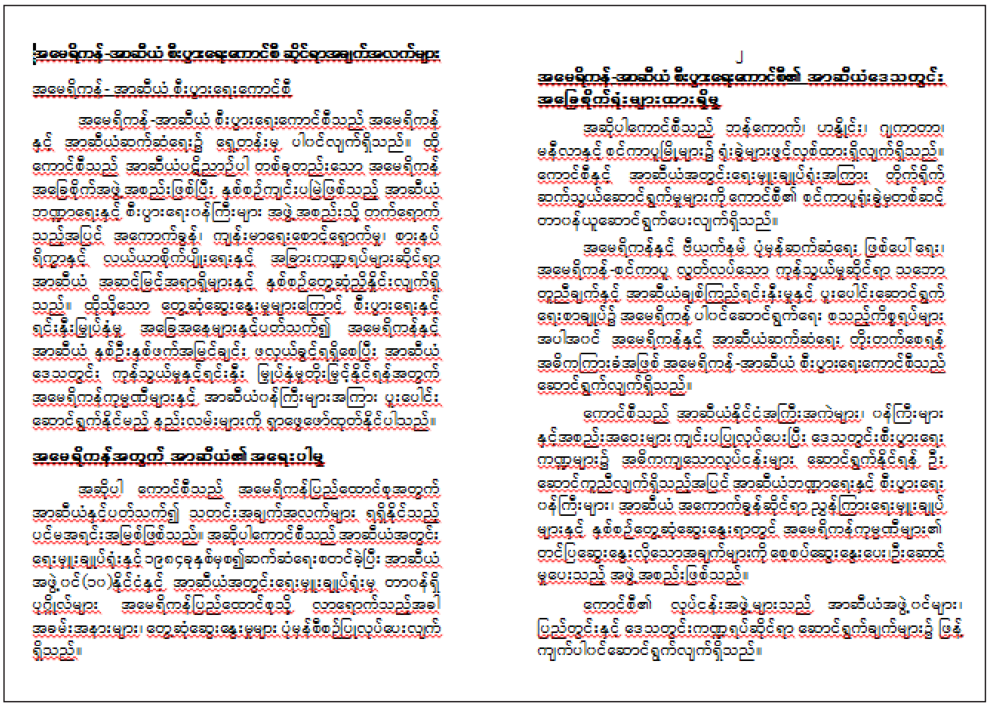
As of 5.3.2013 (1900)

ဒုတိယသမ္မတ ဒေါက်တာစိုင်းမောက်ခမ်း ဦးဆောင်သည့် မြန်မာကိုယ်စားလှယ်အဖွဲ့ လာအိုနိုင်ငံတွင် ကျင်းပမည့် (၅) ကြိမ်မြောက် အက်က်မက်စ် ထိပ်သီးအစည်းအဝေးနှင့် (၆)ကြိမ်မြောက် စီအယ်လ်အမ်ဗွီ ထိပ်သီးအစည်းအဝေးများသို့ တက်ရောက်မည့် ခရီးစဉ်အတွက် ကုန်ကျမည့် ခန့်မှန်း ကုန်ကျစရိတ်

ဟိုတယ်ခန်း ငှားရမ်းခများ

အခန်းအမျိုး အ စား	နေထိုင်မည့် ပုဂ္ဂိုလ်	နှုန်း (အမေရိကန်ဒေါ်လာ)	ရက်	အခန်း အ ရေ အတွက်	သင့်ငွေ (အမေရိကန် ဒေါ်လာ)
Executive Suite	ဦးစိုးမောင်	-	၃	၁	-
Deluxe Suite	ဒုတိယဝန်ကြီးဦးစိုးတင့်	၂၅၅	၃	၁	၇၆၅
Deluxe (Sin gle)	ဒုတိယဝန်ကြီးဒေါ်ခင်စန်းရီ	၂၅၅	၃	၁	၇၆၅
Superior Double	ညွန်/ချုပ်	၁၀၅	၄	၃	၁,၂၆၀
Superior	ညွန်/ချုပ်	၉၅	၄	၂	၇၆၀

Image 11. Unknown.
Dropped by 1d6258bc3688226e7cb56fb821215a8b



အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီ ဆိုင်ရာအချက်အလက်များ

အမေရိကန်- အာဆီယံ စီးပွားရေးကောင်စီ

အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီသည် အမေရိကန်နှင့် အာဆီယံဆက်ဆံရေး၌ ရှေ့တန်းမှ ပါဝင်လျက်ရှိသည်။ ထိုကောင်စီသည် အာဆီယံပဋိညာဉ်ပါ တစ်ခုတည်းသော အမေရိကန်အခြေစိုက်အဖွဲ့အစည်းဖြစ်ပြီး နှစ်စဉ်ကျင်းပမြဲဖြစ်သည့် အာဆီယံဘဏ္ဍာရေးနှင့် စီးပွားရေးဝန်ကြီးများ အဖွဲ့အစည်းသို့ တက်ရောက်သည့်အပြင် အကောက်ခွန်၊ ကျန်းမာရေးစောင့်ရှောက်မှု၊ စားနပ်ရိက္ခာနှင့် လယ်ယာစိုက်ပျိုးရေးနှင့် အခြားကဏ္ဍရပ်များဆိုင်ရာ အာဆီယံ အဆင့်မြင့်အရာရှိများနှင့် နှစ်စဉ်တွေ့ဆုံညှိနှိုင်းလျက်ရှိသည်။ ထိုသို့သော တွေ့ဆုံဆွေးနွေးမှုများကြောင့် စီးပွားရေးနှင့် ရင်းနှီးမြှုပ်နှံမှု အခြေအနေများနှင့်ပတ်သက်၍ အမေရိကန်နှင့် အာဆီယံ နှစ်ဦးနှစ်ဖက်အမြင်ချင်း ဖလှယ်ခွင့်ရရှိစေပြီး အာဆီယံဒေသတွင်း ကုန်သွယ်မှုနှင့်ရင်းနှီး မြှုပ်နှံမှုတိုးမြှင့်နိုင်ရန်အတွက် အမေရိကန်ကုမ္ပဏီများနှင့် အာဆီယံဝန်ကြီးများအကြား ပူးပေါင်းဆောင်ရွက်နိုင်မည့် နည်းလမ်းများကို ရှာဖွေဖော်ထုတ်နိုင်ပါသည်။

