What we know about the South Korea NIS's use of Hacking Team's RCS

August 9, 2015

Tagged: Hacking Team, South Korea

Categories: Author, Bill Marczak, Reports and Briefings, Research News, Sarah McKune

Authors: Bill Marczak, Sarah McKune

Summary

This research note outlines what we know about the use of Hacking Team's Remote Control System (RCS) by South Korea's National Intelligence Service (NIS). The note synthesizes information found in publicly leaked materials, as well as our own research.

The data available in the leaked Hacking Team files provides circumstantial evidence pointing to an interest in compromising individuals with ties to South Korea (i.e., Korean language speakers who use software or apps popular in South Korea, or South Korean editions of Samsung phones).

The leaked data alone cannot identify specific individuals targeted by NIS, nor prove misuse of the technology; further investigation and research is necessary to make those determinations. Moreover, the presence of intrusion software does not necessarily equate to its misuse, as such software may be utilized by intelligence or law enforcement agencies in a manner that conforms with rule of law and democratic principles. We are releasing this report in order to assist with further investigation and research into South Korea's use of Hacking Team.

요약

본 연구노트는 한국 국정원의 해킹팀 RCS (Remote Control System) 사용에 관해 저희가 알고 있는 것을 개략적으로 기술한 것입니다. 노트에는 공개적으로 유출된 자료와 저희의 연구를 통해 발견된 정보가 함께 포함되어 있습니다.

중요한 것은, 유출된 해킹팀 파일에서 발견된 자료에는 국정원이 한국과 관련 있는 개인 (민간인) 들을 사찰하는 데 관심이 있었다는 정황적 증거들(사례 : 한국에서 대중적인 소프트웨어나 앱을 사용하는 한국어 사용자 또는 삼성의 내수용(한국 에디션) 스마트폰)이 포함되어 있다는 점입니다.

유출된 자료만으로는 국정원이 대상으로 삼은 특정인의 신원을 알 수 없으며, 해당 기술이 악용되었는지도 증명할 수 없습니다. 이를 확인하기 위해서는 추가적인 조사와 연구가 필요합니다. 또한 침입소프트웨어/해킹프로그램이 존재한다고 하여 악용되었을 것이라고 단정하기 어렵습니다. 정보기관이나 법집행기관이 이러한 프로그램을 적법한 절차와 민주적 원칙에 따라 사용할 수도 있기 때문입니다. 저희는 한국에서의 해킹팀 사용에 대한 추가적인 조사와 연구를 돕고자 본 보고서를 공개합니다.

Background

The National Intelligence Service (NIS) is Korea's main intelligence agency. It was founded in 1961 as the Korea Central Intelligence Agency (KCIA).[1] The name and functions of the agency have evolved considerably over time. Named the NIS in 1999, it has a three-part mandate: domestic security, national security, and counterintelligence operations against North Korea.[2] Despite widely-reported reform efforts, the agency continues to face criticism for reported and perceived abuses of its power and mandate.[3]

Recent Scrutiny of NIS

The NIS has been scrutinized for misuse of its powers in a number of cases, which have been revisited in media coverage of the Hacking Team leaks.

In February 2015, a former NIS director was sentenced to three years in prison for ordering NIS agents to attempt to influence the 2012 presidential elections by posting negative comments about President Park Geun-hye's rivals.[4] Some of the 1.2 million comments that prosecutors say NIS agents posted accused President Park's rivals of being pro-North Korean sympathizers.[5] NIS denied interfering in the election, claiming that the agency's online activities were solely directed at North Korea.[6] Recently, the Supreme Court ordered a retrial in the case, as some evidence used to convict the former director was ruled inadmissible.[7] Additionally, in 2005, a former deputy chief of NIS was arrested for illegal wiretapping. The prosecutor in the case stated that the deputy chief may have attempted to destroy evidence in the case before his arrest.[8]

Previous Citizen Lab Report

In February 2014, Citizen Lab released a report entitled "Mapping Hacking Team's 'Untraceable' Spyware," which identified 21 suspected government users of Hacking Team's RCS spyware, including South Korea.[9] The report triggered limited media coverage in South Korea at the time.[10]

Current Scandal

On July 6, 2015, it became clear that Hacking Team had suffered a substantial compromise of its internal systems.[11] Shortly thereafter, much of Hacking Team's code, data, and communications were leaked into the public domain. The material not only confirmed that South Korea was a customer of Hacking Team, but exposed substantial commercial interactions between Hacking Team and the "5163 Army Division," whose mailing address matches that of the NIS,[12] and is reported to be a codename of the NIS.[13]

Shortly after this revelation, an employee of the NIS reportedly committed suicide. A note claimed he had deleted information regarding the NIS's use of Hacking Team RCS,[14] triggering nationwide interest in who the NIS was targeting.[15] Lawmakers said that, in a closed-door meeting, the NIS admitted to purchasing Hacking Team spyware.[16] A lawmaker in the Intelligence Committee of the National Assembly of the Republic of Korea disclosed that the NIS testified to the Committee that it had used Hacking Team spyware more than 200 times for counterespionage, and to track the North Korean arms trade.[17]

The NIS Purchases Hacking Team

According to the leaked files, a South Korean company called Nanatech introduced itself to Hacking Team in August 2010, claiming that it provided *"support"* in relation to *"telecommunication equipments to domestic companies."*[18] Nanatech was purportedly attempting to acquire solutions to monitor Skype on behalf of its customer,[19] and noted that the customer was also interested in *"monitoring the voice conversation on the mobile phone."*[20] Nanatech stated that Hacking Team competitor Gamma Group, developer of FinFisher, was also dealing with its customer through another reseller.[21]

Notably, it appears that Nanatech never informed Hacking Team that its customer was NIS. In November 2010, Nanatech responded to Hacking Team queries pressing for more information on its customer[22] with "*About end-user: Our client is the research team of Army (named KINSTEL). I think you don't have to worry about it*," which appeared to satisfy Hacking Team.[23] Renewed exchanges in June 2011 also indicated the "*army*" as end user.[24] In proceeding with the purchase, Nanatech specifically identified its customer to Hacking Team in November 2011 as the "5163 Army Division."[25] The mailing address that Nanatech provided for the Division matches that of the NIS,[26] and "5163 Army Division" is reported to be a codename of the NIS.[27] This obfuscation of customer identity raises significant questions regarding corporate due diligence and overall transparency in identifying end users of the spyware. Indeed, end user verification is often required by export licensing regimes.

In subsequent emails[28] and in its customer list,[29] Hacking Team also variously referred to the customer as "South Korea Army," "SKA," or "The Army South Korea."

Nanatech organized a visit for two representatives from the customer, Sunny Han and Se-Hun Lee, and one person from Nanatech,[30] to Hacking Team's offices in Milan on 21-22 November 2011.[31] Nanatech mentioned that they had managed to

outmaneuver the competition, and arranged for the customer to meet with Hacking Team before any meeting with competitors Gamma International and Trovicor.[32] After the meeting in Milan, Nanatech expressed that the customer wanted to rush to purchase Hacking Team's RCS, claiming that they needed to spend their budget by 20 December 2011.[33]

After some back and forth, Nanatech's customer accepted offer #NA111214Q1.[34] (See Figure 1 below.) The offer included the ability to monitor a total of 10 targets simultaneously on Windows, Symbian, Blackberry, iPhone, and Android platforms. It also included the Remote Mobile Infection/Installation (RMI) feature, and one year of zero-day exploits and maintenance. RMI apparently involves sending WAP push messages (SI and SL) through a GSM modem to mobile devices.[35] Depending on phone settings, such messages can automatically open a browser window or attempt to install an application, and can appear to be from the user's mobile phone operator. The total cost was €390,000.

