The Chronicles of the Hellsing APT: the Empire Strikes Back

SL securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/

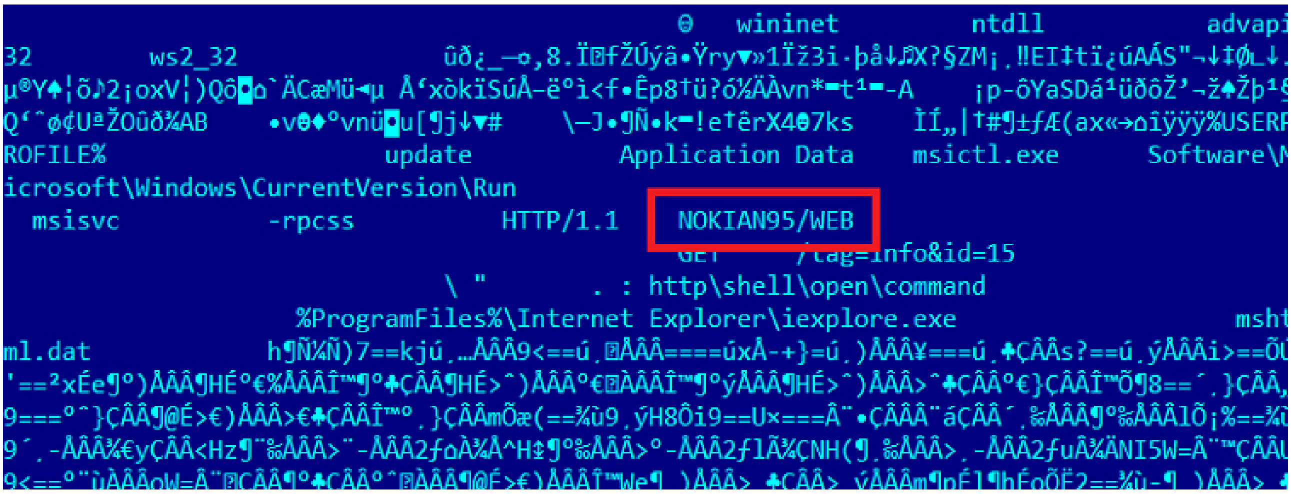
Authors

- Costin Raiu
- Maxim Golovkin

Introduction

One of the most active APT groups in Asia, and especially around the South China Sea area is “Naikon”. Naikon plays a key part in our story, but the focus of this report is on another threat actor entirely; one who came to our attention when they hit back at a Naikon attack.

Naikon is known for its custom backdoor, called RARSTONE, which our colleagues at Trend Micro have described in detail. The name Naikon comes from a custom user agent string, “NOKIAN95/WEB”, located within the backdoor:



```
                                             ⊖   wininet         ntdll           advapi
32        ws2_32             ûð¿_—¤,8.Ï⊡fŽÚýâ•Ÿry▼»1Ïž3i·þå↓♫X?§ZM¡.‼EI‡tï¿úAÁS"¬↓‡∅└↓.
µ®Y♠¦õ♪2¡oxV¦)Qô▪⌂`ÄCæMü◄µ Å‘xòkiSúÅ-ëºì<f•Êp8†ü?ó½ÄÀvn*▬t¹▬-A    ¡p-ôYaSDá¹üðôŽ’¬ž♠Žþ¹§
Q‘ˆø¢UªŽOûð¾AB    •v⊖♦ºvnü▪u[¶j↓▼#    \—J•¶Ñ•k▬!e†êrX4⊖7ks    ÌÍ„|†#¶±ƒÆ(ax«→⌂îÿÿÿ%USERP
ROFILE%                   update          Application Data    msictl.exe      Software\M
icrosoft\Windows\CurrentVersion\Run
  msisvc          -rpcss          HTTP/1.1    NOKIAN95/WEB
                                              GET     /tag=info&id=15
                              \ "         . : http\shell\open\command
                    %ProgramFiles%\Internet Explorer\iexplore.exe                  msht
ml.dat            h¶Ñ¼Ñ)7==kjú.…ÂÂÂ9<==ú.⊡ÂÂÂ====úxÅ-+}=ú.)ÂÂÂ¥===ú.♣ÇÂÂs?==ú.ýÂÂÂi>==ÕÜ
'==²xÉe¶º)ÂÂÂ¶HÉº€%ÂÂÂÎ™¶º♣ÇÂÂ¶HÉ>ˆ)ÂÂÂº€⊡ÀÂÂÎ™¶ºýÂÂÂ¶HÉ>ˆ)ÂÂÂ>ˆ♣ÇÂÂº€}ÇÂÂÎ™Õ¶8==´.}ÇÂÂ,
9===ºˆ}ÇÂÂ¶@É>€)ÂÂÂ>€♣ÇÂÂÎ™º.}ÇÂÂmÕæ(==¾ù9.ýH8Ôi9==U×===Â¨•ÇÂÂÂ¨áÇÂÂ´.‰ÂÂÂ¶º‰ÂÂÂ1Õ¡%==¾ù
9´.-ÂÂÂ¼€yÇÂÂ<Hz¶¨‰ÂÂÂ>¨-ÂÂÂ2ƒ⌂À¾Â^H‡¶º‰ÂÂÂ>º-ÂÂÂ2ƒlÃ¼ÇNH(¶.‰ÂÂÂ>.-ÂÂÂ2ƒuÃ¼ÄNI5W=Â¨™ÇÂÂU
9<==º¨ùÂÂÂoW=Â¨⊡ÇÂÂ¶º♣ÇÂÂºˆ⊡ÂÂÂ¶@É>€)ÂÂÂÎ™We¶ )ÂÂÂ> ♣ÇÂÂ> ýÂÂÂm¶pÉl¶hÉoÕË2==¾ù-¶ )ÂÂÂ> ♣
```