အမေရိကန်အတွက် အာဆီယံ၏ အရေးပါမှု

အဆိုပါ ကောင်စီသည် အမေရိကန်ပြည်ထောင်စုအတွက် အာဆီယံနှင့်ပတ်သက်၍ သတင်းအချက်အလက်များ ရရှိနိုင်သည့် ပင်မအရင်းအမြစ်ဖြစ်သည်။ အဆိုပါကောင်စီသည် အာဆီယံအတွင်း ရေးမှူးချုပ်ရုံးနှင့် ၁၉၈၄ခုနှစ်မှစ၍ဆက်ဆံရေးစတင်ခဲ့ပြီး အာဆီယံအဖွဲ့ဝင်(၁၀)နိုင်ငံနှင့် အာဆီယံအတွင်းရေးမှူးချုပ်ရုံးမှ တာဝန်ရှိပုဂ္ဂိုလ်များ အမေရိကန်ပြည်ထောင်စုသို့ လာရောက်သည့်အခါ အခမ်းအနားများ၊ တွေ့ဆုံဆွေးနွေးမှုများ ပုံမှန်စီစဉ်ပြုလုပ်ပေးလျက်ရှိသည်။

၂

အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီ၏ အာဆီယံဒေသတွင်း အခြေစိုက်ရုံးများထားရှိမှု

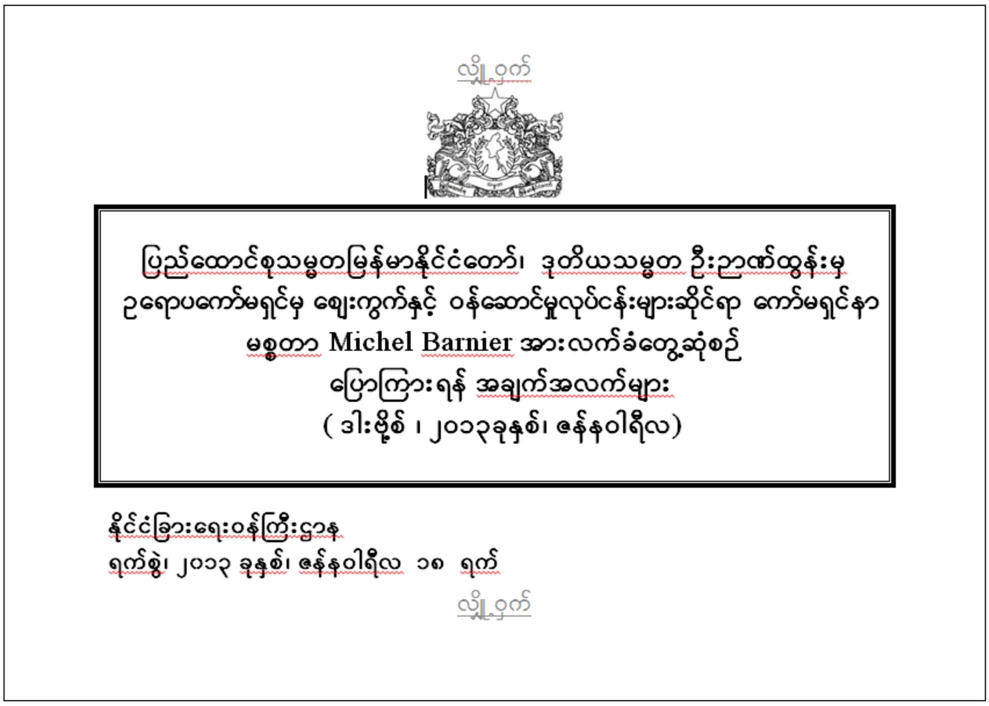
အဆိုပါကောင်စီသည် ဘန်ကောက်၊ ဟနွိုင်း၊ ဂျကာတာ၊ မနီလာနှင့် စင်ကာပူမြို့များ၌ ရုံးခွဲများဖွင့်လှစ်ထားရှိလျက်ရှိသည်။ ကောင်စီနှင့် အာဆီယံအတွင်းရေးမှူးချုပ်ရုံးအကြား တိုက်ရိုက်ဆက်သွယ်ဆောင်ရွက်မှုများကို ကောင်စီ၏ စင်ကာပူရုံးခွဲမှတစ်ဆင့် တာဝန်ယူဆောင်ရွက်ပေးလျက်ရှိသည်။

အမေရိကန်နှင့် ဗီယက်နမ် ပုံမှန်ဆက်ဆံရေး ဖြစ်ပေါ်ရေး၊ အမေရိကန်-စင်ကာပူ လွတ်လပ်သော ကုန်သွယ်မှုဆိုင်ရာ သဘောတူညီချက်နှင့် အာဆီယံချစ်ကြည်ရင်းနှီးမှုနှင့် ပူးပေါင်းဆောင်ရွက်ရေးစာချုပ်၌ အမေရိကန် ပါဝင်ဆောင်ရွက်ရေး စသည့်ကိစ္စရပ်များ အပါအဝင် အမေရိကန်နှင့် အာဆီယံဆက်ဆံရေး တိုးတက်စေရန် အဓိကကြားခံအဖြစ် အမေရိကန်-အာဆီယံ စီးပွားရေးကောင်စီသည် ဆောင်ရွက်လျက်ရှိသည်။