Date : Dec, 14, 2011
Offer No.: NA111214Q1

Currency : EUR

Item	Description	Q'ty	Price(€)
Remote Control System	RCS Infrastructure		€ 136,000.00
	Front - End SW License	1	
	Back End SW License	1	
	Operators Console		€ 16,000.00
	Admin	1	
	Tech	1	
	Log Viewer License	3	
	Target	10	€ 56,000.00
	Platform		
	Windows (32 &64 bit)		€ 19,200.00
	Symbian		€ 19,200.00
	Windows Blackberry		€ 19,200.00
	i-Phone		€ 19,200.00
	Android		€ 19,200.00
	Anonymizer SW License	2	€ 24,000.00
	Alerting Module	Yes	Included
	Remote Mobile Installation	Yes	€ 40,000.00
	1 Year Exploit Portal Subscription (zero day level)		€ 32,000.00
	RCS Training Sessions	Yes	Included
	1st Year Maintenance		Included
		TOTAL	€ 400,000.00
		Special Discount	€ 10,000.00
		Final Total	€ 390,000.00

Figure 1: Nanatech Offer #NA111214Q1.[36]

A letter of credit (#M03QY112GS0014) was issued for this offer,[37] with delivery to be made to the "5163 site." (See Figure 2 below.)

DOCUMENTARY CREDIT NUMBER 20 : M03QY112GS00114

DATE OF ISSUE 31C: 2011-12-14

APPLICABLE RULES 40E: UCP LATEST VERSION

*Date *Place

DATE AND PLACE OF EXPIRY 31D: 2012-03-08 IN THE BENEFICIARY COUNTRY

APPLICANT 50 : THE 5163 ARMY DIVISION.
THE GOVERNMENT OF THE R.O.K.,SEOCHO
P.O.BOX 200 SEOUL, KOREA
(FAX NO.:82-02-2187-0333)

BENEFICIARY 59 : HACKINGTEAM, VIA DELLA MOSCOVA,
13-20121 MILANO, ITALY
(T): +39.02.2906.0803
(F): 439.02.6311.8946

*Currency *Amount

CURRENCY CODE AMOUNT 32B: EUR 390,000.00

DESCP OF GOODS AND/OR SERVICES 45A:
+COMMODITY DESCRIPTION :
-DETAILS AS PER OFFER NO.NA111214Q1,
DATED: 14.DEC.2011 ISSUED BY HT(NANATECH, LTD).
+TOTAL EUR 390,000.00
+PRICE TERMS : DAP ''5163 SITE''
+COUNTRY OF ORIGIN : ITALY

Figure 2: Excerpts from Letter of Credit issued for Offer #NA111214Q1.[38]

Delivery was completed and accepted by the "5163 Army Division."[39] (See Figure 3 below.) The license agreement for Hacking Team's RCS spyware was signed by Sunny Han.[40] (See Figure 4 below.)

The 5163 Army Divisions
Seoul, Korea

Certificate of Acceptance

This is to certify that the delivery has been completed as stipulated in the Contract.

HackingTeam / NANATECH

(CONTRACT NO: FOST-11-1206)
(L/C NO : M03QY112GS00114)

The 5163 Army Div.,
The Government of R.O.K.

Figure 3: Certificate of Acceptance in relation to Letter of Credit #M03QY112GS0014 from the "5163 Army Division."[41]

[THE 5163 DIVISION], an **[ARMY]**, with registered office in **[SEOUL]**, **[SEOCHO P.O BOX 200]**, registered before **[THE GOVERNMENT OF THE R.O.K]**, Fiscal Code and VAT n. **[137-600]**, hereby represented by **[SUNNY HAN]**, in his quality of **[TEAM LEADER]** of the company (hereafter "**User**").

[The 5163 army division]

Sunny Han

Figure 4: Excerpts from License Agreement between Hacking Team and the "5163 Army Division."[42]

The Korean customer purchased 10 additional target licenses in August 2012, for €57,600, allowing them to monitor a total of 20 targets simultaneously.[43]

On 6 December 2012, the Korean customer expressed interested in purchasing an additional 30 target licenses, which would have allowed it to monitor 50 targets at once.[44] The purchase was apparently never completed, and it appears that no further target license purchases were initiated.

Targets in South Korea?

The data available in the leaked Hacking Team files provides circumstantial evidence pointing to an interest in compromising individuals with ties to South Korea (i.e., Korean language speakers who use software or apps popular in South Korea, or South Korean editions of Samsung phones). However, the leaked data does not identify the targets, or conclusively show whether these targets were inside or outside Korea.

Interest in Targeting South Korean-Edition Phones

The customer communicated with Hacking Team via the email accounts devilangel1004@gmail.com[45] ("devilangel") and smiolean@gmail.com.[46] Devilangel filed several support tickets[47,48,49,50] in August and September 2012 asking for support for call recording on "SHW-M series" (South Korean edition) Samsung phones, as well as, in one case, on "Galaxy S3 Chinese models." Nanatech also contacted Hacking Team to ask for voice recording support for South Korean edition Galaxy 3 phones.[51] In January 2013, Nanatech sent a South Korean edition Galaxy S3 to Hacking Team[52] to help them support call recording.[53] An August 2013 e-mail requests that Hacking Team test their Android exploit against South Korean edition phones.[54]

Interest in Targeting South Korean Software (KakaoTalk and AhnLab Anti-Virus)

Devilangel requested that Hacking Team test their solution against the latest version of South Korean company AhnLab's antivirus program,[5] as well as popular Chinese anti-virus programs, mentioning that they have "some targets in China."[56]

According to a trip report filed by a Hacking Team employee who visited the Korean customer on 24 March 2014, the customer *"asked about the progress of Kakao Talk which they mentioned is very commonly used in their country."*[57] One of the "*key takeaways*" of the report was that *"Kakao Talk is something which SKA is emphasising."* The customer also requested support for voice and message recording on the PC versions of KakaoTalk and LINE (a chat application similar to KakaoTalk developed by LINE Corporation, a Japan-based company).[58]

KakaoTalk is a chat program developed and owned by the South Korea-based company Daum-Kakao. A May 2015 article notes that KakaoTalk is the most popular chat application used in South Korea and has 35 million users in the country, representing 70% of South Korea's population of 50 million.[59]

KakaoTalk has previously been the target of government pressure. In 2014, President Park Geun-hye announced a crackdown on the spread of rumors online following criticism of how her administration handled the capsize of a South Korean ferry. As part of this crackdown, a South Korean student and an opposition politician involved in discussions and protests around the ferry incident were notified that law enforcement officials were given access to data from their KakaoTalk accounts.[60]