NOKIAN string in Naikon backdoor

The Naikon group is mostly active in countries such as the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, and Nepal, hitting a variety of targets in a very opportunistic way. What was perhaps one of the biggest operations of the Naikon group was launched in March 2014, in the wake of the MH370 tragedy that took place on March 8th. By March 11th, the Naikon group was actively hitting most of the nations involved in the search for MH370. The targets were extremely wide-ranging but included institutions with access to information related to the disappearance of MH370, such as:

- Office of the President
- Armed Forces
- Office of the Cabinet Secretary
- National Security Council(s)
- Office of the Solicitor General
- National Intelligence Coordinating Agency
- Civil Aviation Authority
- Department of Justice
- National Police
- Presidential Management Staff

The Naikon group used mostly spear-phished documents for the attacks, with CVE-2012-0158 exploits that dropped the group's signature backdoor.

While many of these attacks were successful, at least one of the targets didn't seem to like being hit, and instead of opening the documents, decided on a very different course of action.

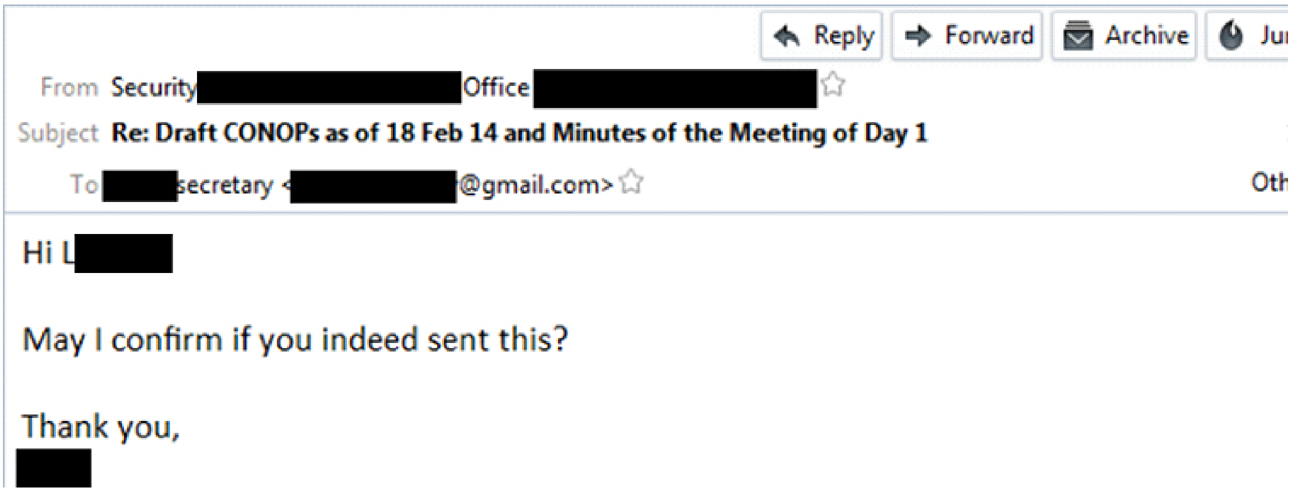
The empire strikes back

Here's a question – what should you do when you receiving a suspicious document from somebody you don't know, or know very little? Choose one:

- Open the document
- Don't open the document
- Open the document on a Mac (everybody knows Mac's don't get viruses)
- Open the document in a virtual machine with Linux

Based on our experience, most people would say 2, 3 or 4. Very few would open the document and even fewer would actually decide to test the attacker and verify its story.

But this is exactly what happened when one of the Naikon spear-phishing targets received a suspicious email. Instead of opening the document or choosing to open it on an exotic platform, they decided to check the story with the sender:



From Security[redacted]Office [redacted]

Subject Re: Draft CONOPs as of 18 Feb 14 and Minutes of the Meeting of Day 1

To [redacted]secretary <[redacted]@gmail.com>

Hi L[redacted]

May I confirm if you indeed sent this?

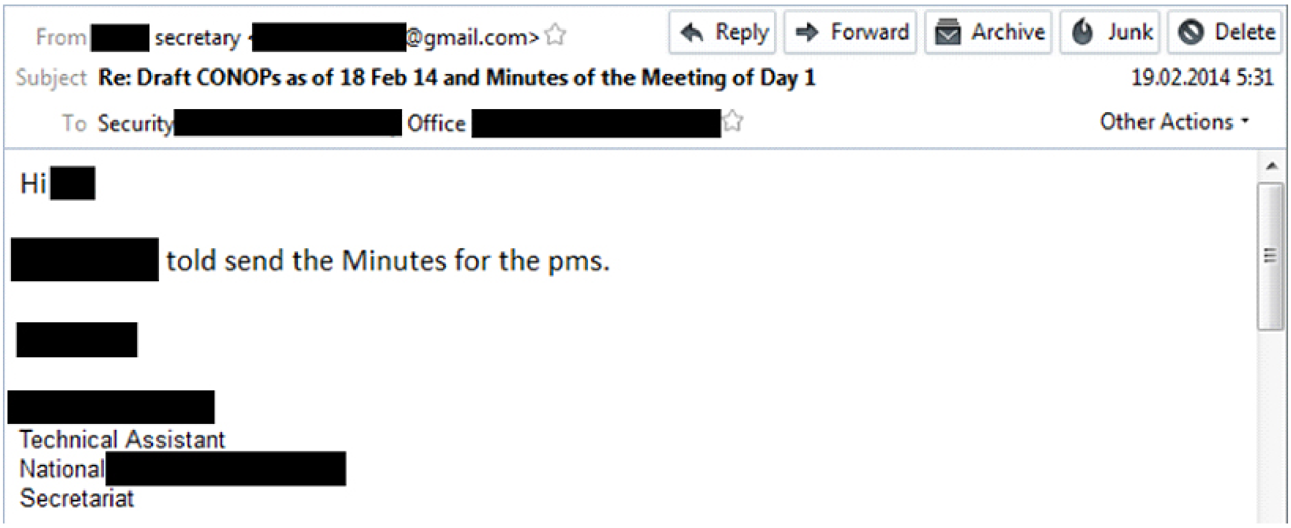
Thank you,

[redacted]

Naikon target asks for confirmation of the email

In the email above, we can see the target questioning the authenticity of the Naikon spear-phishing. They ask the sender if it was their intention to email this document.

