THE MsnMM CAMPAIGNS

The Earliest Naikon APT Campaigns

Kurt Baumgartner, Maxim Golovkin
May, 2015
CONTENTS

INTRODUCTION .................................................................................................................................. 3

SHARED EXPLOIT GENERATION KIT .............................................................................................. 5

SHARED STRINGS, FUNCTIONALITY, TARGETS, AND INFRASTRUCTURE ACROSS CAMPAIGNS .......... 6
  Similar strings ................................................................................................................................... 6
  Shared infrastructure ..................................................................................................................... 7
  Correlating Target Profiles with spear-phish and Decoy Content .............................................. 7

NAIKON APT MSNMM CAMPAIGN BACKDOORS AND LATERAL MOVEMENT TOOLSET .................. 11
  SslMM ........................................................................................................................................... 11
  WinMM .......................................................................................................................................... 13
  exe_exchange (used in attacks prior to ~2012) ............................................................................. 14
  INJECTv1/INJECTRESOURCE ......................................................................................................... 14
  The xsPlus/nokian backdoor and keylogger ............................................................................... 14

NAIKON AND MINOR LINKS WITH APT30 ...................................................................................... 15
  Sys10 ........................................................................................................................................... 16
  WininetMM/Sakto .......................................................................................................................... 17

SECOND STAGE TOOLS .................................................................................................................... 18

CUSTOM HDOOR .............................................................................................................................. 19

TARGET AND VICTIM PROFILES ................................................................................................... 21

SPEAR-PHISH, DROPPED FILES, WEB BROWSER INJECTION ......................................................... 22

APPENDIX A: MsnMM SPEAR-PHISH AND DECOY CONTENT .......................................................... 28
  winMM-related Dropped Decoy Documents ............................................................................... 32

APPENDIX B: KASPERSKY LAB VERDICT NAMES ............................................................................. 43

APPENDIX C: MD5 REFERENCE SET ............................................................................................... 46
  SslMM ........................................................................................................................................... 46
  WinMM .......................................................................................................................................... 46
  WininetMM/Sakto .......................................................................................................................... 46
  Injectv1/InjectResource ................................................................................................................. 46
  Exe_Exchange .............................................................................................................................. 46
  Sys10 ........................................................................................................................................... 46
  xsPlus (nokian) and plugin .......................................................................................................... 47

APPENDIX D: C2 (DOMAIN) REFERENCE SET .................................................................................. 48

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

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

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

<table>
<thead>
<tr>
<th>backdoor</th>
<th>exe_exchange</th>
<th>sys10</th>
<th>winMM</th>
<th>sslMM</th>
<th>wininetMM/ sakto</th>
<th>xsPlus/naikon</th>
</tr>
</thead>
<tbody>
<tr>
<td>ahzx.eicp.net</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mncgn.51vip.biz</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bkav.imshop.in</td>
<td></td>
<td></td>
<td>yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>ubaoyouxiang.gicp.net</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td>yes</td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>googlemm.vicp.net</td>
<td></td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>myanmartech.vicp.net</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

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:

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Letpadaung copper mine.doc</td>
<td>Myanmar Wanbao to commence construction of Letpadaung project</td>
<td>December 2014</td>
</tr>
<tr>
<td>nuclear agreement burma.doc</td>
<td>Burma Signs New Nuclear Deal With IAEA</td>
<td>September 2013</td>
</tr>
<tr>
<td>Calendar Misslao 2013 Free.doc</td>
<td>Miss Lao Calendars</td>
<td>January 2014</td>
</tr>
<tr>
<td>ASEAN and Partners Firmly Committed to Narrowing the Development Gap.doc</td>
<td>ASEAN and Partners Firmly Committed to Narrowing the Development Gap</td>
<td>April 2013</td>
</tr>
<tr>
<td>refer to the 11th ACD Ministerial Meeting.doc</td>
<td>Asia Co-operation Dialogue eyes peace</td>
<td>December 2013</td>
</tr>
<tr>
<td>Asia’s Military Developments.doc</td>
<td>Asia’s military developments</td>
<td>November 2013</td>
</tr>
</tbody>
</table>
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:

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:
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
NAIKON APT MSNMM CAMPAIGN
BACKDOORS AND LATERAL
MOVEMENT TOOLSET

SslMM

<table>
<thead>
<tr>
<th>MD5 – Filename</th>
<th>File Size</th>
<th>Compilation date</th>
<th>Linker version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7b1199523a662a3844ba590f83b56dae - %temp%\conime.exe</td>
<td>77,824 bytes</td>
<td>2013:01:31 01:25:38+00:00</td>
<td>6.0</td>
</tr>
</tbody>
</table>

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.