Interest in Deploying Spyware via OTA Updates and Wireless Networks

Nanatech also twice inquired about "*over the air*"[61] and Wi-Fi infections, mentioning they wanted to "*remotely and forcibly 'push'*" the spyware "*in a stealth manner onto the target's device without his knowledge or cooperation.*"[62] The Korean customer expressed interest in Hacking Team's TNI (Tactical Network Injector),[63] a laptop that "provides everything needed in order to crack a WiFi network, join it, identify the interested target and deploy the RCS Agent."[64] The TNI can also create rogue WiFi networks, and can even work with wired networks given special infrastructure access. The Korean customer tested the TNI from April[65] until July 2014, but ultimately decided not to purchase the TNI, citing issues including lack of reliable support for mobile phones.[66]

Use of Korean Bait Content

We identified several instances of the Korean customer using Korean language or Korea-themed bait content:

- We observed a drive-by-download attack in 2014 that used a bait content file called “free korean movies.” (see: **Attribution of “Drive-by-Download” Samples** below)
- In the leaked files, we found bait content including a file containing the names and phone numbers of Seoul University alumni in Southern California,[67] and a file containing information pertaining to the sinking of the ROKS Cheonan,[68,69] (and a Computer Science presentation about Machine Learning).[70,71]
- One bait content link[72,73,74] contained a picture showing the schedule for the 2015 Geumcheon Harmony Cherry Blossom Festival in Seoul, while another one contained a link to a blog about reviews of rice cake dishes at Korean restaurants.[75,76,77,78]
- One bait content link contained a link to a Google app on the Google Play Store called “Google Korean Input.”[79,80]

Attribution of “Drive-by-Download” Samples

The leaked Hacking Team e-mails allowed us the opportunity to attribute several samples of Hacking Team RCS spyware that we previously observed:

```
SHA256: cbde6a113a54b8dcf122d9d879b7c21c8b03a89d792f49210bbe41e8466d121a
URL: http://free.dramakorea.asia/s/free_korean_movies.exe
```

The command and control (C&C) server used in the sample is **hulahope.mooo.com**, which matches the C&C for numerous Android samples submitted by devilangel to Hacking Team for preparation of exploits. This sample was submitted to VirusTotal on 21 July 2014, and was submitted eight additional times to VirusTotal in the following month, including twice from Korea.[81] This sample appears to have been served through a drive-by-download strategy, involving a file “x.js:”

```
SHA256: 8793d6eda87163b04a3db9251ff89b7c8a66500a4ed475c7026b5fc9a4c8abe9
```

On its own, the script causes an Internet Explorer user to see a popup asking them to authorize an ActiveX control. If the control is authorized, then the spyware is downloaded and executed.

We also found the following sample:

```
SHA256: 21e8d495bca60edc3b64ac970f9a9fa896d0eadc6491452ea937d64849b1f4a0
URL: http://shrook.mooo.com/cn/notify.exe
```

The sample was submitted to VirusTotal once on September 12, 2014,[82] and was apparently served by the same drive-by-download javascript method. The C&C server is also **hulahope.mooo.com**.

Analysis of Bait Content

According to the leaked documents, Hacking Team provides an exploit service to customers that requires that the customers transmit them basic information, including a bait document or link, and their monitoring agent.[83] Depending on the type of request, Hacking Team then modifies the bait document to include an exploit to install the agent, or creates a URL that, when clicked, exploits the target’s web browser to install the agent. The exploits and agents are hosted on servers belonging to Hacking Team. Hacking Team sends the bait documents back to the customer, who can then send the booby-trapped bait document to targets to infect them.[84] The leaked Hacking Team documents contain numerous customer requests to create exploit documents or links, often with bait content attached. In some cases, these bait documents or links speak to the interests, or identity, of potential targets.

Devilangel expressed concern about having to furnish Hacking Team with bait content used to infect victims, as the information *“can be related with my target.”*[85] Hacking Team responded that they do not *“retain any information about the files the customers send us”* (note, however, we were able to identify many files sent by devilangel for infection) and suggested that devilangel choose a document *“containing not so sensitive data.”*[86] Given devilangel’s concerns and Hacking Team’s advice, bait documents may have been chosen to minimize the link between the bait content and the target.

Devilangel’s exploit requests also sometimes included a statement as to whether the exploit would be used for “testing” or “real targets.” Below, we provide an overview of some common themes associated with the bait content and bait links submitted by

devilangel to Hacking Team. We exclude any marked “testing:”

- We describe Korean-themed bait content above (see: **Use of Korean Bait Content**).
- Some of the bait content includes generic holiday greetings. For example, “Happy New Year” messages, or Christmas greetings

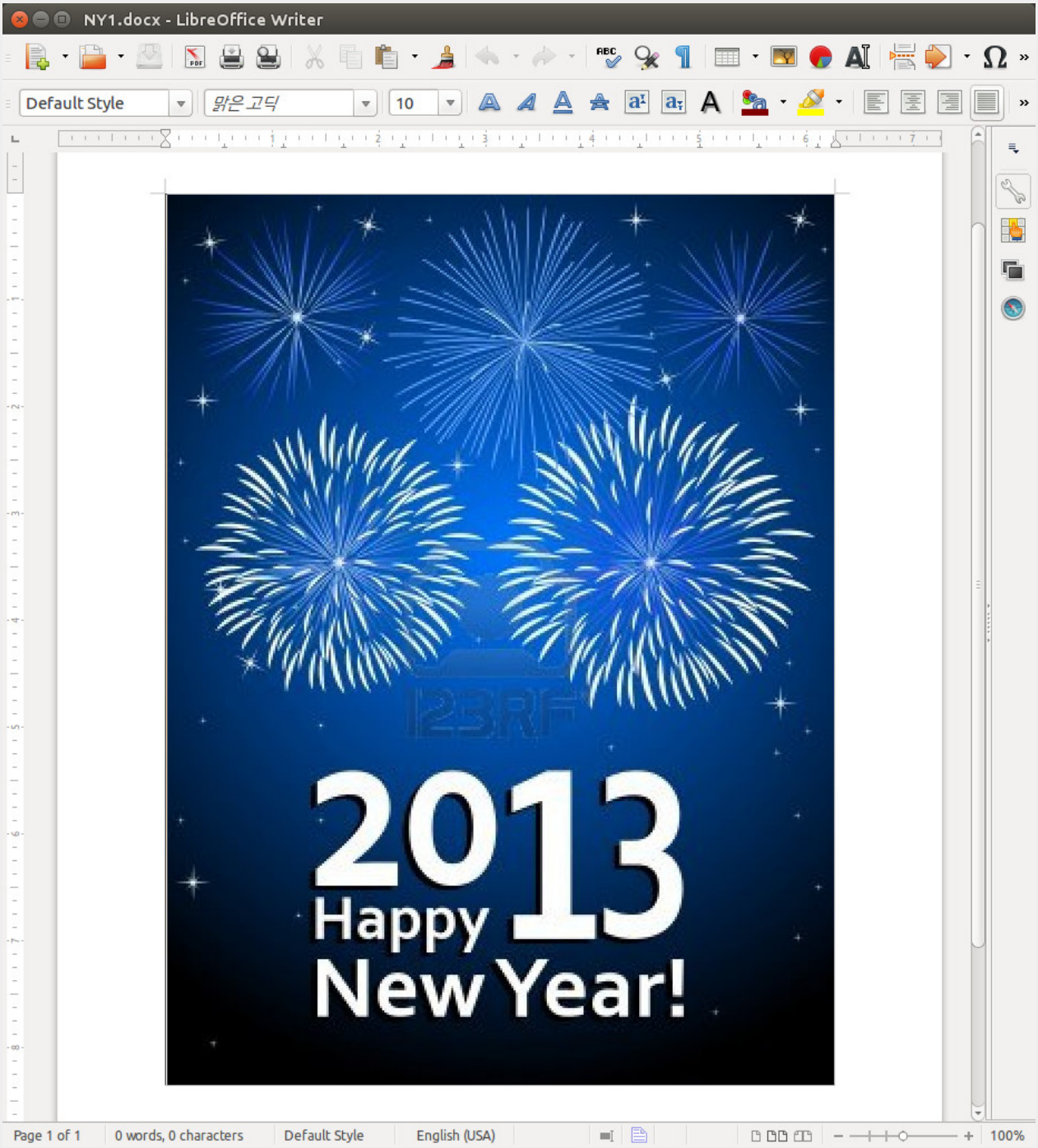

Figure 5: A “Happy New Year!” bait document submitted by devilangel to create an exploit document.[87]

