The Naikon APT

SL securelist.com/analysis/publications/69953/the-naikon-apt/

Authors

-  Kurt Baumgartner
- Expert Maxim Golovkin

Tracking Down Geo-Political Intelligence Across APAC, One Nation at a Time

Our recent report, "The Chronicles of the Hellsing APT: the Empire Strikes Back" began with an introduction to the Naikon APT, describing it as "One of the most active APTs in Asia, especially around the South China Sea". Naikon was mentioned because of its role in what turned out to be a unique and surprising story about payback. It was a Naikon attack on a Hellsing-related organization that first introduced us to the Hellsing APT. Considering the volume of Naikon activity observed and its relentless, repeated attack attempts, such a confrontation was worth looking into, so we did.

> The #NaikonAPT group was spear-phished by an actor we now call “Hellsing”
>
> Tweet

The Naikon APT aligns with the actor our colleagues at FireEye recently revealed to be APT30, but we haven’t discovered any exact matches. It is hardly surprising that there is an element of overlap, considering both actors have for years mined victims in the South China Sea area, apparently in search of geo-political intelligence.

> The #NaikonAPT group has for 5 years mined victims, apparently in search of geo-political intelligence
>
> Tweet

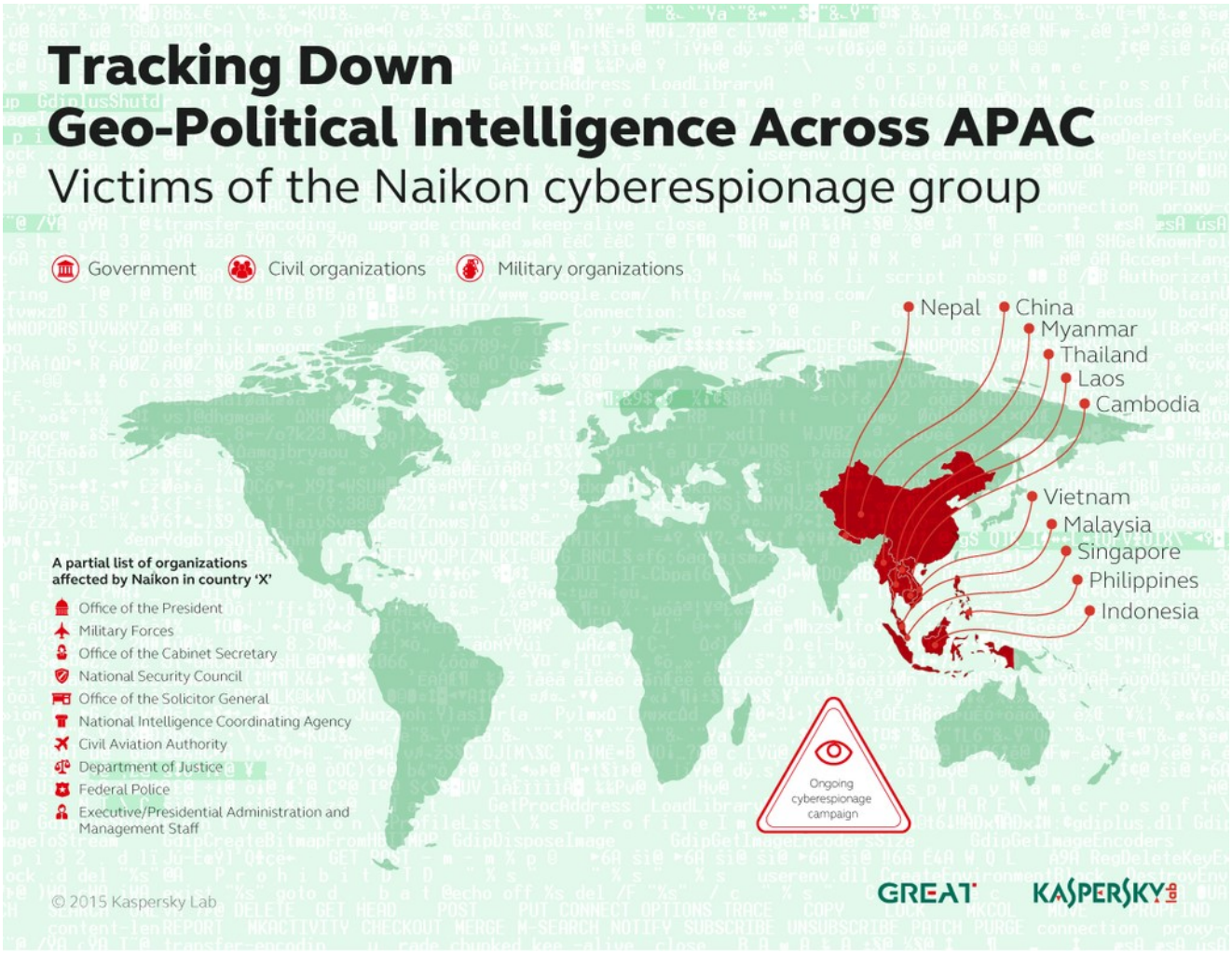
This Naikon report will be complemented by a follow-on report that will examine the Naikon TTP and the incredible volume of attack activity around the South China Sea that has been going on since at least 2010.