The attacker was, of course, not confused in the slightest, and being very familiar with the internal structure of the target's government agency, replied claiming that they work for the secretariat division and were instructed to send it by the organization's management:



From [redacted] secretary [redacted]@gmail.com>

Subject Re: Draft CONOPs as of 18 Feb 14 and Minutes of the Meeting of Day 1 19.02.2014 5:31

To Security [redacted] Office [redacted]

Hi [redacted]

[redacted] told send the Minutes for the pms.

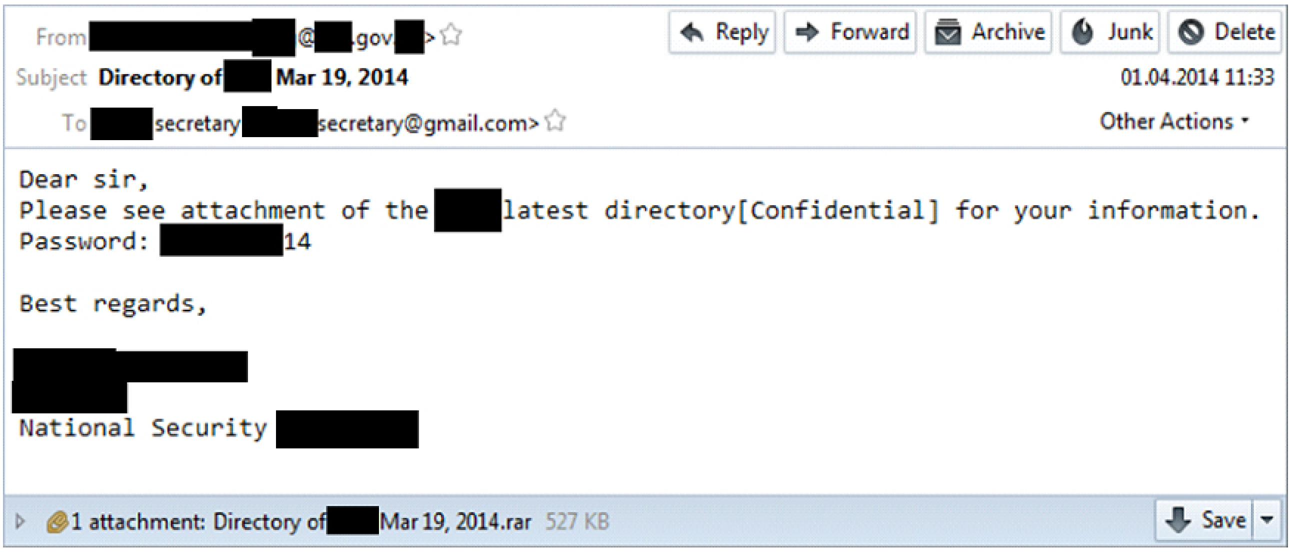
[redacted]

[redacted]
Technical Assistant
National [redacted]
Secretariat

Naikon attacker replies to the target

The reply is written in poor English and indicates that the attacker is probably not as proficient in the language as the intended victim. Seeing the reply, the target obviously decided not to open the document. Moreover, they decided to go a bit further and try to learn more about the attacker.

Not long after the first exchange, the following email was sent to the attacker by the target:



From [redacted]@[redacted].gov[redacted]>

Subject Directory of [redacted] Mar 19, 2014 01.04.2014 11:33

To [redacted] secretary [redacted] secretary@gmail.com>

Dear sir,
Please see attachment of the [redacted] latest directory[Confidential] for your information.
Password: [redacted] 14

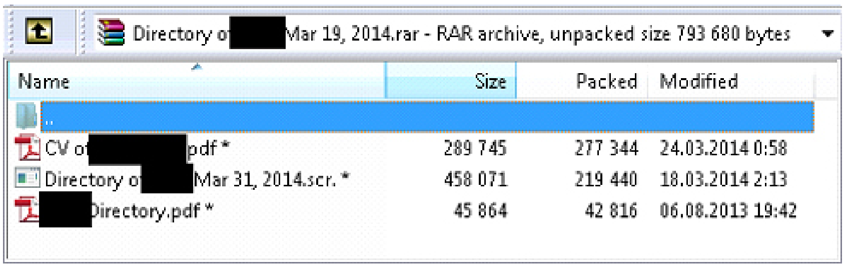
Best regards,

[redacted]

National Security [redacted]

1 attachment: Directory of [redacted] Mar 19, 2014.rar 527 KB

The attachment is a RAR archive with password, which allows it to safely bypass malware scanners associated with the free email account used by the attackers. Inside the archive we find two decode PDF files and one SCR file:



Directory o[redacted]Mar 19, 2014.rar - RAR archive, unpacked size 793 680 bytes

Name	Size	Packed	Modified
..			
CV o[redacted]pdf *	289 745	277 344	24.03.2014 0:58
Directory o[redacted]Mar 31, 2014.scr. *	458 071	219 440	18.03.2014 2:13
[redacted]Directory.pdf *	45 864	42 816	06.08.2013 19:42

Much to our surprise, the “SCR” file turned out to be a backdoor prepared especially for the Naikon fraudsters.