Figure 6: A "Christmas Blessing" e-card submitted by devilangel to create an exploit link.[88]

- A number of pieces of bait content included medical themes, including a PowerPoint presentation about a Belfast cancer conference, and links about MERS[89] and Avian Flu.[90]

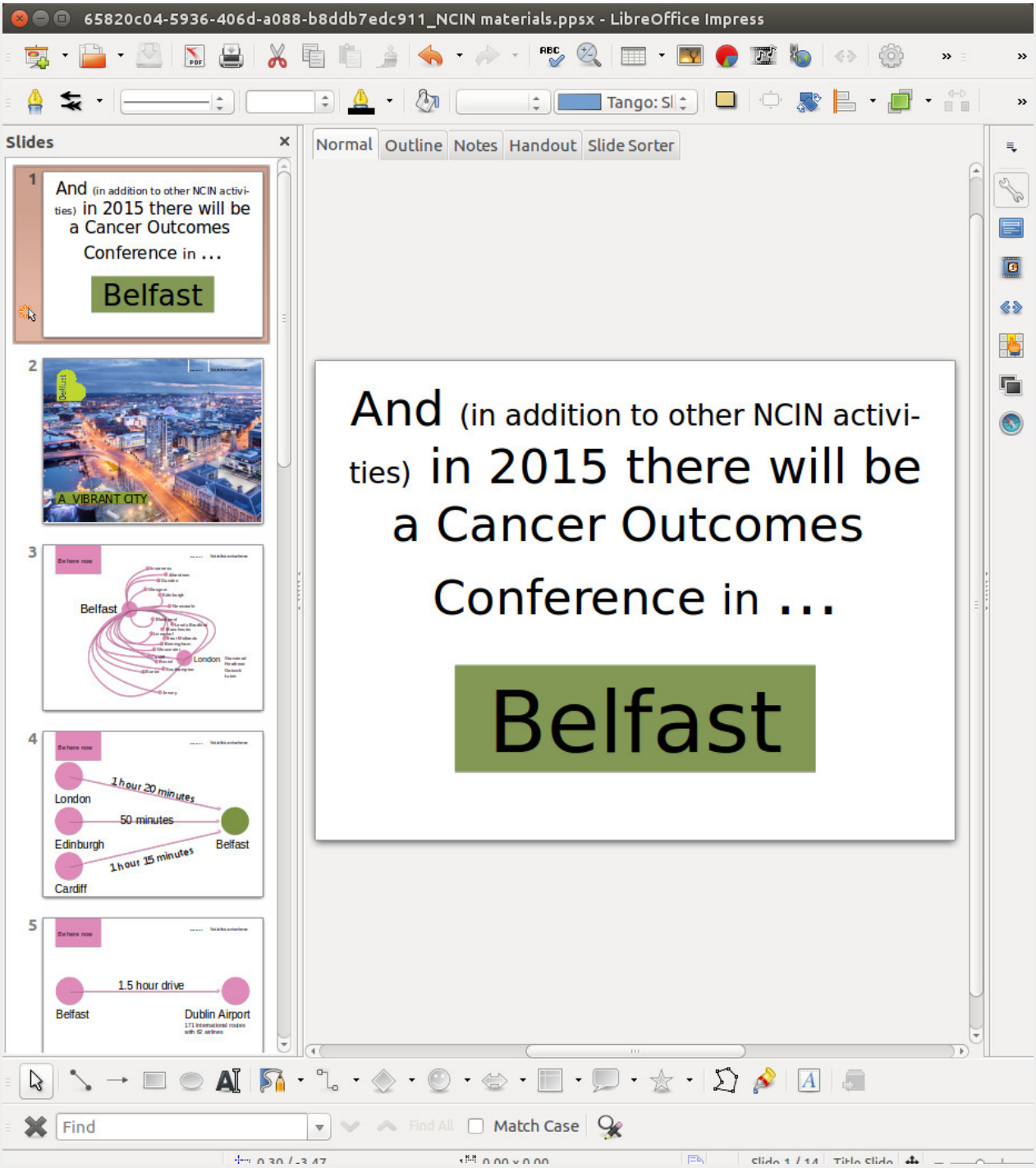

Figure 7: A bait document about the 2015 National Cancer Intelligence Network (NCIN) Cancer Outcomes Conference submitted by devilangel to create an exploit document.[91]

- Some bait content included tips for protecting online privacy, including one PowerPoint presentation called “Save you Privacy” and a Word document called “How to Access and Clear Your iPhone’s Web Browsing History.”