Noteworthy operational and logistical characteristics of this APT include:

- At least five years of high volume, high profile, geo-political attack activity
- Geographical focus – per-country, individual operator assignment and proxy presence
- Dynamic, well organized infrastructure
- Reliance on an externally developed, consistent set of tools comprising a full-featured backdoor, a builder, and an exploit builder
- High success rate in infiltrating national organisations in ASEAN countries

Highly Focused and Effective Around the South China Sea

In the spring of 2014, we noticed an increase in the volume of attack activity by the Naikon APT. The attackers appeared to be Chinese-speaking and targeted mainly top-level government agencies and civil and military organizations in countries such as the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, Nepal, Thailand, Laos and China.



Decoy

An attack typically starts with an email carrying an attachment that contains information of interest to the potential victim. The document may be based on information from open sources or on proprietary information stolen from other compromised systems.

This bait "document", or email attachment, appears to be a standard Word document, but is in fact an CVE-2012-0158 exploit, an executable with a double extension, or an executable with an RTLO filename, so it can execute code without the user's knowledge or consent. When the executable is launched, spyware is installed on the victim computer at the same time as a decoy document is displayed to the user; fooling them into thinking they have simply opened a document.

Configuration

The Naikon tool of choice generates a special, small, encrypted file which is 8,000 bytes in size, containing code to be injected into the browser along with configuration data. With the help of a start-up module, this whole file is injected into the browser memory and decrypts the configuration block containing the following:

- C&C server
- Ports and path to the server
- User-agent string
- Filenames and paths to its components
- Hash sums of the user API functions

The same code then downloads its main body from the C&C server using the SSL protocol, loads it independently from the operating system functions and, without saving it to the hard drive, hands over control to the XS02 function. All functionality is handled in memory.

```
mov     eax, [ebp+F.RtlGetLastWin32Error]
push    eax
mov     ecx, [ebp+F.VirtualFree]
push    ecx
mov     edx, [ebp+F.VirtualAlloc]
push    edx
mov     eax, [ebp+F.GetProcAddress]
push    eax
mov     ecx, [ebp+F.LoadLibraryA]
push    ecx
mov     edx, [ebp+lpModuleName]
push    edx
call    LoadModule      ; Manual loading of main payload module
add     esp, 18h
mov     [ebp+payMod], eax
cmp     [ebp+payMod], 0
jz      short loc_B13
push    7C8EB852h       ; "XS02" hash
mov     eax, [ebp+payMod]
push    eax
call    GetProcByHash   ; Manual getting of XS02 function address
add     esp, 8
mov     [ebp+var_XS02], eax
cmp     [ebp+var_XS02], 0
jz      short loc_AFF
lea     edx, [ebp+var_A88]
push    edx
call    [ebp+var_XS02]  ; Execute main payload function XS02
```

Payload

The main module is a remote administration utility. Using SSL, the module establishes a reverse connection to the C&C server as follows: it sets up an outgoing connection to the C&C server and checks if there is a command that it should execute. If there is, it executes the command and returns the result to the C&C. There are 48 commands in the module's repertoire, which a remote operator can use to effectively control the victim computer. This includes taking a complete inventory, downloading and uploading data, installing add-on modules, or working with the command line.