The file “**Directory of … Mar 31, 2014.scr**” (md5: **198fc1af5cd278091f36645a77c18ffa**) drops a blank document containing the error message and a backdoor module (md5: **588f41b1f34b29529bc117346355113f**). The backdoor connects to the command server located at **philippinenews[.]mooo[.]com**.

The backdoor can perform the following actions:

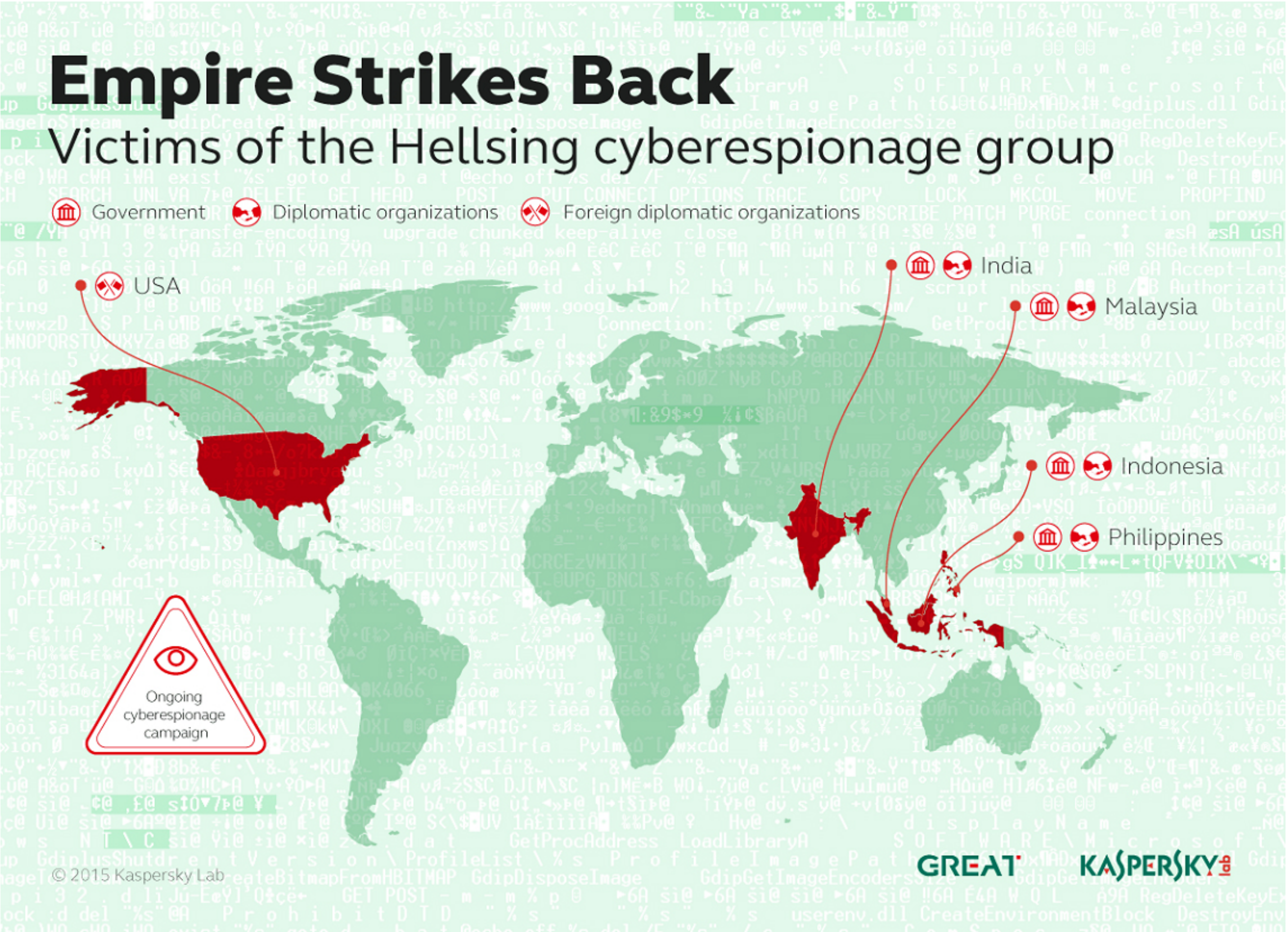
- download files
- upload files
- update itself
- uninstall itself

We were amazed to see this course of action and decided to investigate the “Empire Strikes Back”-door further; naming the actor “Hellsing” (explained later).

The malware used by the intended victim appears to have the following geographical distribution, according to KSN data:

- Malaysia – government networks
- Philippines – government networks
- Indonesia – government networks
- USA – diplomatic agencies
- India (old versions of malware)

In addition, we’ve observed the targeting of ASEAN-related entities.



Victims of Hellsing attacks

The actor targets its intended victims using spear-phishing emails with archives containing malware, similar to the one it used against the Naikon group. Some of the attachment names we observed include:

- 2013 Mid-Year IAG Meeting Admin Circular FINAL.7z
- HSG FOLG ITEMS FOR USE OF NEWLY PROMOTED YNC FEDERICO P AMORADA 798085 PN CLN.zip
- Home Office Directory as of May 2012.Please find attached here the latest DFA directory and key position officials for your referenece.scr
- LOI Nr 135-12 re 2nd Quarter.Scr
- Letter from Paquito Ochoa to Albert Del Rosario,the Current Secretary of Foreign Affairs of the Philippines.7z
- Letter to SND_Office Call and Visit to Commander, United States Pacific Command (USPACOM) VER 4.0.zip
- PAF-ACES Fellowship Program.scr
- RAND Analytic Architecture for Capabilities Based Planning, Mission System Analysis, and Transformation.scr
- Update Attachments_Interaction of Military Personnel with the President _2012_06_28.rar
- Update SND Meeting with the President re Hasahasa Shoal Incident.scr
- Washington DC Directory November 2012-EMBASSY OF THE PHILIPPINES.zip
- ZPE-791-2012&ZPE-792-2012.rar
- zpe-791-2012.PDF.scr

We’ve observed RAR, ZIP and 7ZIP archives in the attacks – the 7ZIP archives with passwords were probably introduced as a way to bypass the recent security features on Gmail, which block password-protected archives with executables inside.