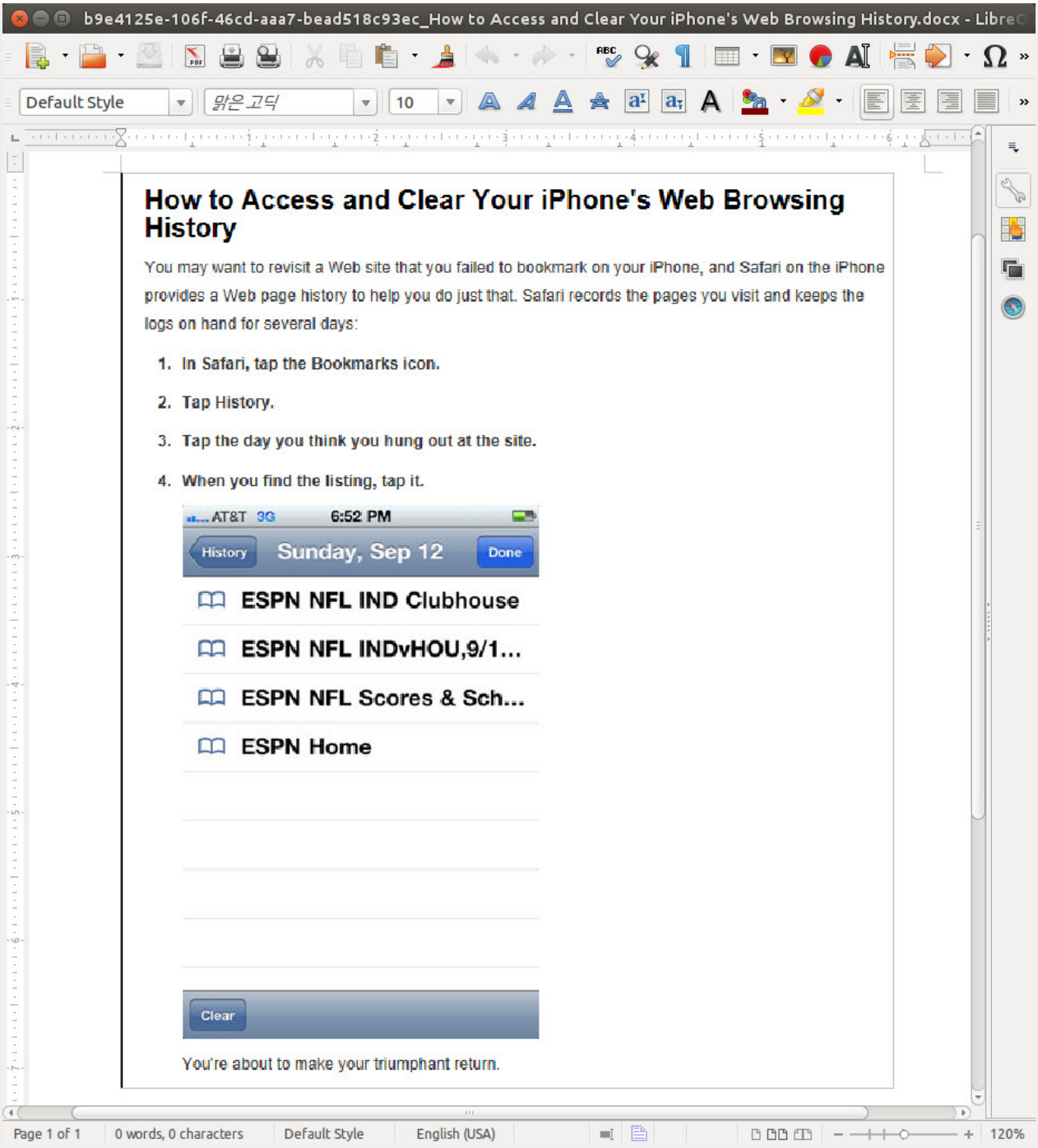

Figure 8: A bait document containing information about iPhone browsing history submitted by devilangel to create an exploit document.[92]

- Some bait links involved Asian pornography, including a website featuring "only Chinese porn,"[93] a page on a pornography website featuring a search for the term "chinese,"[94] and a website called "Asian Porn Tube."[95,96]

Exploit server Logs

The leaked Hacking Team data contains files "Exploit_Delivery_Network_android.tar.gz," and "Exploit_Delivery_Network_windows.tar.gz," which appear to contain detailed information about each exploit link or document generated by Hacking Team upon customer request (for May and June 2015), as well as details of which IP addresses clicked on each link (or opened each document), whether the exploitation was successful or not, which website directed each visitor to the exploit (if applicable), as well as the language and model of the phone (in some cases of Android exploits). The log information is in "var/www/files/[ID]/log.jsonl," where "[ID]" is the six character alphanumeric ID assigned to the exploit by Hacking Team.

We present details on all clicks on Android exploit links below (we did not identify any Windows exploits requested by Hacking Team during this period). Hacking Team's Android exploit involved a link sent to the target's phone. If the target opened the link in the

built-in Android web browser app, then the exploit may have installed Hacking Team's RCS on their phone. Importantly, the list below excludes individuals who did not click on the link (as Hacking Team cannot record logs in this case):

ID	Time[97]	IP	Country	Phone	Locale	Referer URL	Hit?[98]
BBltjx[99]	6/29/2015 13:01:49	212.5.158.22	BG	NX403A	en-US		No
BBltjx	6/29/2015 13:02:16	212.5.158.70	BG	NX403A	en-US		No
bO47cc[100]	6/22/2015 11:24:22	93.84.2.181	BY	SM-A500F			No
BR2u9z[101]	6/22/2015 10:50:03	109.188.125.17	RU	SM-G800H			No
8CS48M[102]	6/18/2015 10:32:23	92.230.140.206	DE	GT-I9103	ko-KR		No
v9K0GQ[103]	6/18/2015 10:45:13	213.87.129.241	RU	GT-I8190	ru-RU		**Yes**
jAWxkt[104]	6/26/2015 01:33:51	220.181.132.217	CN	G700-U00	zh-CN	http://video.sexyhub.co/x/?rd=SjLzM2	No
zuggfM[105]	6/17/2015 11:23:43	49.230.231.158	TH	SM-G900F			No
zuggfM	6/17/2015 11:28:25	49.230.225.3	TH	SM-N910C			No
zuggfM	6/17/2015 15:37:27	139.193.176.58	ID	S5E	en-US		No
zEsa9i[106]	6/17/2015 10:55:09	111.80.143.117	TW	SM-G900I			No
vYLpBl[107]	6/18/2015 03:34:39	175.168.46.204	CN	SAMSUNG-SM-N9008V_TD	zh-CN		No
8n3gio[108]	6/12/2015 12:01:41	114.124.0.237	ID	GT-S7270			No
7ZSBlX[109]	6/4/2015 06:32:58	223.62.169.2	KR	SHV-E250S	ko-KR	http://dns.cdc-asia.org/docs/7ZSBlX/fwd	**Yes**
9hN2Zn[110]	6/1/2015 9:07:03	41.210.154.105	UG	GT-I9100	ko-KR		No
9hN2Zn	6/1/2015 9:14:43	41.210.154.13	UG	SM-N900			No
uPz4mj[111]	6/17/2015 10:46:17	223.62.212.18	KR	GT-N7100	en-PH	http://link.sexyhub.co/docs/uPz4mj/fwd	**Yes**

South Korean Targets?

The data shows that there were two successful Android exploitations of phones with Korean IP addresses: one SK Telecom edition Galaxy Note 2 with SK Telecom IP address and Korean-Korea locale, one international Galaxy Note 2 with SK Telecom IP address and English-Phillippines locale. There was only one other successful exploit in May and June 2015: a Galaxy S3 Mini with a Russian IP address and Russian-Russia locale.

One individual with a Ugandan IP address, and one individual with a German IP address, clicked on the link with their locale set to "Korean-Korea."

Command and Control and Exploit Infrastructure

Using referrer URLs in the exploit server logs, as well as domain names and IP addresses found in the Korean customer's malware samples, we were able to characterize their Hacking Team infrastructure.

We start from the domain name **dns.cdc-asia.org**, used in a referrer URL seen in the exploit logs. We assume that the Korean customer controlled **dns.cdc-asia.org**, because this URL referred to the exploit requested from Hacking Team, and was not sent to them by Hacking Team. We further assume that the customer controlled the domain name **cdc-asia.org**, as the registration date of the domain (June 3, 2015) matches the date that devilangel requested the exploit[112] that was clicked on with referring domain **dns.cdc-asia.org**.

We found the following registrant information for **cdc-asia.org**:

```
Registrant Name:krystal Freeman
Registrant Organization:Co
Registrant Street: 136 Driftwood Road
Registrant City:CA
Registrant State/Province:CA
Registrant Postal Code:95129
Registrant Country:US
Registrant Phone:+1.14083799445
Registrant Email:insomnia214@outlook.com
Name Server:NS4.ITITCH.COM
Name Server:NS3.ITITCH.COM
Name Server:NS2.ITITCH.COM
Name Server:NS1.ITITCH.COM
```

The name server suggests that the domain was registered with ititch.com, a service for purchasing domain names and web hosting using Bitcoin.