> The main module supports 48 commands, which the attackers can use to control the victim machine #NaikonAPT
>
> Tweet

Here is the complete list of commands:

0	CMD_MAIN_INFO
1	CMD_PROCESS_REFRESH
2	CMD_PROCESS_NAME
3	CMD_PROCESS_KILL
4	CMD_PROCESS_MODULE
5	CMD_DRIVE_REFRESH
6	CMD_DIRECTORY
7	CMD_DIRECTORY_CREATE
8	CMD_DIRECTORY_CREATE_HIDDEN
9	CMD_DIRECTORY_DELETE
10	CMD_DIRECTORY_RENAME
11	CMD_DIRECOTRY_DOWNLOAD
12	CMD_FILE_REFRESH
13	CMD_FILE_DELETE
14	CMD_FILE_RENAME
15	CMD_FILE_EXECUTE_NORMAL
16	CMD_FILE_EXECUTE_HIDDEN
17	CMD_FILE_EXECUTE_NORMAL_CMD
18	CMD_FILE_EXECUTE_HIDDEN_CMD
19	CMD_FILE_UPLOAD
20	CMD_FILE_DOWNLOAD
21	CMD_WINDOWS_INFO
22	CMD_WINDOWS_MESSAGE

23	CMD_SHELL_OPEN
24	CMD_SHELL_CLOSE
25	CMD_SHELL_WRITE
26	CMD_SERVICE_REFRESH
27	CMD_SERVICE_CONTROL
28	CMD_PROGRAM_INFO
29	CMD_UNINSTALL_PROGRAM
30	CMD_REGESTRY_INFO
31	CMD_ADD_AUTO_START
32	CMD_MY_PLUGIN
33	CMD_3RD_PLUGIN
34	CMD_REG_CREATEKEY
35	CMD_REG_DELETEKEY
36	CMD_REG_SETVALUE
37	CMD_REG_DELETEVALUE
38	CMD_SELF_KILL
39	CMD_SELF_RESTART
40	CMD_SELF_CONFIG
41	CMD_SELF_UPDATE
42	CMD_SERVER_INFO
43	CMD_INSTALL_SERVICE
44	CMD_FILE_DOWNLOAD2
45	CMD_RESET
46	CMD_CONNECTION_TABLE
50	CMD_HEART_BEAT

Several modifications of the main module exist. There are no fundamental differences between modifications; it's just that extra features get added to the latest versions, such as compression and encryption of transmitted data, or the piecemeal download of large files.

d085ba82824c1e61e93e113a705b8e9a	118272	Aug 23 18:46:57 2012
b4a8dc9eb26e727eafb6c8477963829c	140800	May 20 11:56:38 2013
172fd9cce78de38d8cbcad605e3d6675	118784	Jun 13 12:14:40 2013
d74a7e7a4de0da503472f1f051b68745	190464	Aug 19 05:30:12 2013
93e84075bef7a11832d9c5aa70135dc6	154624	Jan 07 04:39:43 2014

CC-Proxy-Op

C&C server operations are characterized by the following:

- Low maintenance requirements
- Organized geo-specific task assignments
- Different approaches to communication

The C&C servers must have required only a few operators to manage the entire network. Each operator appears to have focused on their own particular set of targets, because a correlation exists between C&C and the location of targets/victims.

> There is a geo-specific correlation between the location of #NaikonAPT C&Cs and that of targets/victims
>
> Tweet

Communication with victim systems changed depending on the target involved. In some cases, a direct connection was established between the victim computer and the C&C. In other cases, the connection was established via dedicated proxy servers installed on dedicated servers rented in third countries. In all likelihood, this additional setup was a reaction to the network administrators in some targets limiting or monitoring outbound network connections from their organizations.

Here is a partial list of C&C servers and victim locations, demonstrating the geo-specific correlation:

ID	Jakarta	linda.googlenow.in
ID	Jakarta	admin0805.gnway.net
ID	Jakarta	free.googlenow.in