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

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 NetUser-GetInfo 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.

For full indicator and other details, please contact intelreports@kaspersky.com
exe_exchange (used in attacks prior to ~2012)

<table>
<thead>
<tr>
<th>MDS – Filename</th>
<th>File Size</th>
<th>Compilation date</th>
<th>Linker version</th>
</tr>
</thead>
<tbody>
<tr>
<td>6a82c153bd370250cc2fed89f1bb5c91 - %temp%\services.exe</td>
<td>69,632 bytes</td>
<td>2012-03-13 07:54:19</td>
<td>6.0</td>
</tr>
</tbody>
</table>

INJECTv1/INJECTRESOURCE

<table>
<thead>
<tr>
<th>MDS – Filename</th>
<th>File Size</th>
<th>Compilation date</th>
</tr>
</thead>
<tbody>
<tr>
<td>b295274423c91ad9e254475bf8edd459 - wmiaprve.exe</td>
<td>159,744 bytes</td>
<td>May 27, 2013</td>
</tr>
</tbody>
</table>

The xsPlus/nokian backdoor and keylogger

<table>
<thead>
<tr>
<th>MDS – Filename</th>
<th>File Size</th>
<th>Compilation date</th>
<th>Linker version</th>
</tr>
</thead>
<tbody>
<tr>
<td>d86106f9aa398b8d83437176bf5e39c4</td>
<td>281,624 bytes</td>
<td>2011.12.19 08:06:30</td>
<td>6.0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Date</th>
<th>IP1</th>
<th>IP2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-10-07</td>
<td>208.77.46.251</td>
<td>174.36.159.165</td>
</tr>
<tr>
<td>2013-04-03</td>
<td>174.36.159.165</td>
<td>219.90.115.251</td>
</tr>
<tr>
<td>2013-04-14</td>
<td>219.90.115.251</td>
<td>174.36.159.164</td>
</tr>
</tbody>
</table>

While the MsnMM components include the unusual “MM” in internal names sslMM, winMM, and wininetMM, some of the strings in the APT30 GEMSTONE software include the same – search and retrieval of the registry key “Software\Microsoft\GetMM”, and three function names “MicrosoftGMMExit, MicrosoftGMMHaveExit, 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) /autoMM/ 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.Ink” shortcuts to the Start Menu Startup location for persistence, just like the MsnMM components spoof “Msn Gaming Zone.Ink” and “Msn Talk.Ink” for persistence.
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

<table>
<thead>
<tr>
<th>MD5 – Filename</th>
<th>File Size</th>
<th>Compilation date</th>
<th>Linker version</th>
</tr>
</thead>
<tbody>
<tr>
<td>516f64dd4fce3b9a325ea8501f97a88a</td>
<td>95,744 bytes</td>
<td>2014.11.03 07:59:14</td>
<td>9.0</td>
</tr>
</tbody>
</table>

For full indicator and other details, please contact intelreports@kaspersky.com
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, procexe.exe, psexec
- Prosolve: winscan.exe
- Rarlabs: rar.exe
- Other: procexe.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

<table>
<thead>
<tr>
<th>MD5 – Filename</th>
<th>File Size</th>
<th>Compilation date</th>
<th>Detection Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>bf6d3f52ab8176122be858ddccc22148 - lms.dat</td>
<td>56 kb</td>
<td>2015.05.20</td>
<td>HackTool.Win32.Agent.whj</td>
</tr>
</tbody>
</table>

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:

```
G:\>hd -hbs 192.168.0.5 /b /n
192.168.0.5  >:  <3435/100>

Done. Sleep 5 seconds and wait to end.
192.168.0.5  1:  Port 135 Open!!1
192.168.0.5  1:  Port 139 Open!!!
192.168.0.5  1:  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.
G:\>
```
The corresponding hbs.txt output file content that is sometimes left behind on victim systems:

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-Subuntu1.1
[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 transferred 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