ကောင်စီသည် အာဆီယံနိုင်ငံအကြီးအကဲများ၊ ဝန်ကြီးများနှင့်အစည်းအဝေးများ ကျင်းပပြုလုပ်ပေးပြီး ဒေသတွင်းစီးပွားရေးကဏ္ဍများ၌ အဓိကကျသောလုပ်ငန်းများ ဆောင်ရွက်နိုင်ရန် ဦးဆောင်ကူညီလျက်ရှိသည့်အပြင် အာဆီယံဘဏ္ဍာရေးနှင့် စီးပွားရေးဝန်ကြီးများ၊ အာဆီယံ အကောက်ခွန်ဆိုင်ရာ ညွှန်ကြားရေးမှူးချုပ်များနှင့် နှစ်စဉ်တွေ့ဆုံဆွေးနွေးရာတွင် အမေရိကန်ကုမ္ပဏီများ၏ တင်ပြဆွေးနွေးလိုသောအချက်များကို စုစပ်ဆွေးနွေးပေးဦးဆောင်မှုပေးသည့် အဖွဲ့အစည်းဖြစ်သည်။

ကောင်စီ၏ လုပ်ငန်းအဖွဲ့များသည် အာဆီယံအဖွဲ့ဝင်များ၊ ပြည်တွင်းနှင့် ဒေသတွင်းကဏ္ဍရပ်ဆိုင်ရာ ဆောင်ရွက်ချက်များ၌ ဖြန့်ကျက်ပါဝင်ဆောင်ရွက်လျက်ရှိသည်။

Image 12. Unknown.
Dropped by 7a9712cbb3e340e577ce0320cceeb05f



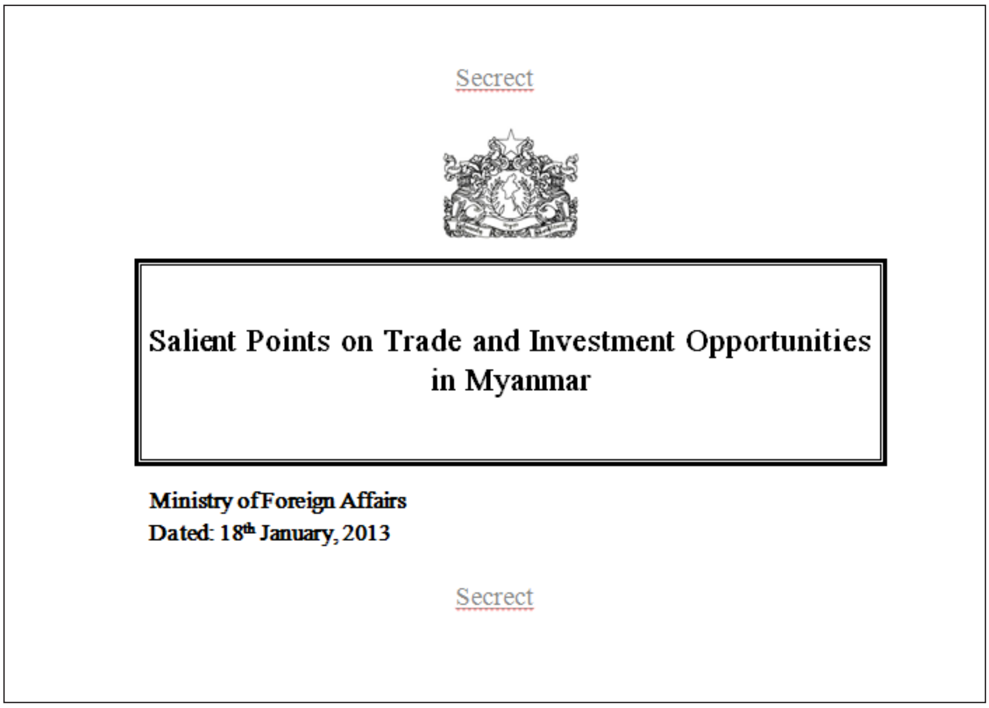
လျှို့ဝှက်

ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်၊ ဒုတိယသမ္မတ ဦးညဏ်ထွန်းမှ
ဥရောပကော်မရှင်မှ ဈေးကွက်နှင့် ဝန်ဆောင်မှုလုပ်ငန်းများဆိုင်ရာ ကော်မရှင်နာ
မစ္စတာ Michel Barnier အားလက်ခံတွေ့ဆုံစဉ်
ပြောကြားရန် အချက်အလက်များ
(ဒါးဗိုစ် ၊ ၂၀၁၃ခုနှစ်၊ ဇန်နဝါရီလ)

နိုင်ငံခြားရေးဝန်ကြီးဌာန
ရက်စွဲ၊ ၂၀၁၃ ခုနှစ်၊ ဇန်နဝါရီလ ၁၈ ရက်

လျှို့ဝှက်

Image 13. “tp for ec (myanmar).doc”
Dropped by “tp for ec (myanmar).doc .exe”, 9f23c0aed27f0874308bbd5f173ed85b