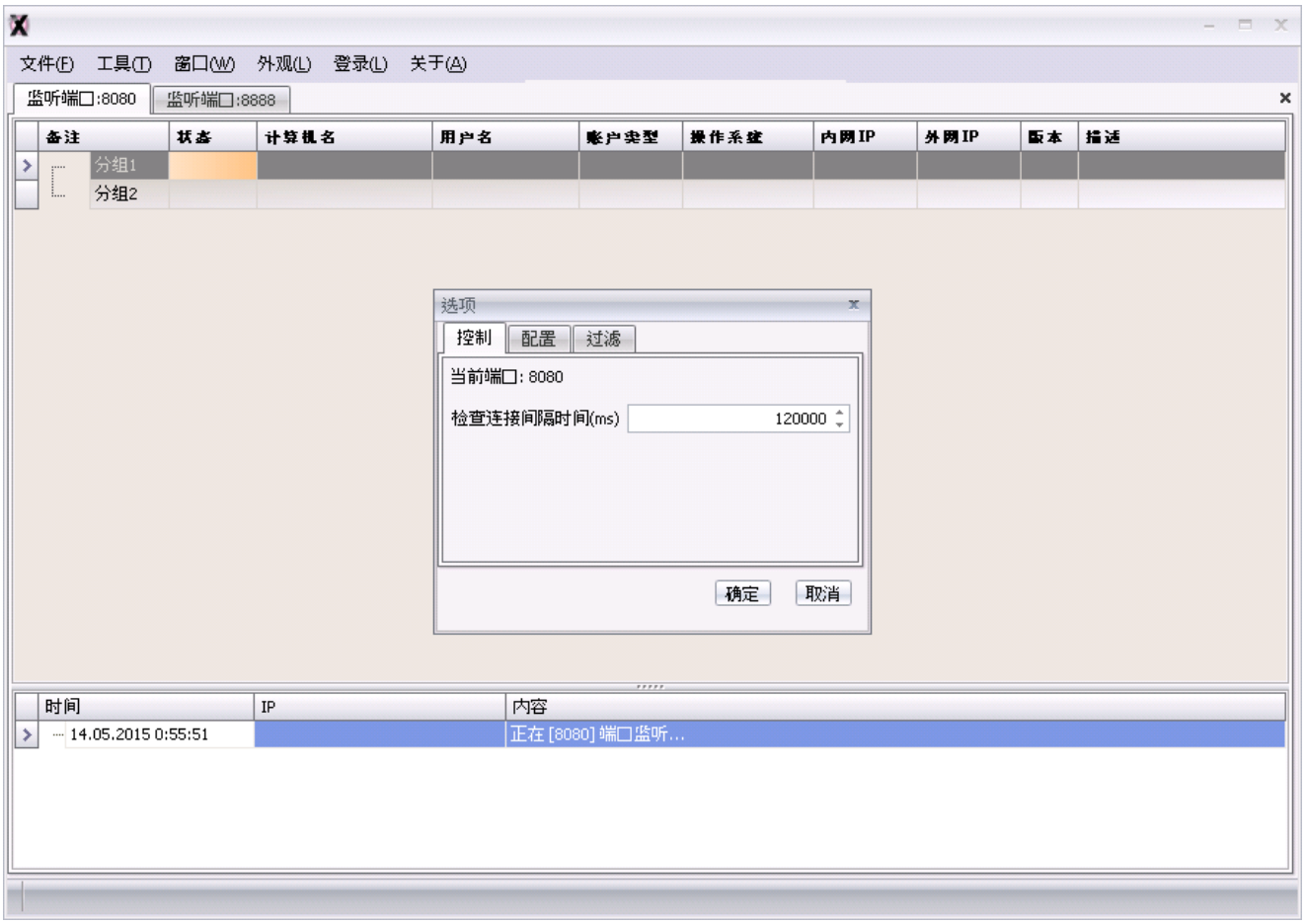
ID		frankhere.oicp.net
ID	Bandung	frankhere.oicp.net
ID	Bandung	telcom.dhtu.info
ID	Jakarta	laotel08.vicp.net
JP	Tokyo	greensky27.vicp.net
KH		googlemm.vicp.net
KH	Phnom Penh	googlemm.vicp.net
MM		peacesyou.imwork.net
MM		sayakyaw.xicp.net
MM		ubaoyouxiang.gicp.net
MM	Yangon	htkg009.gicp.net
MM		kyawthumyin.xicp.net
MM		myanmartech.vicp.net
MM		test-user123.vicp.cc
MY		us.googlereader.pw
MY		net.googlereader.pw
MY		lovethai.vicp.net
MY		yahoo.goodns.in
MY	Putrajaya	xl.findmy.pw
MY	Putrajaya	xl.kevins.pw
PH	Caloocan	oraydns.googlesec.pw
PH	Caloocan	gov.yahoomail.pw
PH		pp.googledata.pw
PH		xl.findmy.pw
PH		mlfjcjssl.gicp.net
PH		o.wm.ggpw.pw