Each backdoor has a command and control server inside as well as a version number and a campaign or victim identifier. Some examples include:

MD5	Date	C&C	Campaign identifier
2682a1246199a18967c98cb32191230c	Mar 31 2014	freebsd.extrimtur[.]com	1.6.1_MOTAC
31b3cc60dbecb653ae972db9e57e14ec	Mar 31 2014	freebsd.extrimtur[.]com	1.6.1_MOTAC
4dbfd37fd851daebdae7f009adec3cbd	Nov 08 2013	articles.whynotad[.]com	1.5_articles.whynotad.com-nsc
015915bbfcda1b2b884db87262970a11	Feb 19 2014	guaranteed9.strangled[.]net	1.5_guaranteed9-nsc
3a40e0deb14f821516eadaed24301335	Mar 31 2014	hosts.mysaol[.]com	1.6.1_imi;simple
73396bacd33cde4c8cb699bcf11d9f56	Nov 08 2013	web01.crabdance[.]com	1.5_op_laptop
7c0be4e6aee5bc5960baa57c6a93f420	Nov 08 2013	hosts.mysaol[.]com	1.5_MMEA
bff9c356e20a49bbcb12547c8d483352	Apr 02 2014	imgs09.homenet[.]org	1.6.1_It
c0e85b34697c8561452a149a0b123435	Apr 02 2014	imgs09.homenet[.]org	1.6.1_It
f13deac7d2c1a971f98c9365b071db92	Nov 08 2013	hosts.mysaol[.]com	1.5_MMEA
f74ccb013edd82b25fd1726b17b670e5	May 12 2014	second.photo-frame[.]com	1.6.2s_Ab

The campaign identifiers could be related to the organizations targeted by the specific builds of this APT. Some possible descriptions for these initials could be:

- MOTAC – Ministry of Tourism and Culture, Malaysia – http://www.motac.gov.my/en/
- NSC – http://www.nsc.gov.my/
- MMEA – Malaysian Maritime Enforcement Agency – http://www.mmea.gov.my

Artifacts and overlap with other APTs

Interestingly, some of the infrastructure used by the attackers appears to overlap (although around a year apart) with a group tracked internally at Kaspersky Lab as PlayfullDragon (also known as “GREF”); while other aspects of the infrastructure overlap with a group known as Mirage or Vixen Panda.

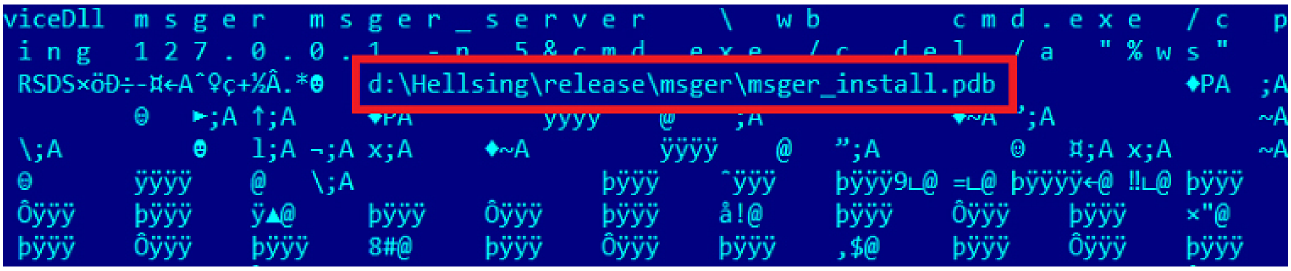
For instance, one of the PlayfullDragon's Xslcmd backdoors described by our colleagues from FireEye (md5: 6c3be96b65a7db4662ccaae34d6e72cc) beams to **cdi.indiadigest[.]in:53**. One of the Hellsing samples we analysed (md5: 0cbefd8cd4b9a36c791d926f84f10b7b) connects to the C&C server at **webmm[.]indiadigest[.]in**. Although the hostname is not the same, the top level domain suggests some kind of connection between the groups. Several other C&C subdomains on "indiadigest[.]in" include:

- aac.indiadigest[.]in
- ld.indiadigest[.]in
- longc.indiadigest[.]in

Another overlap we observed is with an APT known as Cycldek or Goblin Panda. Some of the Hellsing samples we analysed in this operation (e.g. md5: a91c9a2b1bc4020514c6c49c5ff84298) communicate with the server **webb[.]huntingtomingalls[.]com**, using a protocol specific to the Cycldek backdoors (binup.asp/textup.asp/online.asp).