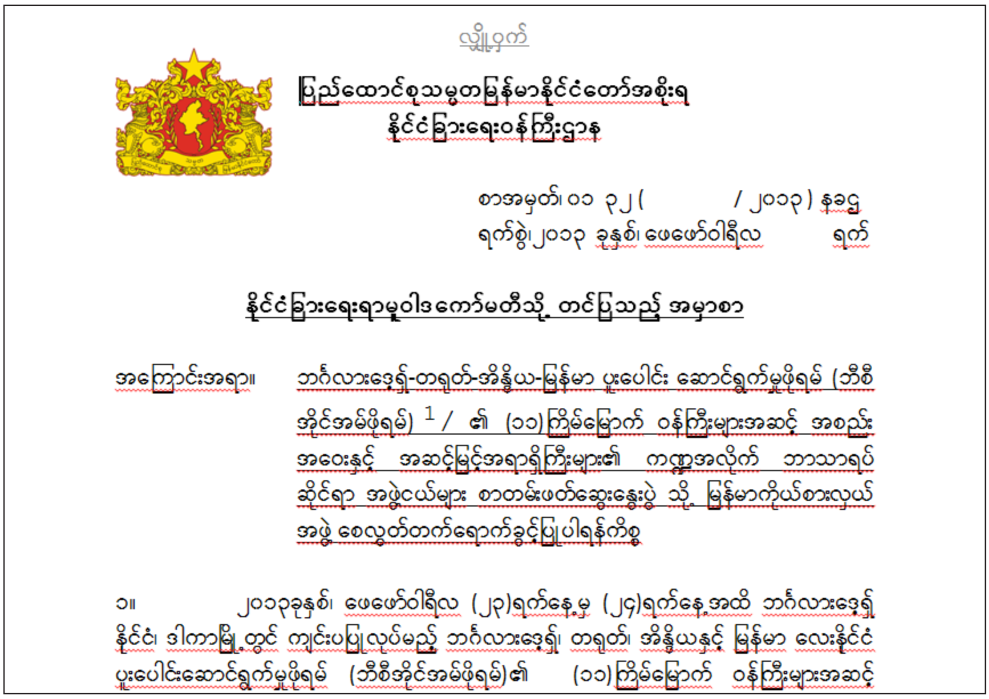
Secrect

Salient Points on Trade and Investment Opportunities in Myanmar

Ministry of Foreign Affairs
Dated: 18th January, 2013

Secrect

Image 14. “trade and investment (english).doc”
Dropped by “trade and investment (english).doc .exe”, dabba458b13cb676406c2bb219af9f81



လျှို့ဝှက်

ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်အစိုးရ
နိုင်ငံခြားရေးဝန်ကြီးဌာန

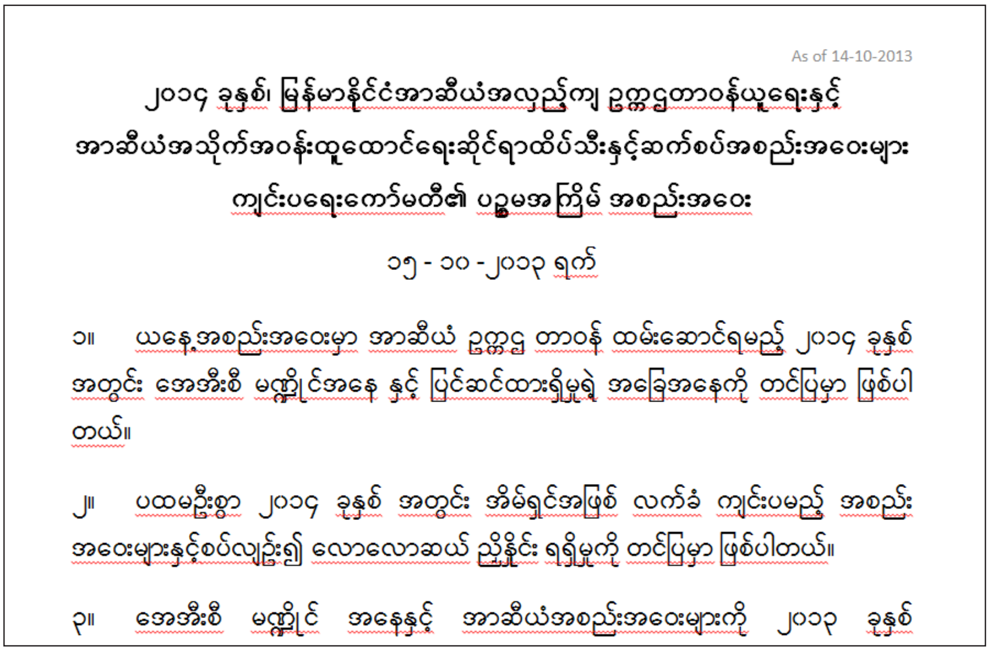
စာအမှတ်၊ ၀၁ ၃၂ (/ ၂၀၁၃) နခ၅
ရက်စွဲ၊ ၂၀၁၃ ခုနှစ်၊ ဖေဖော်ဝါရီလ   ရက်

နိုင်ငံခြားရေးရာမူဝါဒကော်မတီသို့ တင်ပြသည့် အမှာစာ

အကြောင်းအရာ။ ဘင်္ဂလားဒေ့ရှ်-တရုတ်-အိန္ဒိယ-မြန်မာ ပူးပေါင်း ဆောင်ရွက်မှုဖိုရမ် (ဘီစီအိုင်အမ်ဖိုရမ်) [1] / ၏ (၁၁)ကြိမ်မြောက် ဝန်ကြီးများအဆင့် အစည်းအဝေးနှင့် အဆင့်မြင့်အရာရှိကြီးများ၏ ကဏ္ဍအလိုက် ဘာသာရပ်ဆိုင်ရာ အဖွဲ့ငယ်များ စာတမ်းဖတ်ဆွေးနွေးပွဲ သို့ မြန်မာကိုယ်စားလှယ်အဖွဲ့ စေလွှတ်တက်ရောက်ခွင့်ပြုပါရန်ကိစ္စ

၁။ ၂၀၁၃ခုနှစ်၊ ဖေဖော်ဝါရီလ (၂၃)ရက်နေ့မှ (၂၄)ရက်နေ့အထိ ဘင်္ဂလားဒေ့ရှ် နိုင်ငံ၊ ဒါကာမြို့တွင် ကျင်းပပြုလုပ်မည့် ဘင်္ဂလားဒေ့ရှ်၊ တရုတ်၊ အိန္ဒိယနှင့် မြန်မာ လေးနိုင်ငံ ပူးပေါင်းဆောင်ရွက်မှုဖိုရမ် (ဘီစီအိုင်အမ်ဖိုရမ်)၏ (၁၁)ကြိမ်မြောက် ဝန်ကြီးများအဆင့်

Image 15. "11th bcim fapc memo.doc"
Dropped by "11th bcim fapc memo.doc .exe", d57a7369d79467d7c768bb08febcc6a2



As of 14-10-2013

၂၀၁၄ ခုနှစ်၊ မြန်မာနိုင်ငံအာဆီယံအလှည့်ကျ ဥက္ကဋ္ဌတာဝန်ယူရေးနှင့်
အာဆီယံအသိုက်အဝန်းထူထောင်ရေးဆိုင်ရာထိပ်သီးနှင့်ဆက်စပ်အစည်းအဝေးများ
ကျင်းပရေးကော်မတီ၏ ပဉ္စမအကြိမ် အစည်းအဝေး