We found two other domains registered with the same registrant email:

mytelkomsel.co
telegram-apps.org

We plugged these domains, as well as **cdc-asia.org**, into PassiveTotal[113] in order to identify other domains using the same IP address. PassiveTotal is an infrastructure analysis tool designed for security research. We found that **cdc-asia.org** resolved to 180.235.132.45, and two other websites resolved to this same address: **droidlatestnews.com**, and **enjoyyourandroid.com**.

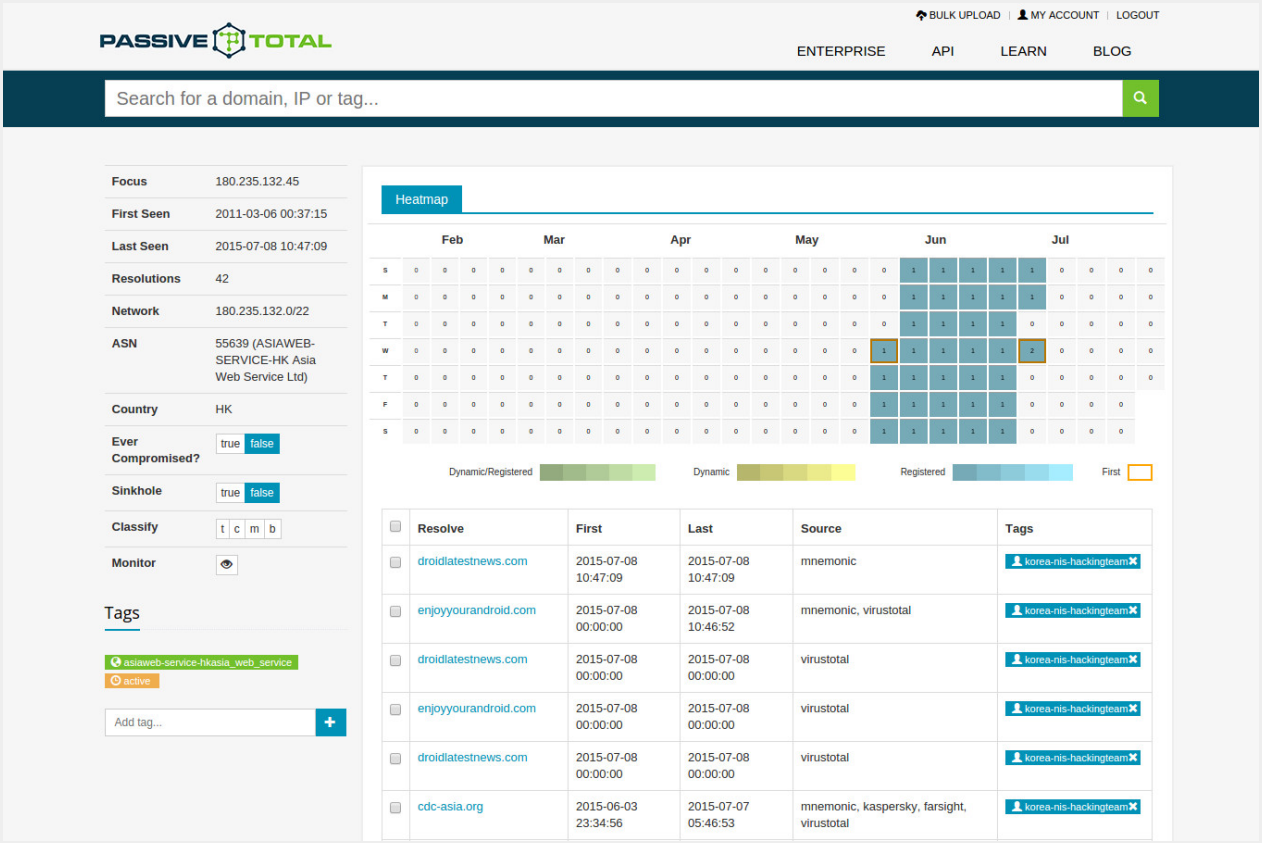

Figure 9: Excerpt of PassiveTotal results for 180.235.132.45.

The initial registrant information for both domains was as follows:

```
Registrant Name: Leonard Freeman
Registrant Organization: N/A
Registrant Street: 1203 Grove Street
Registrant City: Bethpage
Registrant State/Province: New York
Registrant Postal Code: 11714
Registrant Country: US
Registrant Phone: +1.4194763271
Registrant Email: mappingmechanism@hotmail.com
Name Server: domains4bitcoins.earth.orderbox-dns.com
Name Server: domains4bitcoins.mars.orderbox-dns.com
Name Server: domains4bitcoins.mercury.orderbox-dns.com
Name Server: domains4bitcoins.venus.orderbox-dns.com
```

The name server suggests that the domain was registered with domains4bitcoins.com, a service for purchasing domain names and web hosting using Bitcoin.

Note that the registrant name, “Leonard Freeman,” uses the same surname, “Freeman,” as the registrant for the previous three domains “Krystal Freeman.” The registrant email address for both domains was updated after July 8, 2015 (after the Hacking Team leak) to the following:

```
Registrant Name: Alexis
Registrant Organization: N/A
Registrant Street: 4403
Registrant City: Los Angeles
Registrant State/Province: California
Registrant Postal Code: 90017
Registrant Country: US
Registrant Phone: +1.9174849999
Registrant Email: prmgrabzi@hotmail.com
```

We plugged **droidlatestnews.com** and **enjoyyourandroid.com** into PassiveTotal, and found that these resolved to 95.215.46.224. We found several other domains that resolved to this IP address:

```
bijiaexhibition.com
samsung-update.net
getnewandroid.com
secure.anyurl.org
update.indoorapps.com
```

We also checked registrant email addresses and phone numbers to find additional domains:

```
facebook-update.info
samsung-update.net
play-mob.org
```

It is noteworthy that **play-mob.org** was registered on 8 April 2015, a day after devilangel requested Android exploits redirecting to “play.mob.org”.[114] We provide a list of suspected domain names linked to the Korean customer below, including the domain names above, as well as domain names from RCS samples submitted by devilangel to Hacking Team, and RCS samples detected by Hacking Team on VirusTotal and attributed to the same customer:

```
cdc-asia.org
mytelkomsel.co
telegram-apps.org
bijiaexhibition.com
samsung-update.net
getnewandroid.com
facebook-update.info
samsung-update.net
play-mob.org
boardingpasstohome.com[115]
mywealthpop.com[116]
secure.anyurl.org
update.indoorapps.com
```

```
video.sexyhub.co
link.sexyhub.co
shrook.mooo.com
free.dramakorea.asia
nkpro.lalanews.net[117]
androidgplay.us.to[118]
hulahope.mooo.com
publiczone.now.im[119]
reflect.dalnet.ca[120]
pantheon.tobban.com[121]
```

The domain names above were associated with the following e-mail addresses:

```
checkonetwothree@hotmail.com
mappingmechanism@hotmail.com
watermelonholicq@eclipso.email
insomnia214@outlook.com
prmgrabzi@hotmail.com
```

We also identified the following IP addresses associated with the Korean customer's infrastructure:

```
131.72.137.10
198.105.125.107
198.105.125.108
131.72.137.11
198.105.122.117
185.7.35.79
131.72.137.104
131.72.137.101
95.215.46.224
180.235.132.45
103.13.228.240
185.10.57.150
46.19.143.244
37.46.114.43
5.199.166.180
```

It also appeared that the Korean customer's exploits were served from the following IP addresses, which may belong to Hacking Team, and thus have also been used to serve exploits for other Hacking Team customers:

```
46.38.63.194
188.166.5.201
46.38.63.112
46.251.239.150
212.117.180.108
```

In our 2014 report, "Mapping Hacking Team's 'Untraceable' Spyware," we identified the following IP addresses associated with the South Korean customer:

```
211.51.14.129
101.99.83.12
5.255.87.146
198.144.178.104
198.144.178.118
204.188.221.198
185.7.35.79
185.7.35.80
64.32.12.75
124.217.245.64
185.29.8.202
```

Conclusion and Further Investigation

We have outlined circumstantial evidence indicating that NIS was interested in targets with links to South Korea, and in two cases infected devices belonging to “real targets” inside South Korea.