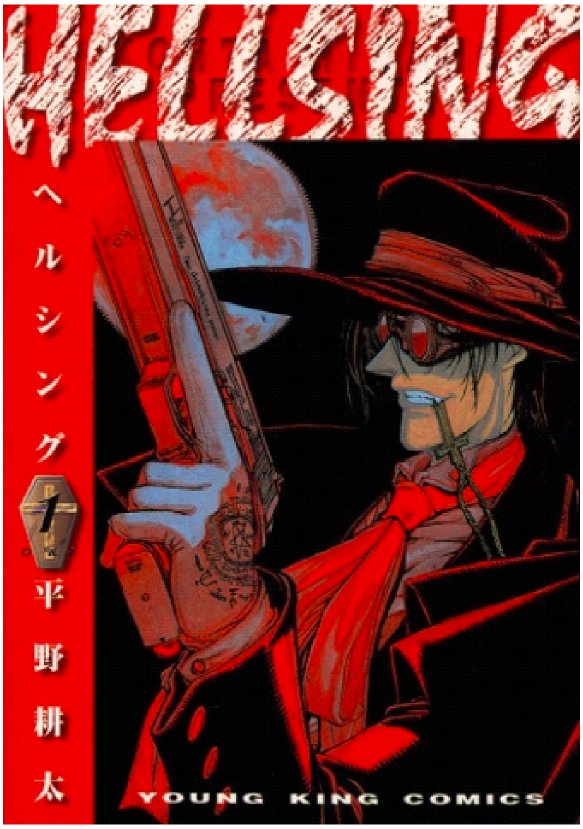
It appears that the Hellsing developer started with the Cycldek sources and worked together with the operators from other APT groups. Nevertheless, it is sufficiently different to warrant classification as a stand-alone operation.

So, where does the Hellsing name come from? One of the samples we analysed (md5: 036e021e1b7f61cddfd294f791de7ea2) appears to have been compiled in a rush and the attacker forgot to remove the debug information. One can see the project name is Hellsing and the malware is called "msger":



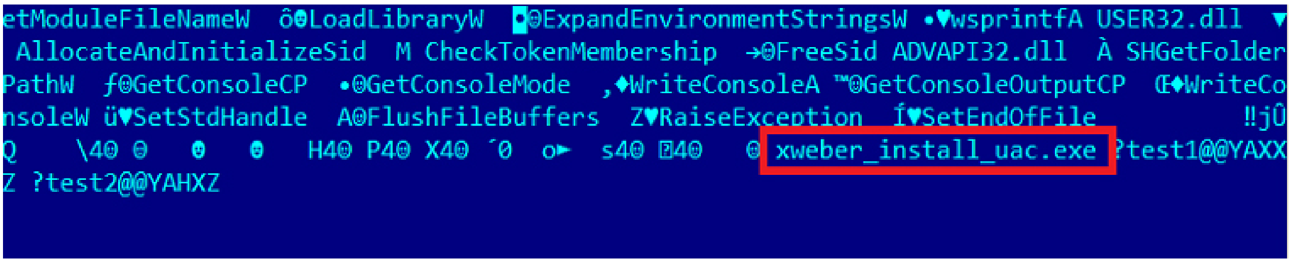
```
viceDll  msger  msger_server   \  wb      cmd.exe  /c  p
 ing  127.0.0.1  -n  5&cmd  exe  /c  del  /a  "%ws"
 RSDS×öÐ÷-¤←A˜♀ç+½Â.*☻  d:\Hellsing\release\msger\msger_install.pdb        ♦PA  ;A
        ☺   ►;A ↑;A      ♦PA        yyyy    @    ;A          ♦~A  ';A            ~A
\;A          ☻   l;A ¬;A x;A     ♦~A          ÿÿÿÿ    @    ";A         ☺   ¤;A x;A    ~A
 ☺       ÿÿÿÿ     @    \;A                  þÿÿÿ    ˆÿÿÿ    þÿÿÿ9└@ =└@ þÿÿÿÿ←@ ‼└@ þÿÿÿ
 Ôÿÿÿ    þÿÿÿ    ÿ▲@     þÿÿÿ    Ôÿÿÿ    þÿÿÿ    å!@     þÿÿÿ    Ôÿÿÿ    þÿÿÿ    ×"@
 þÿÿÿ    Ôÿÿÿ    þÿÿÿ    8#@     þÿÿÿ    Ôÿÿÿ    þÿÿÿ    ,$@     þÿÿÿ    Ôÿÿÿ    þÿÿÿ
```

Of course, Hellsing can have many different meanings, including the famous doctor from Bram Stoker's Dracula. However, according to Wikipedia, *"Hellsing (ヘルシング Herushingu) is also a Japanese manga series written and illustrated by Kouta Hirano. It first premiered in Young King Ours in 1997 and ended in September 2008"*.



The Hellsing series chronicles the efforts of the mysterious and secret Hellsing Organization, as it combats vampires, ghouls, and other supernatural foes; which makes it perhaps an appropriate name for our group.

In addition to the Hellsing/msger malware, we've identified a second generation of Trojan samples which appear to be called "xweber" by the attackers:



```
etModuleFileNameW  ô☻LoadLibraryW  •☺ExpandEnvironmentStringsW •♥wsprintfA USER32.dll  ▼
 AllocateAndInitializeSid  M CheckTokenMembership  →☺FreeSid ADVAPI32.dll  À SHGetFolder
PathW  ƒ☺GetConsoleCP  •☺GetConsoleMode  ,♦WriteConsoleA ™☺GetConsoleOutputCP  Œ♦WriteCo
nsoleW ü♥SetStdHandle  A☺FlushFileBuffers  Z♥RaiseException  Í♥SetEndOfFile        ‼jÛ
Q    \4☺ ☺   ☻   ☻   H4☺ P4☺ X4☺ ´0  o►  s4☺ ?4☺   ☺ xweber_install_uac.exe ?test1@@YAXX
Z ?test2@@YAHXZ
```

"Xweber" seems to be the more recent Trojan, taking into account compilation timestamps. All the "msger" samples we have seen appear to have been compiled in 2012. The "Xweber" samples are from 2013 and from 2014, indicating that at some point during 2013 the "msger" malware project was renamed and/or integrated into "Xweber".

During our investigation we've observed the Hellsing APT using both the "Xweber" and "msger" backdoors in their attacks, as well as other tools named "xrat", "clare", "irene" and "xKat".