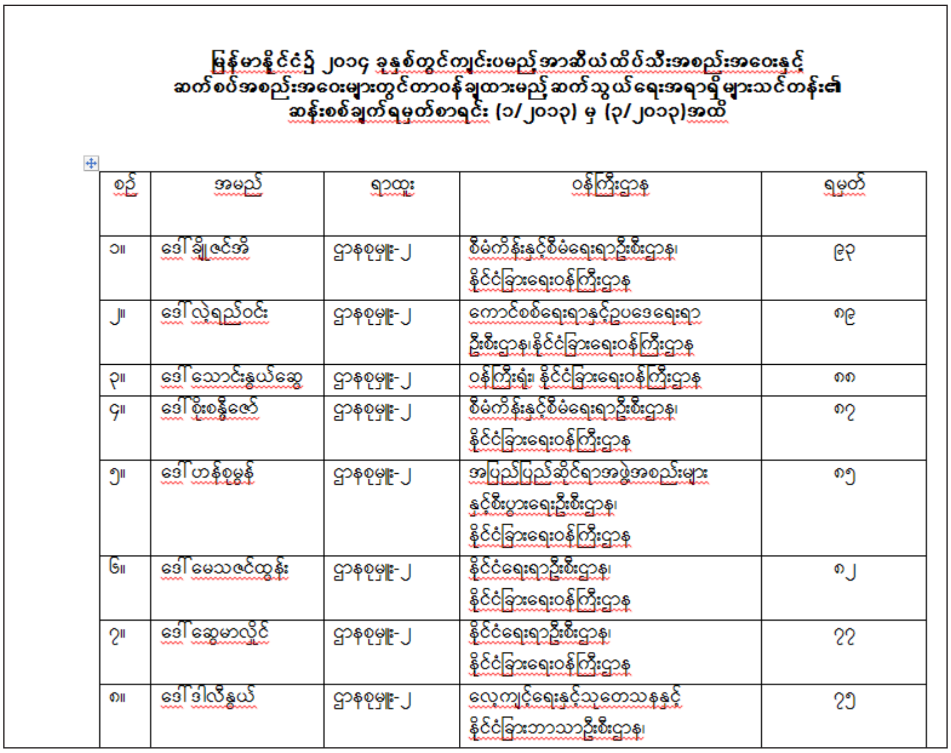
၁၅ - ၁၀ - ၂၀၁၃ ရက်

၁။ ယနေ့အစည်းအဝေးမှာ အာဆီယံ ဥက္ကဋ္ဌ တာဝန် ထမ်းဆောင်ရမည့် ၂၀၁၄ ခုနှစ် အတွင်း အေအီးစီ မဏ္ဍိုင်အနေ နှင့် ပြင်ဆင်ထားရှိမှုရဲ့ အခြေအနေကို တင်ပြမှာ ဖြစ်ပါတယ်။

၂။ ပထမဦးစွာ ၂၀၁၄ ခုနှစ် အတွင်း အိမ်ရှင်အဖြစ် လက်ခံ ကျင်းပမည့် အစည်းအဝေးများနှင့်စပ်လျဉ်း၍ လောလောဆယ် ညှိနိုင်း ရရှိမှုကို တင်ပြမှာ ဖြစ်ပါတယ်။

၃။ အေအီးစီ မဏ္ဍိုင် အနေနှင့် အာဆီယံအစည်းအဝေးများကို ၂၀၁၃ ခုနှစ်

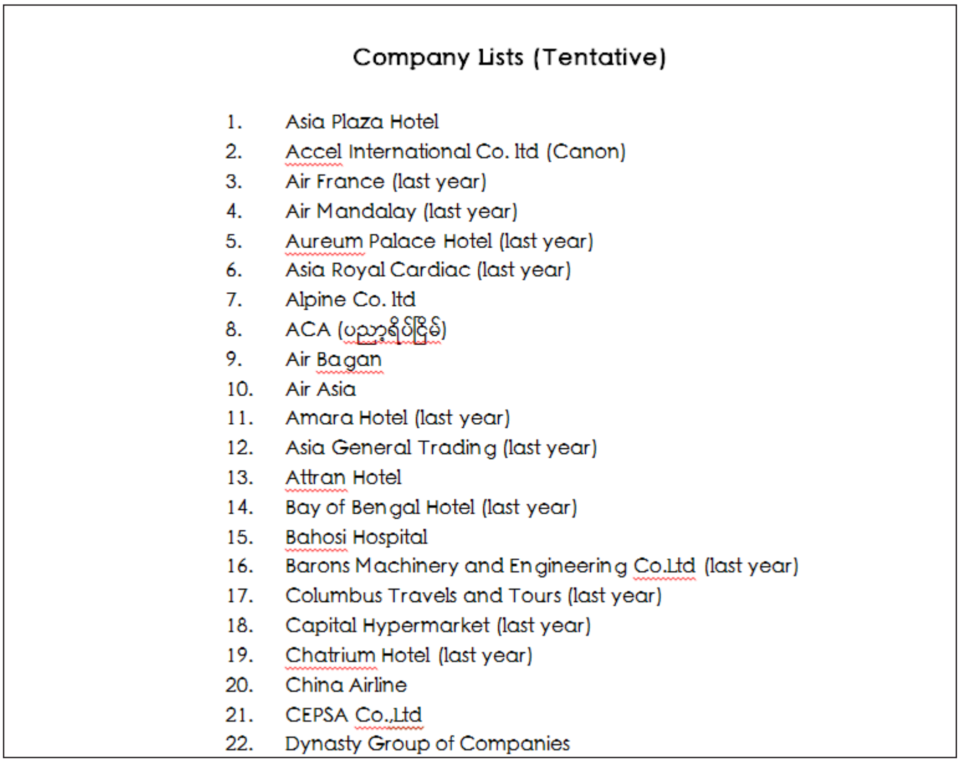
Image 16. "(r) final – h.e remarks.doc"
Dropped by "(r) final – h.e remarks.doc .exe", 7c0676d950a1443e98b7d5b4727923ea