The leaked data alone cannot identify specific targets. Thus, we presented some technical data regarding the NIS’s Hacking Team RCS command and control infrastructure, which may be useful in further investigation.

We briefly outline some promising avenues for further investigation:

- First, obtaining DNS logs over the past year associated with the domains publiczone.now.im and hulahope.mooo.com would be very helpful, as this would reveal IP addresses of infected devices.
- Second, organizations or institutions that run Intrusion Detection Systems should check their logs for hits on the IP addresses and domain names provided herein.
- Third, groups focused on testing should scan the e-mail accounts of potential targets, as well as their SMS message logs, WAP push message logs, and logs of any other mobile messaging apps, for any e-mails or messages containing the domain names we identified (or any links, such as Tinyurl links, that unshorten to these domains), and any attachments matching Hacking Team’s exploits or spyware.
- Finally, if NIS initiated their Bitcoin domain name purchases from a single address, it may be possible to trace NIS’s Bitcoin address by searching the Blockchain using the registration times associated with the domains. Tracing NIS’s Bitcoin address could illuminate further elements associated with their C&C architecture.

Footnotes

[1] http://eng.nis.go.kr/svc/history.do?method=content&cmid=11915

[2] http://www.economist.com/blogs/banyan/2014/03/south-korean-intelligence

[3] http://www.economist.com/blogs/banyan/2014/03/south-korean-intelligence

[4] http://www.bbc.com/news/world-asia-31284704

[5] http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html

[6] http://www.nytimes.com/2013/05/01/world/asia/prosecutors-raid-south-korean-spy-agency.html

[7] http://www.reuters.com/article/2015/07/16/southkorea-spychief-retrial-idINKCN0PQ0LJ20150716

[8] http://web.international.ucla.edu/asia/article/31102

[9] https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

[10] http://www.ohmynews.com/NWS_Web/view/at_pg.aspx?CNTN_CD=A0001970476

[11] http://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/

[12] See “서울 서초우체국 사서함 200호” on http://www.nis.go.kr/svc/community.do?method=content&cmid=11477, which matches “Seocho P.O Box 200, Seocho-dong, Seocho-gu, Seoul, Korea” on https://wikileaks.org/hackingteam/emails/emailid/441251.

[13] http://english.hani.co.kr/arti/english_edition/e_national/700356.html

[14] http://english.yonhapnews.co.kr/national/2015/07/19/43/0302000000AEN20150719001152315F.html

[15] http://www.nytimes.com/2015/07/20/world/asia/in-suicide-note-south-korea-hacking-expert-denies-domestic-spying.html?_r=0

[16] http://bigstory.ap.org/article/acd838d482254df9b7e401607bfce9a0/south-korean-spy-agency-explored-technology-hack-chat-app

[17] http://english.yonhapnews.co.kr/news/2015/08/04/0200000000AEN20150804000900315.html

[18] https://wikileaks.org/hackingteam/emails/emailid/441228

[19] https://wikileaks.org/hackingteam/emails/emailid/441228

[20] https://wikileaks.org/hackingteam/emails/emailid/440571

[21] https://wikileaks.org/hackingteam/emails/emailid/441056

[22] https://wikileaks.org/hackingteam/emails/emailid/440827

[23] https://wikileaks.org/hackingteam/emails/emailid/441309

[24] https://wikileaks.org/hackingteam/emails/emailid/440989

[25] https://wikileaks.org/hackingteam/emails/emailid/441105

[26] See “서울 서초우체국 사서함 200호” on http://www.nis.go.kr/svc/community.do?method=content&cmid=11477, which matches “Seocho P.O Box 200, Seocho-dong, Seocho-gu, Seoul, Korea” on https://wikileaks.org/hackingteam/emails/emailid/441251.

[13] http://english.hani.co.kr/arti/english_edition/e_national/700356.html

[27] http://english.hani.co.kr/arti/english_edition/e_national/700356.html

[28] See, e.g., https://wikileaks.org/hackingteam/emails/emailid/16742; https://wikileaks.org/hackingteam/emails/emailid/608816; https://wikileaks.org/hackingteam/emails/emailid/585101; https://wikileaks.org/hackingteam/emails/emailid/42977

[29] https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/6%20-%20Offensiva/Client%20List_Renewal%20date.xlsx

[30] https://wikileaks.org/hackingteam/emails/emailid/441306

[31] https://wikileaks.org/hackingteam/emails/emailid/441293

[32] https://wikileaks.org/hackingteam/emails/emailid/440837

[33] https://wikileaks.org/hackingteam/emails/emailid/441269

[34] https://wikileaks.org/hackingteam/emails/emailid/440822

[35] https://wikileaks.org/hackingteam/emails/emailid/437543

[36] Source: “Price_1214-1[1].pdf” extracted from “Price_1214-1[1].zip” in e-mail: https://wikileaks.org/hackingteam/emails/emailid/440822. The attachment is unavailable on WikiLeaks. The password to extract the .zip file is “ejopenit” (without quotes).

[37] https://wikileaks.org/hackingteam/emails/emailid/441001

[38] Source: “LC.pdf” extracted from “LC.zip” in e-mail: https://wikileaks.org/hackingteam/emails/emailid/441001. The attachment is unavailable on WikiLeaks. The password to extract the .zip file is “ejopenit” (without quotes).

[39] https://wikileaks.org/hackingteam/emails/emailid/441207

[40] https://wikileaks.org/hackingteam/emails/emailid/441001

[41] Source: “certificate of acceptance.pdf” extracted from “certificate of acceptance.zip” in e-mail https://wikileaks.org/hackingteam/emails/emailid/441207. The attachment is unavailable on WikiLeaks. The password to extract the .zip file is “ejopenit” (without quotes).

[42] Source: “software license agreement.pdf” extracted from “software license agreement.zip” in e-mail https://wikileaks.org/hackingteam/emails/emailid/441001. The attachment is unavailable on WikiLeaks. The password to extract the .zip file is “ejopenit” (without quotes).

[43] https://wikileaks.org/hackingteam/emails/emailid/440599

[44] https://wikileaks.org/hackingteam/emails/emailid/441209

[45] https://wikileaks.org/hackingteam/emails/emailid/808281

[46] See “My googletalk id for communication is smiolean” in https://wikileaks.org/hackingteam/emails/emailid/715100.