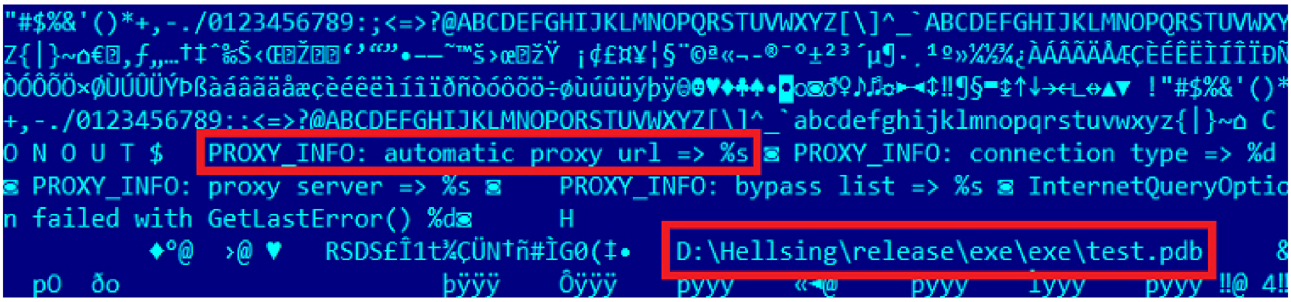
Other tools

Once the Hellsing attackers compromise a computer, they deploy other tools which can be used for gathering further information about the victim or doing lateral movement. One such tool is "test.exe":

Name	test.exe
Size	45,568 bytes
MD5	14309b52f5a3df8cb0eb5b6dae9ce4da

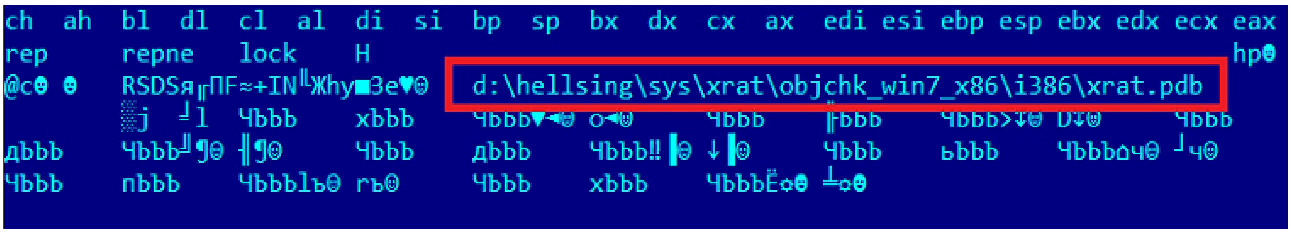
Type	Win32 PE i386 executable

This tool is used to gather information and test available proxies. Interestingly, it also contains the Hellsing debug path:



```
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXY
Z{|}~⌂€,ƒ„…†‡ˆ‰Š‹ŒŽ‘’“”•–—˜™š›œžŸ ¡¢£¤¥¦§¨©ª«¬-®¯°±²³´µ¶·¸¹º»¼½¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑ
ÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñòóôõö÷øùúûüýþÿ☺☻♥♦♣♠•◘○◙♂♀♪♫☼►◄↕‼¶§▬↨↑↓→←∟↔▲▼ !"#$%&'()*
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~⌂ C
O N O U T $   PROXY_INFO: automatic proxy url => %s ◙ PROXY_INFO: connection type => %d
◙ PROXY_INFO: proxy server => %s ◙    PROXY_INFO: bypass list => %s ◙ InternetQueryOptio
n failed with GetLastError() %d◙      H
          ♦°@  ›@ ♥   RSDS£Î1t¾ÇÜN†ñ#ÌG0(‡•   D:\Hellsing\release\exe\exe\test.pdb     &
 pO  ðo                     þÿÿÿ    Ôÿÿÿ    pyyy    «◄@     pyyy    Iyyy    pyyy ‼@ 4‼
```

Another attack tool deployed in a victim's environment was a file system driver, named "diskfilter.sys", although internally it claims to be named "xrat.sys". The driver is unsigned and compiled for 32-bit Windows. It was used briefly in 2013, before being abandoned by the attackers, possibly due to Windows 7 driver signing requirements:



```
ch  ah  bl  dl  cl  al  di  si  bp  sp  bx  dx  cx  ax  edi esi ebp esp ebx edx ecx eax
rep     repne   lock    H                                                           hp☻
@c☻ ☻   RSDSя╓ПF≈+IN╙Жhy■Зe♥☺  d:\hellsing\sys\xrat\objchk_win7_x86\i386\xrat.pdb
        ░j  ┘l  Чbbb    xbbb    Чbbb▼◄☺ o◄☺     Чbbb    ╟bbb    Чbbb>↨☻ D↨☺     Чbbb
дbbb    Чbbb╝¶☻ ╢¶☺     Чbbb    дbbb    Чbbb‼▐☻ ↓▐☺     Чbbb    ьbbb    Чbbb⌂ч☻ ┘ч☺
Чbbb    пbbb    Чbbblь☻ rь☺     Чbbb    xbbb    ЧbbbЁ¤☻ ╧¤☻
```

Another tool used by the attackers is called "xKat":

Name	xkat.exe
Size	78,848 bytes
MD5	621e4c293313e8638fb8f725c0ae9d0f
Type	Win32 PE i386 executable

This is a powerful file deletion and process killer which uses a driver (Dbgv.sys) to perform the operations. We've seen it being used by the attackers to kill and delete malware belonging to their competitors.