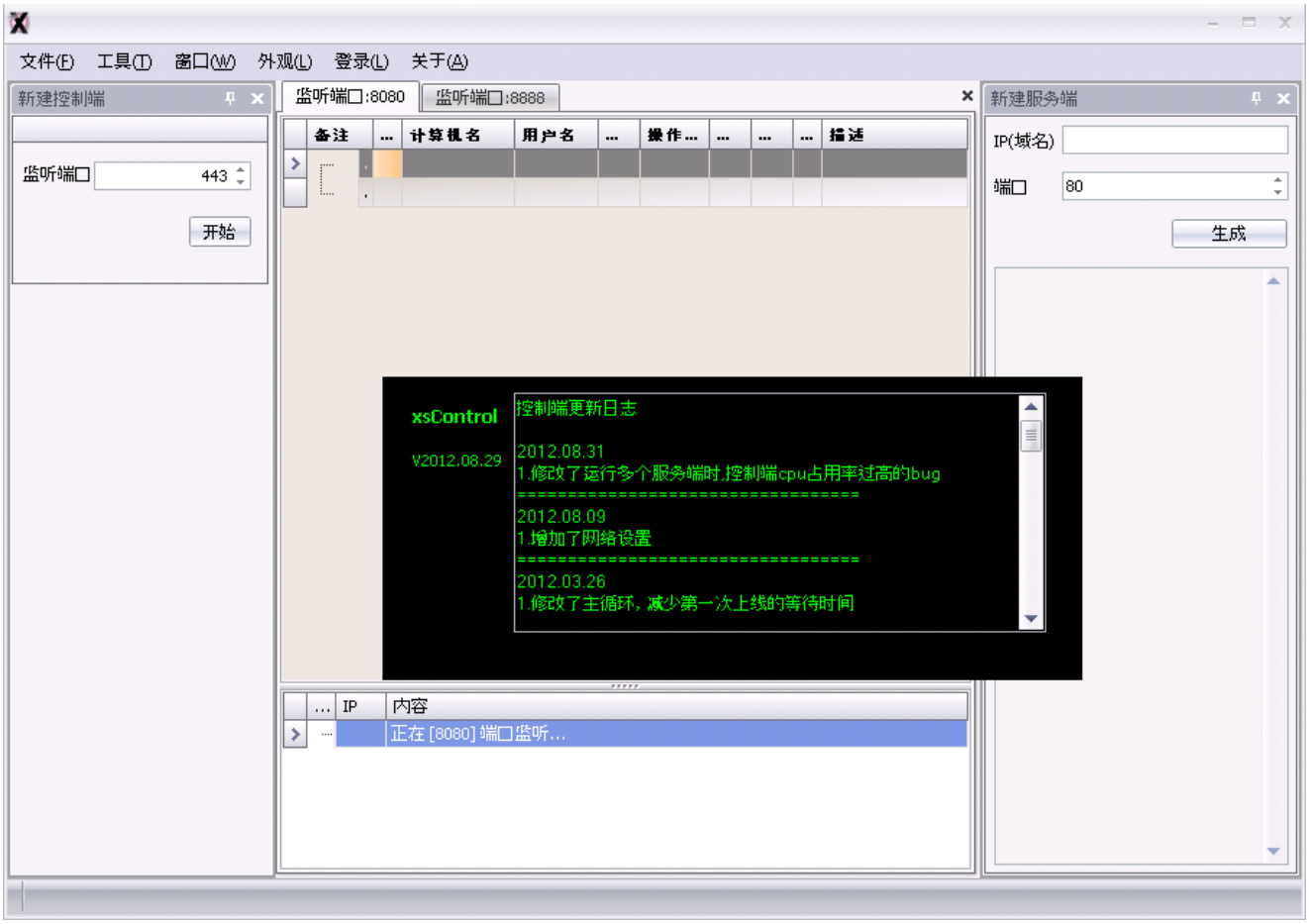
PH		oooppp.findmy.pw
PH		cipta.kevins.pw
PH		phi.yahoomail.pw
SG	Singapore	xl.findmy.pw
SG	Singapore	dd.googleoffice.in
VN	Hanoi	moziliafirefox.wicp.net
VN	Hanoi	bkav.imshop.in
VN	Hanoi	baomoi.coyo.eu
VN	Dong Ket	macstore.vicp.cc
VN	Hanoi	downloadwindows.imwork.net
VN	Hanoi	vietkey.xicp.net
VN	Hanoi	baomoi.vicp.cc
VN	Hanoi	downloadwindow.imwork.net
VN	Binh Duong	www.ttxvn.net
VN	Binh Duong	vietlex.gnway.net
VN	Hanoi	www.ttxvn.net
VN	Hanoi	us.googlereader.pw
VN	Hanoi	yahoo.goodns.in
VN	Hanoi	lovethai.vicp.net
VN	Hanoi	vietlex.gnway.net