မြန်မာနိုင်ငံ၌ ၂၀၁၄ ခုနှစ်တွင်ကျင်းပမည့်အာဆီယံထိပ်သီးအစည်းအဝေးနှင့်
ဆက်စပ်အစည်းအဝေးများတွင်တာဝန်ချထားမည့်ဆက်သွယ်ရေးအရာရှိများသင်တန်း၏
ဆန်းစစ်ချက်ရမှတ်စာရင်း (၁/၂၀၁၃) မှ (၃/၂၀၁၃)အထိ

စဉ်	အမည်	ရာထူး	ဝန်ကြီးဌာန	ရမှတ်
၁။	ဒေါ်ချိုဇင်အိ	ဌာနစုမှူး-၂	စီမံကိန်းနှင့်စီမံရေးရာဦးစီးဌာန၊ နိုင်ငံခြားရေးဝန်ကြီးဌာန	၉၃
၂။	ဒေါ်လဲ့ရည်ဝင်း	ဌာနစုမှူး-၂	ကောင်စစ်ရေးရာနှင့်ဥပဒေရေးရာ ဦးစီးဌာန၊နိုင်ငံခြားရေးဝန်ကြီးဌာန	၈၉
၃။	ဒေါ်သောင်းနွယ်ဆွေ	ဌာနစုမှူး-၂	ဝန်ကြီးရုံး၊ နိုင်ငံခြားရေးဝန်ကြီးဌာန	၈၈
၄။	ဒေါ်စိုးစန္ဒီဇော်	ဌာနစုမှူး-၂	စီမံကိန်းနှင့်စီမံရေးရာဦးစီးဌာန၊ နိုင်ငံခြားရေးဝန်ကြီးဌာန	၈၇
၅။	ဒေါ်ဟန်စုမွန်	ဌာနစုမှူး-၂	အပြည်ပြည်ဆိုင်ရာအဖွဲ့အစည်းများ နှင့်စီးပွားရေးဦးစီးဌာန၊ နိုင်ငံခြားရေးဝန်ကြီးဌာန	၈၅
၆။	ဒေါ်မေသဇင်ထွန်း	ဌာနစုမှူး-၂	နိုင်ငံရေးရာဦးစီးဌာန၊ နိုင်ငံခြားရေးဝန်ကြီးဌာန	၈၂
၇။	ဒေါ်ဆွေမာလှိုင်	ဌာနစုမှူး-၂	နိုင်ငံရေးရာဦးစီးဌာန၊ နိုင်ငံခြားရေးဝန်ကြီးဌာန	၇၇
၈။	ဒေါ်ဒါလီနွယ်	ဌာနစုမှူး-၂	လေ့ကျင့်ရေးနှင့်သုတေသနနှင့် နိုင်ငံခြားဘာသာဦးစီးဌာန၊	၇၅

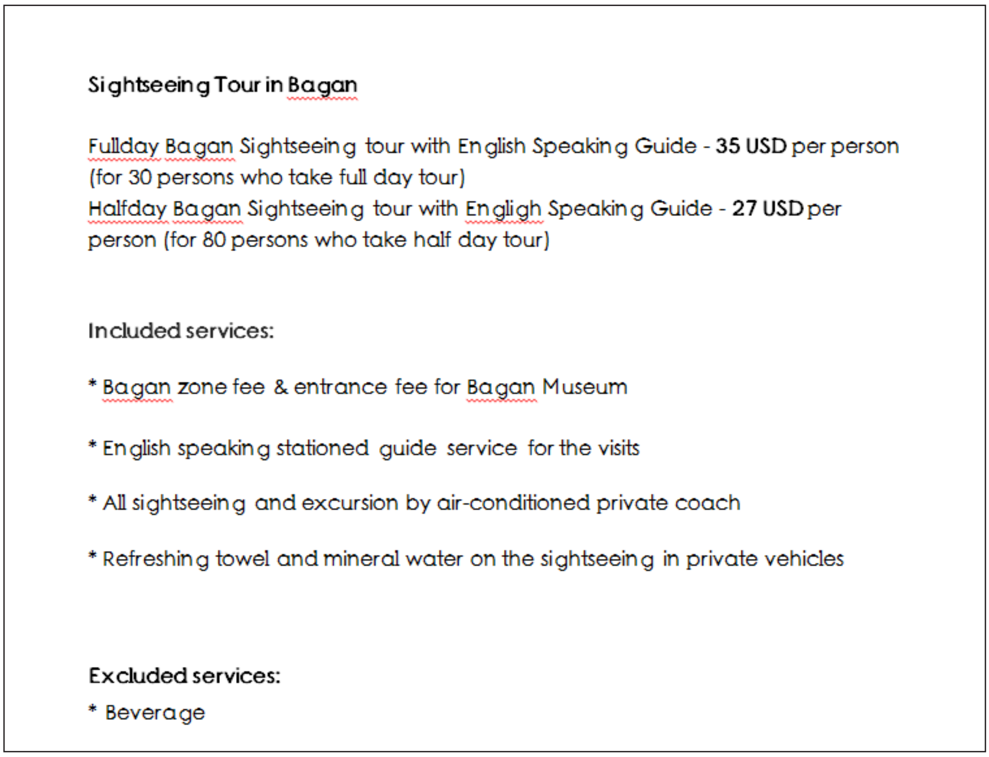
Image 17. lo list(26-8-2013).docx
Dropped by “lo list(26-8-2013).docx .exe”, 55048b78e9549c462c1463f7648454a5



Company Lists (Tentative)