[47] https://wikileaks.org/hackingteam/emails/emailid/790170

[48] https://wikileaks.org/hackingteam/emails/emailid/797052

[49] https://wikileaks.org/hackingteam/emails/emailid/781892

[50] https://wikileaks.org/hackingteam/emails/emailid/782084

[51] https://wikileaks.org/hackingteam/emails/emailid/441239

[52] https://wikileaks.org/hackingteam/emails/emailid/440900

[53] https://wikileaks.org/hackingteam/emails/emailid/673756

[54] https://wikileaks.org/hackingteam/emails/emailid/353110

[55] https://wikileaks.org/hackingteam/emails/emailid/702485

[56] https://wikileaks.org/hackingteam/emails/emailid/73106

[57] https://wikileaks.org/hackingteam/emails/emailid/16742

[58] https://wikileaks.org/hackingteam/emails/emailid/75661

[59] http://www.forbes.com/sites/kathleenchaykowski/2015/05/28/creator-of-messaging-app-kakaotalk-acquires-social-network-path/

[60] http://bigstory.ap.org/article/97c92b056482488abd990db9a4acb388/s-korea-rumor-crackdown-jolts-social-media-users

[61] https://wikileaks.org/hackingteam/emails/emailid/441040

[62] https://wikileaks.org/hackingteam/emails/emailid/440923

[63] https://wikileaks.org/hackingteam/emails/emailid/17076

[64] Source: “TNI Datasheet.docx” in e-mail https://wikileaks.org/hackingteam/emails/emailid/511703.

[65] https://wikileaks.org/hackingteam/emails/emailid/728653

[66] https://wikileaks.org/hackingteam/emails/emailid/18952

[67] https://wikileaks.org/hackingteam/emails/emailid/361888

[68] https://wikileaks.org/hackingteam/emails/emailid/354147

[69] https://wikileaks.org/hackingteam/emails/emailid/482969

[70] https://wikileaks.org/hackingteam/emails/emailid/665890

[71] https://wikileaks.org/hackingteam/emails/emailid/786233

[72] https://wikileaks.org/hackingteam/emails/emailid/31789

[73] https://wikileaks.org/hackingteam/emails/emailid/33868

[74] https://wikileaks.org/hackingteam/emails/emailid/44184

[75] https://wikileaks.org/hackingteam/emails/emailid/27950

[76] https://wikileaks.org/hackingteam/emails/emailid/33398

[77] https://wikileaks.org/hackingteam/emails/emailid/38800

[78] https://wikileaks.org/hackingteam/emails/emailid/43363

[79] https://wikileaks.org/hackingteam/emails/emailid/27419

[80] https://wikileaks.org/hackingteam/emails/emailid/40565

[81] https://www.virustotal.com/en/file/cbde6a113a54b8dcf122d9d879b7c21c8b03a89d792f49210bbe41e8466d121a/analysis/

[82] https://www.virustotal.com/en/file/21e8d495bca60edc3b64ac970f9a9fa896d0eadc6491452ea937d64849b1f4a0/analysis/

[83] https://wikileaks.org/hackingteam/emails/emailid/686579

[84] https://wikileaks.org/hackingteam/emails/emailid/674354

[85] https://wikileaks.org/hackingteam/emails/emailid/673712

[86] https://wikileaks.org/hackingteam/emails/emailid/676667

[87] https://wikileaks.org/hackingteam/emails/emailid/315891

[88] https://wikileaks.org/hackingteam/emails/emailid/630854

[89] https://wikileaks.org/hackingteam/emails/emailid/1526

[90] https://wikileaks.org/hackingteam/emails/emailid/22456

[91] https://wikileaks.org/hackingteam/emails/emailid/27582

[92] https://wikileaks.org/hackingteam/emails/emailid/27029

[93] https://wikileaks.org/hackingteam/emails/emailid/1031218

[94] https://wikileaks.org/hackingteam/emails/emailid/25540

[95] https://wikileaks.org/hackingteam/emails/emailid/1079340

[96] https://wikileaks.org/hackingteam/emails/emailid/1079405

[97] This reflects the time of the initial click (i.e., the time in the log of the request for “/fwd”).

[98] This reflects whether there is a log entry for the “.apk” file for the IP, indicating that the Hacking Team RCS was installed.

[99] https://wikileaks.org/hackingteam/emails/emailid/1079122

[100] https://wikileaks.org/hackingteam/emails/emailid/1078587

[101] https://wikileaks.org/hackingteam/emails/emailid/1078587

[102] https://wikileaks.org/hackingteam/emails/emailid/1078956

[103] https://wikileaks.org/hackingteam/emails/emailid/1078956

[104] https://wikileaks.org/hackingteam/emails/emailid/1079019

[105] https://wikileaks.org/hackingteam/emails/emailid/1079095

[106] https://wikileaks.org/hackingteam/emails/emailid/1079095

[107] https://wikileaks.org/hackingteam/emails/emailid/1079521

[108] https://wikileaks.org/hackingteam/emails/emailid/789

[109] https://wikileaks.org/hackingteam/emails/emailid/1450

[110] https://wikileaks.org/hackingteam/emails/emailid/779

[111] https://wikileaks.org/hackingteam/emails/emailid/1079521

[112] https://wikileaks.org/hackingteam/emails/emailid/1526

[113] https://www.passivetotal.org/

[114] https://wikileaks.org/hackingteam/emails/emailid/25016

[115] https://wikileaks.org/hackingteam/emails/emailid/628450

[116] https://wikileaks.org/hackingteam/emails/emailid/628450

[117] https://wikileaks.org/hackingteam/emails/emailid/371942

[118] Shares IP address 119.59.123.78 with free.dramakorea.asia and shrook.mooo.com, according to PassiveTotal.

[119] C&C server for newer RCS samples, e.g., https://wikileaks.org/hackingteam/emails/emailid/1078904.

[120] https://wikileaks.org/hackingteam/emails/emailid/473090

[121] https://wikileaks.org/hackingteam/emails/emailid/1001778

2 Comments

1. Heesob Nam
   Posted August 10, 2015 at 2:01 am | Permalink

   Better prima facie case of civilian surveillance by NIS is here.

   https://www.wikileaks.org/hackingteam/emails/emailid/495052

   “Attached is the device information. I understand from the customer that the target is a lawyer and is not technical. The customer is not agreeable to uninstall 31(1) but he promise to update us if he discover something strange. I suggested him to get a few more VPS and isolate 31(1). Thats the best I can do now.”

2. AHELI
   Posted August 10, 2015 at 4:20 pm | Permalink

   Hi,

   I really appreciate your great job. I have some questions.

   First of all, is there any evidence of Trovicor found in South Korea?
   According Email (footnotes 32), we could easily guess NIS might have bought Trovicor since it’s not same type of HT’s programme.

   Well, What kind of thing could we do find some information of NIS’s Bitcoin? I’m really afraid that the affair NIS and RCS will be going to finish without any results.

   And could you give some advices for now?

   Thanks in advance.

One Trackback

1. By August 14, 2015 | cybersecurity update on August 14, 2015 at 10:45 am

   […] Canada’s Quiet History Of Weakening Communications Encryption [Citizen Lab / Also: What We Know About the South Korea NIS’s Use of Hacking Team’s RCS] […]

Post a Comment

Your email is *never* shared. Required fields are marked *

Name *

Email *

Website

Comment

Post Comment