---

For full indicator and other details, please contact intelreports@kaspersky.com
Example details, exhibiting the “common” sequence of events on systems:

```
c334737ea5e8f74567bfdc2f6717b9,2 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
  6cbc73fae711e8d0fae328ce8ee6050,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

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

The Earliest Naikon APT Campaigns TLP White

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

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”

55b8b8779001b7e8a6adc55fb546401,C:\DOCUME~1\user\LOCALS~1\Temp\update.exe

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

C2: ubaoyouxiang.gicp.net

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

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 capabilities.

Example decoy Word document targeting PH gov

27ed7c7dd840ff7936418cf029d56603, AFP Summary.doc → %temp%\iph.bat
ceb6e4499cfd8650f3e94fbcf7de48f6,%temp%\iExplorer.exe WMcal
b6424852dd0187ea554a1bc4e3490f3,%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” (4972dc7205e3279322637f609b9199ee97). The dropper maintains a clean copy of this decoy pdf that opens on execution, [as well as?] the Naikon backdoor (ab0185f3dc70af754559297f6f47492) and accompanying mshxml.dat component (03A3251BDE74DF30AB5BF0B73OE08C8D)

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>23march_coordinationHCM_MAG</td>
<td>49 KB</td>
<td>PDF File</td>
<td>3/25/2014 6:36 PM</td>
</tr>
<tr>
<td>24march_final_TAHE_TRANS~1</td>
<td>215 KB</td>
<td>Application</td>
<td>3/25/2014 8:38 PM</td>
</tr>
</tbody>
</table>
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”

Snack Menu (A)

Chicken Puff

Cheese Sandwich

B’cheer

Tea (or) Coffee

Image 2. “FDI Law Weeding Menu.doc”

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns TLP White

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

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 transition 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.

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 for and 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, Laos PDR, Myanmar, and Viet Nam (GLMV) and determines the approaches to improve delivery of IAI activities.

"ASEAN highly values the interest, participation and contribution of the Dialogue Partners and External Partners 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
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

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


Image 7. “ISEAS Perspective 29nov12.doc”
### Advanced Security Cooperation Course 13-1

<table>
<thead>
<tr>
<th>Learning Journal ASC 13-1</th>
<th>Today’s Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
<td></td>
</tr>
<tr>
<td>- General Insights</td>
<td>Reflections on processes or discussions</td>
</tr>
<tr>
<td>- Specific points of knowledge</td>
<td>- Things that you can/will use upon your return home</td>
</tr>
</tbody>
</table>

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 negotiation 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 interest of their countries.

---

**Image 8. “Learning Journal ASC 13-1_1.doc”**

---

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

For full indicator and other details, please contact intelreports@kaspersky.com
winMM-related Dropped Decoy Documents

Image 1. "book form for naming 30-8.doc" (dropped by 448cd7c3ae0ae445d805a4849fe5e120)
### Image 2. Unknown. Dropped by 748c4761822dc7076399922df58551ae

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>For full indicator and other details, please contact <a href="mailto:intelreports@kaspersky.com">intelreports@kaspersky.com</a></td>
</tr>
</tbody>
</table>
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

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

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

Image 4. Trade and Investment (english).doc
Dropped by b049fdee707e86e5e334f72cd50fdd8 “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

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>M/F</th>
<th>Address</th>
<th>Contact</th>
<th>Day 1</th>
<th>Day 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>H.E. U Thein Kyaw</td>
<td>M</td>
<td>Deputy Minister for the Foreign Affairs, Ministry of Foreign Affairs,</td>
<td>Ph./Fax: Mobile: Email:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Office No. 9, Nay Pyi Taw, Myanmar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Mr. San Yu Kyaw</td>
<td>M</td>
<td>Head of Branch, Ministry of Foreign Affairs, Office No. 9, Nay Pyi Taw,</td>
<td>Ph./Fax: (+95) 67412224 Mobile: (+95) 674075882 Email: <a href="mailto:sanyukyaw@gmail.com">sanyukyaw@gmail.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Myanmar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Mr. Kyaw Tin Shin</td>
<td>M</td>
<td>Deputy Director, Ministry of Foreign Affairs, Office No. 9, Nay Pyi Taw,</td>
<td>Ph./Fax: 413341 Mobile: 09-5033042 Email: <a href="mailto:ktkshin@gmail.com">ktkshin@gmail.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Myanmar</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Image 5. List of Attendance.doc
Dropped by F14C42765F130EE6DEC3A87DC50A47E1

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