XSControl – the Naikon APT's "victim management software"

In the Naikon scheme, a C&C server can be specialized XSControl software running on the host machine. It can be used to manage an entire network of infected clients. In some cases, a proxy is used to tunnel victim traffic to the XSControl server. A Naikon proxy server is a dedicated server that accepts incoming connections from victim computers and redirects them to the operator's C&C. An individual Naikon proxy server can be set up in any target country with traffic tunnelling from victim systems to the related C&C servers

XSControl is written in .NET with the use of DevExpress:


文件(F)
工具(T)
窗口(W)
外观(L)
登录(L)
关于(A)
监听端口:8080
监听端口:8888
备注
状态
计算机名
用户名
账户类型
操作系统
内网IP
外网IP
版本
描述
分组1
分组2
选项
控制
配置
过滤
当前端口: 8080
检查连接间隔时间(ms)
120000
确定
取消
时间
IP
内容
14.05.2015 0:55:51
正在 [8080] 端口监听...



Its main capabilities are:

- Accept initial connections from clients
- Provide clients with the main remote administration module
- Enable them to remotely administer infected computers with the help of a GUI
- Keep logs of client activity
- Keep logs of operator activity
- Upload logs and files to an FTP server

The operator's activity logs contain the following:

- An XML database of downloaded files, specifying the time of operation, the remote path and the local path
- A database of file names, the victim computer registry keys for the folders and requested sections
- A history of executed commands

Country X, Operator X

Now let's do an overview of one Naikon campaign, focusing on country "X".

Analysis revealed that the cyber-espionage campaign against country X had been going on for many years. Computers infected with the remote control modules provided attackers with access to employees' corporate email and internal resources, and access to personal and corporate email content hosted on external services.

Below is a partial list of organizations affected by Naikon's "operator X's" espionage campaign in country X.

- Office of the President
- Military Forces
- Office of the Cabinet Secretary
- National Security Council
- Office of the Solicitor General
- Intelligence Services
- Civil Aviation Authority
- Department of Justice
- Federal Police
- Executive/Presidential Administration and Management Staff

A few of these organizations were key targets and under continuous, real-time monitoring. It was during operator X's network monitoring that the attackers placed Naikon proxies within the countries' borders, to cloak and support real-time outbound connections and data exfiltration from high-profile victim organizations.

In order to obtain employees' credentials, operator X sometimes used keyloggers. If necessary, operator X delivered them via the remote control client. In addition to stealing keystrokes, this attacker also intercepted network traffic. Lateral movements included copying over and remotely setting up winpcap across desktop systems within sensitive office networks, then remotely setting up AT jobs to run these network sniffers. Some APTs like Naikon distribute tools such as these across multiple systems in order to regain control if it is lost accidentally and to maintain persistence.

> The #NaikonAPT group took advantage of cultural idiosyncrasies in its target countries
>
> Tweet

Operator X also took advantage of cultural idiosyncrasies in its target countries, for example, the regular and widely accepted use of personal Gmail accounts for work. So it was not difficult for the Naikon APT to register similar-looking email addresses and to spear-phish targets with attachments, links to sites serving malware, and links to google drive.

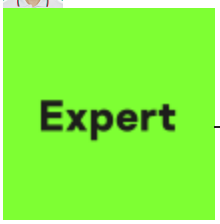
The empire strikes back

Every once in a while the Naikon group clashes with other APT groups that are also active in the region. In particular, we noticed that the Naikon group was spear-phished by an actor we now call “Hellsing”. More details about the cloak and dagger games between Naikon and Hellsing can be found in our blogpost: “The Chronicles of the Hellsing APT: The Empire Strikes Back“.

Read more about how you can protect your company against the Naikon threat actor here

- APT
- Cyber espionage
- Social engineering
- Targeted attacks
- Vulnerabilities and exploits

Authors

-  Kurt Baumgartner
- 

Maxim Golovkin

The Naikon APT

Your email address will not be published. Required fields are marked *