1. Asia Plaza Hotel
2. Accel International Co. ltd (Canon)
3. Air France (last year)
4. Air Mandalay (last year)
5. Aureum Palace Hotel (last year)
6. Asia Royal Cardiac (last year)
7. Alpine Co. ltd
8. ACA (ပညာ့ရိပ်မြိုင်)
9. Air Bagan
10. Air Asia
11. Amara Hotel (last year)
12. Asia General Trading (last year)
13. Attran Hotel
14. Bay of Bengal Hotel (last year)
15. Bahosi Hospital
16. Barons Machinery and Engineering Co.Ltd (last year)
17. Columbus Travels and Tours (last year)
18. Capital Hypermarket (last year)
19. Chatrium Hotel (last year)
20. China Airline
21. CEPSA Co.,Ltd
22. Dynasty Group of Companies

Image 18. “company lists.doc”
Dropped by “company lists.doc .exe”, 113822c9bfeed38c099ae9004f1d8404



Sightseeing Tour in Bagan

Fullday Bagan Sightseeing tour with English Speaking Guide - **35 USD** per person (for 30 persons who take full day tour)
Halfday Bagan Sightseeing tour with Engligh Speaking Guide - **27 USD** per person (for 80 persons who take half day tour)

Included services:

* Bagan zone fee & entrance fee for Bagan Museum

* English speaking stationed guide service for the visits

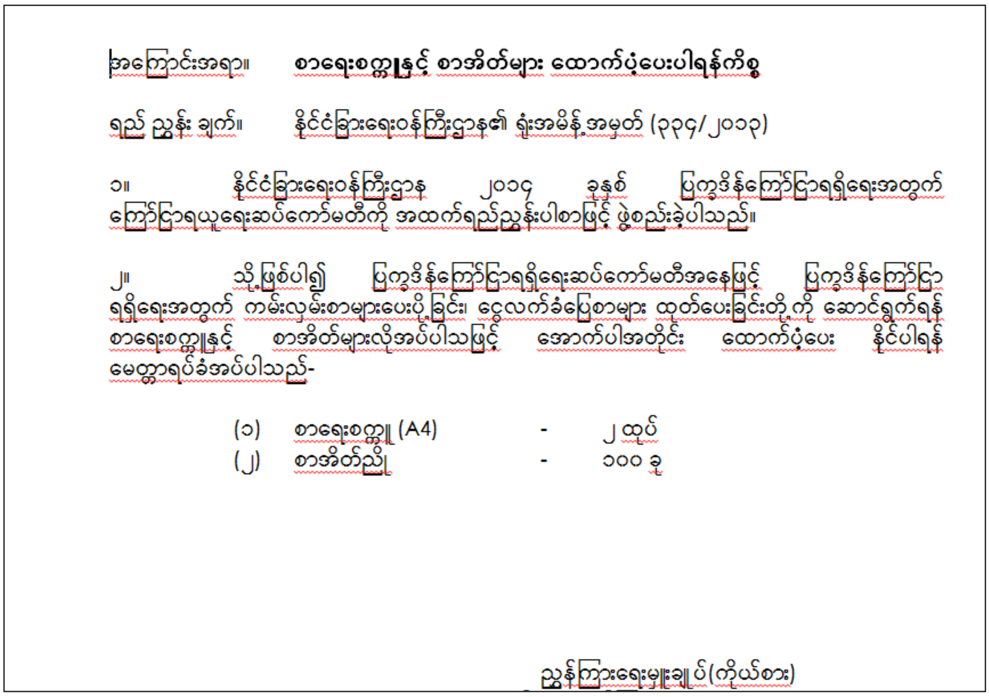
* All sightseeing and excursion by air-conditioned private coach

* Refreshing towel and mineral water on the sightseeing in private vehicles

Excluded services:

* Beverage

Image 19. “sightseeing tour in bagan.doc”
Dropped by “sightseeing tour in bagan.doc .exe”, 21119ddd01694bb9181286b52cf1203c



အကြောင်းအရာ။ **စာရေးစက္ကူနှင့် စာအိတ်များ ထောက်ပံ့ပေးပါရန်ကိစ္စ**

ရည် ညွှန်း ချက်။ နိုင်ငံခြားရေးဝန်ကြီးဌာန၏ ရုံးအမိန့်အမှတ် (၃၃၄/၂၀၁၃)

၁။ နိုင်ငံခြားရေးဝန်ကြီးဌာန ၂၀၁၄ ခုနှစ် ပြက္ခဒိန်ကြော်ငြာရရှိရေးအတွက် ကြော်ငြာရယူရေးဆပ်ကော်မတီကို အထက်ရည်ညွှန်းပါစာဖြင့် ဖွဲ့စည်းခဲ့ပါသည်။

၂။ သို့ဖြစ်ပါ၍ ပြက္ခဒိန်ကြော်ငြာရရှိရေးဆပ်ကော်မတီအနေဖြင့် ပြက္ခဒိန်ကြော်ငြာရရှိရေးအတွက် ကမ်းလှမ်းစာများပေးပို့ခြင်း၊ ငွေလက်ခံပြေစာများ ထုတ်ပေးခြင်းတို့ကို ဆောင်ရွက်ရန် စာရေးစက္ကူနှင့် စာအိတ်များလိုအပ်ပါသဖြင့် အောက်ပါအတိုင်း ထောက်ပံ့ပေး နိုင်ပါရန် မေတ္တာရပ်ခံအပ်ပါသည်-

(၁)	စာရေးစက္ကူ (A4)	-	၂ ထုပ်
(၂)	စာအိတ်ညို	-	၁၀၀ ခု

ညွှန်ကြားရေးမှူးချုပ်(ကိုယ်စား)

Image 20. Ns admin.docx
Dropped by “ns admin.docx .exe”, 6f9b6adbb33b7c8912aa2e5ae1c39f7a

APPENDIX B: KASPERSKY LAB VERDICT NAMES

Components related to the Naikon APT are detected under a range of verdict names. Below is a listing of the most common:

Backdoor.Win32.MsnMM.*
Backdoor.Win32.MsnMM.a - .af

Backdoor.Win32.Sakto.*
Backdoor.Win32.Sakto.a - .ct

Trojan-Downloader.Win32.Cordmix.*
Trojan-Downloader.Win32.Cordmix.b
Trojan-Downloader.Win32.Cordmix.ch
Trojan-Downloader.Win32.Cordmix.cs
Trojan-Downloader.Win32.Cordmix.ds

HackTool.Win32.Agent.*
HackTool.Win32.Agent.whj

Exploit.MSWord.CVE-2012-0158.*
Exploit.MSWord.CVE-2012-0158.cb
Exploit.MSWord.CVE-2012-0158.ci
Exploit.MSWord.CVE-2012-0158.di
Exploit.MSWord.CVE-2012-0158.dj
Exploit.MSWord.CVE-2012-0158.du
Exploit.MSWord.CVE-2012-0158.eb

Exploit.Win32.CVE-2012-0158.*
Exploit.Win32.CVE-2012-0158.a
Exploit.Win32.CVE-2012-0158.aw
Exploit.Win32.CVE-2012-0158.j

Trojan-Dropper.MSWord.Agent.*
Trojan-Dropper.MSWord.Agent.hc

Exploit.OLE2.CVE-2012-1856.a

HEUR:Exploit.MSWord.CVE-2012-0158.gen

Exploit.OLE2.Toolbar.a

Backdoor.Win32.Agent.*
Backdoor.Win32.Agent.bjer
Backdoor.Win32.Agent.dcyv
Backdoor.Win32.Agent.dfbk
Backdoor.Win32.Agent.dgpd

Backdoor.Win32.Zegost.*
Backdoor.Win32.Zegost.aekr

Trojan.Win32.Agent.*
Trojan.Win32.Agent.acflt
Trojan.Win32.Agent.acfma
Trojan.Win32.Agent.adddt
Trojan.Win32.Agent.hofz
Trojan.Win32.Agent.siai
Trojan.Win32.Agent.spde
Trojan.Win32.Agent.tlhi
Trojan.Win32.Agent.tpbo
Trojan.Win32.Agent.unhn
Trojan.Win32.Agent.xikp

Trojan.Win32.Agentb.*
Trojan.Win32.Agentb.bbca
Trojan.Win32.Agentb.bphx
Trojan.Win32.Agentb.iqj
Trojan.Win32.Agentb.jwp

Trojan-Downloader.Win32.Agent.*
Trojan-Downloader.Win32.Agent.gxqe
Trojan-Downloader.Win32.Agent.zzrd

Trojan-Spy.Win32.Agent.*
Trojan-Spy.Win32.Agent.chrj
Trojan-Spy.Win32.Agent.chuq
Trojan-Spy.Win32.Agent.cibn
Trojan-Spy.Win32.Agent.cicz
Trojan-Spy.Win32.Agent.ciet
Trojan-Spy.Win32.Agent.cifj
Trojan-Spy.Win32.Agent.ciry
Trojan-Spy.Win32.Agent.ciiu
Trojan-Spy.Win32.Agent.cita

Trojan-Spy.Win32.Agent.cjez
Trojan-Spy.Win32.Agent.cjkg
Trojan-Spy.Win32.Agent.cjmv

Trojan.Win32.Pincav.*
Trojan.Win32.Pincav.cngx

Trojan.Win32.Sasfis.*
Trojan.Win32.Sasfis.dmmt

Trojan-Dropper.MSIL.Agent.*
Trojan-Dropper.MSIL.Agent.aidh

Trojan-Dropper.Win32.Dycler.*
Trojan-Dropper.Win32.Dycler.ssr
Trojan-Dropper.Win32.Dycler.sss

Trojan-Dropper.Win32.Injector.*
Trojan-Dropper.Win32.Injector.jujl
Trojan-Dropper.Win32.Injector.kblf
Trojan-Dropper.Win32.Injector.kbre

Trojan.Win32.Zapchast.*
Trojan.Win32.Zapchast.aerr
Trojan.Win32.Zapchast.aest
Trojan.Win32.Zapchast.aetr
Trojan.Win32.Zapchast.aety
Trojan.Win32.Zapchast.aevb
Trojan.Win32.Zapchast.aevg
Trojan.Win32.Zapchast.afma
Trojan.Win32.Zapchast.afcz

HEUR:Trojan.Win32.Generic
HEUR:Trojan.Win32.Invader

APPENDIX C: MD5 REFERENCE SET

SslMM

469ca0c73398903908babcad14300d8d
95c4a236faa65b75dbb0076d8248584c

WinMM

c8c81cca4645e71213f2310cec6c277d
45a99f60654f22b671aec980687d0f15

WininetMM/Sakto

9883abc829870478ce6f3cfddbcbbaf2
a5721c5e7f2b49df82595819b5a49c0c

Injectv1/InjectResource

5c04904a50f0285851fb7292c13858ec

Exe_Exchange

6a82c153bd370250cc2fed89f1bb5c91
48fb78e8ba531505e246760c0d02d6b0

Sys10

c58df5892700ac3f467524f86bf325c0
33d388c6e841ede3920f79516b5da032

xsPlus (nokian) and plugin

d86106faaa398b8d83437176bf5e39c4
041436594c1ce9e99c569fb7402fe0c7
d0fba5db608ac8f5a3d05a71ceb0eca1

APPENDIX D: C2 (DOMAIN) REFERENCE SET

ahzx.eicp.net
bkav.imshop.in
googlemm.vicp.net
mncgn.51vip.biz
myanmartech.vicp.net
thailand.vicp.net
ubaoyouxiang.gicp.net
vietnam.gnway.net

Securelist, the resource for Kaspersky Lab experts' technical research,
analysis, and thoughts.

Kaspersky Lab global Website

Kaspersky Lab B2C Blog

Kaspersky Lab security news service

Follow us

Eugene Kaspersky Blog

Kaspersky Lab B2B Blog

Kaspersky Lab Academy

For full indicator and other details, please contact intelreports@kaspersky.com

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

more contact details

Tel: +7-495-797-8700
Fax: +7-495-797-8709