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns TLP White

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

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

Image 8. Unknown.
Dropped by 6758fc7e483ad9cd6280bcc3f4d85222

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns TLP White

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

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

<table>
<thead>
<tr>
<th>1</th>
<th>척</th>
<th>A thing or an object</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>하다</td>
<td>To do</td>
</tr>
<tr>
<td>3</td>
<td>있다</td>
<td>To be</td>
</tr>
<tr>
<td>4</td>
<td>수</td>
<td>way, method</td>
</tr>
<tr>
<td>5</td>
<td>하다</td>
<td>To do</td>
</tr>
<tr>
<td>6</td>
<td>나</td>
<td>He</td>
</tr>
<tr>
<td>7</td>
<td>없다</td>
<td>Do not exist, absent</td>
</tr>
<tr>
<td>8</td>
<td>떨다</td>
<td>To not be, to not do</td>
</tr>
<tr>
<td>9</td>
<td>사람</td>
<td>Person</td>
</tr>
<tr>
<td>10</td>
<td>우리</td>
<td>us, our</td>
</tr>
<tr>
<td>11</td>
<td>그</td>
<td>He</td>
</tr>
<tr>
<td>12</td>
<td>아니다</td>
<td>To not be</td>
</tr>
<tr>
<td>13</td>
<td>보다</td>
<td>To try</td>
</tr>
<tr>
<td>14</td>
<td>그</td>
<td>That thing</td>
</tr>
</tbody>
</table>

Image 10. Unknown.
Dropped by 7F422B43EEB93B230FF7553C841C4785

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

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

Image 11. Unknown.
Dropped by 1d6258bc3688226e7cb56fb8215a8b

Image 12. Unknown.
Dropped by 7a9712cbb3e340e577ce0320ccee05f

As of 5.2.2013 [1900]

<table>
<thead>
<tr>
<th></th>
<th>0.00</th>
<th>100.00</th>
<th>0.00</th>
<th>0.00</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(0)</td>
<td>(1)</td>
<td>(2)</td>
<td>(3)</td>
</tr>
<tr>
<td>Executive Suite</td>
<td>40,000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Deluxe Suite</td>
<td>60,000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Deluxe (Single)</td>
<td>40,000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Superior Double</td>
<td>60,000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Superior</td>
<td>40,000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

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

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

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

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns TLP White

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

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

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

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns TLP White

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

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

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

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 (ဗ်စ်လျင်)
9. Air Bagan
10. Air Asia
11. Amara Hotel (last year)
12. Asia General Trading (last year)
13. Atran 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

For full indicator and other details, please contact intelreports@kaspersky.com
### Sightseeing Tour in Bagan

**Full Day Bagan Sightseeing tour with English Speaking Guide - 35 USD per person**
(for 30 persons who take full day tour)

**Half Day Bagan Sightseeing tour with English 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.docexe", 21119ddd01694bb9181286b52cf1203c

---

**Image 20. Ns admin.docx**

Dropped by "ns admin.docx.exe", 6f9b6adbb33b7c8912aa2e5ae1c39f7a

---

For full indicator and other details, please contact intelreports@kaspersky.com
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.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
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

Backdoor.Win32.Agent.*
Backdoor.Win32.Agent.bjer
Backdoor.Win32.Agent.dcyv
Backdoor.Win32.Agent.dbfk
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.cfj
Trojan-Spy.Win32.Agent.ciry
Trojan-Spy.Win32.Agent.ciui
Trojan-Spy.Win32.Agent.cita

For full indicator and other details, please contact intelreports@kaspersky.com
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

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

Trojan.Win32.Pincav.*
Trojan.Win32.Pincav.cnx

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

For full indicator and other details, please contact intelreports@kaspersky.com
APPENDIX C: MD5 REFERENCE SET

SslMM

469ca0c73398903908babcad14300d8d
95c4a236faa65b75dbb0076d8248584c

WinMM

c8c81cca4645e71213f2310cec6c277d
45a99f60654f22b671aec980687d0f15

WininetMM/Sakto

9883abc829870478ce6f3cfddbcbbaf2
a5721c5e7f2b49df82595819b5a49c0c

Injectv1/InjectResource

5c04904a50f0285851fb7292c13858ec

Exe_Exchange

6a82c153bd370250cc2fed89f1bb5c91
48fb78e8ba531505e246760c0d02d6b0

For full indicator and other details, please contact intelreports@kaspersky.com
Sys10

c58df5892700ac3f467524f86bf325c0
33d388c6e841ede3920f79516b5da032

xsPlus (nokian) and plugin

d86106faaa398b8d83437176bf5e39c4
041436594c1ce9e99c569fb7402fe0c7
d0fba5db608ac8f5a3d05a71ceb0eca1

For full indicator and other details, please contact intelreports@kaspersky.com
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
The MsnMM Campaigns
The Earliest Naikon APT Campaigns

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