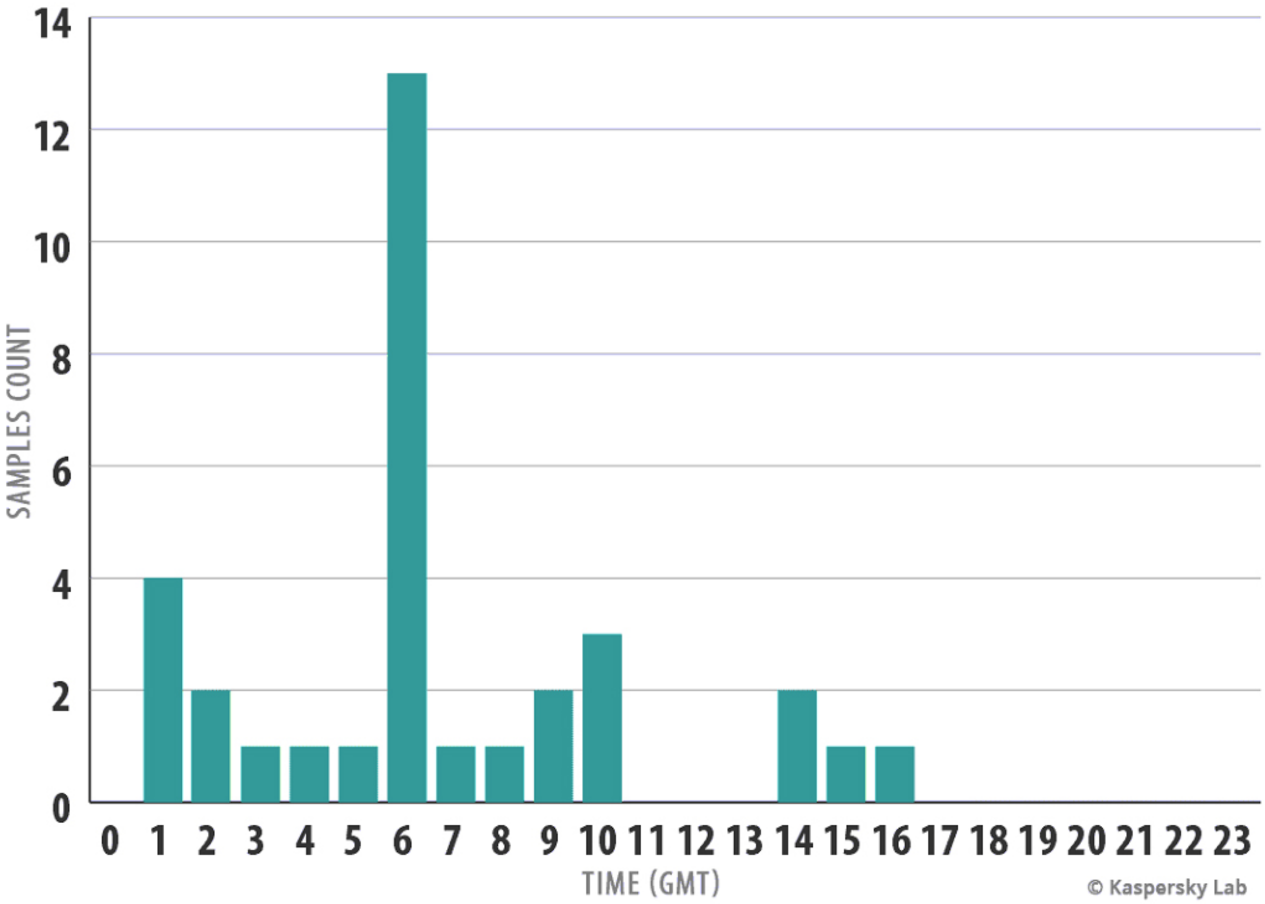
Some of the debug paths found in the binaries include:

- e:\Hellsing\release\clare.pdb
- e:\Hellsing\release\irene\irene.pdb
- d:\hellsing\sys\irene\objchk_win7_x86\i386\irene.pdb
- d:\hellsing\sys\xkat\objchk_win7_x86\i386\xKat.pdb
- d:\Hellsing\release\msger\msger_install.pdb
- d:\Hellsing\release\msger\msger_server.pdb
- d:\hellsing\sys\xrat\objchk_win7_x86\i386\xrat.pdb
- D:\Hellsing\release\exe\exe\test.pdb

Attribution

In general, the attribution of APTs is a very tricky task which is why we prefer to publish technical details and allow others to draw their own conclusions.

The Hellsing-related samples appear to have been compiled around the following times:



Assuming normal work starts at around 9 am, the attacker seems to be most active in a time-zone of GMT+8 or +9, considering a work program of 9/10 am to 6/7pm.

Conclusions

The Hellsing APT group is currently active in the APAC region, hitting targets mainly in the South China Sea area, with a focus on Malaysia, the Philippines and Indonesia. The group has a relatively small footprint compared to massive operations such as "Equation". Smaller groups can have the advantage of being able to stay under the radar for longer periods of time, which is what happened here.

The targeting of the Naikon group by the Hellsing APT is perhaps the most interesting part. In the past, we've seen APT groups accidentally hitting each other while stealing address books from victims and then mass-mailing everyone on each of these lists. But, considering the timing and origin of the attack, the current case seems more likely to be an APT-on-APT attack.

To protect against a Hellsing attack, we recommend that organisations follow basic security best practices:

- Don't open attachments from people you don't know
- Beware of password-protected archives which contain SCR or other executable files inside
- If you are unsure about the attachment, try to open it in a sandbox
- Make sure you have a modern operating system with all patches installed
- Update all third party applications such as Microsoft Office, Java, Adobe Flash Player and Adobe Reader

Kaspersky Lab products detect the backdoors used by the Hellsing attacker as: **HEUR:Trojan.Win32.Generic, Trojan-Dropper.Win32.Agent.kbuj, Trojan-Dropper.Win32.Agent.kzqq**.

Authors

- Costin Raiu

- Maxim Golovkin

The Chronicles of the Hellsing APT: the Empire Strikes Back