# New Sykipot developments





March 21, 2013 | Jaime Blasco

**Summary**

During the last few years, we have been publishing about a group of hackers who have focused on targeting DIB (Defence Industrial Base) and other government organizations:

- Another Sykipot sample likely targeting US federal agencies

- Are the Sykipot's authors obsessed with next generation US drones?

- Sykipot variant hijacks DOD and Windows smart cards

- Sykipot is back

Sykipot are a highly skilled group of individuals who have exploited a wide range of zeroday vulnerabilities in the last few years including:

| CVE | Date | Product |
|---|---|---|
| CVE-2007-0671 | 2007-02-02 | Microsoft Excel |
| CVE-2009-3957 | 2010-12-01 | Adobe Reader |
| CVE-2010-0806 | 2010-05-04 | Internet Explorer |
| CVE-2010-2883 | 2010-09-08 | Adobe Reader |
| CVE-2010-3654 | 2010-10-28 | Adobe Flash Player |
| CVE-2011-2462 | 2011-12-06 | Adobe Reader |

In this blog post we will unveil the new vulnerabilities that this group have used using during the last 8 months and we will publish the new infrastructure they have used. We will expose several examples of the campaigns they have launched and new versions of the Sykipot backdoor they have used to access the compromised systems. We have found evidences that show they have exploited at least the following vulnerabilities during the last few months:

| CVE | Date | Product |
|---|---|---|
| CVE-2012-1889 | 06/13/2012 | MSXML/Internet Explorer |
| CVE-2012-1723 | 06/12/2012 | Java 7 |
| CVE-2012-4969 | 09/16/2012 | Microsoft Internet Explorer |
| CVE-2013-0640 | 02/12/2012 | Adobe Acrobat Reader |

Several times the date of the exploit was a few days after the vulnerability had been disclosed and there wasn't a patch released by the vendor.

**Campaigns**

In the past most of the campaigns which we found related to the Sykipot actors were based on SpearPhishing mails with attachments that exploited vulnerabilities in software like Microsoft Office, Adobe Flash, Adobe PDF and some times Internet Explorer. During the last 8-10 months we have seen a change and the number of SpearPhishing campaigns which have

included a link instead of an attachment and this has increased. Once the victim clicks in the link the attackers will use vulnerabilities in Internet Explorer, Java, etc to access the system.

Some examples of the campaigns they have launched are detailed below.

**gsasmartpay.org - 2012-06-20**

The last summer, we found a malicious site that the Sykipot actors set up to try and phish government employees. When the victim visited the link the following page appeared:


As we can see it shows the information present in https://smartpay.gsa.gov/.

"The GSA SmartPay program, established in 1998, is the largest charge card program in the world serving more than 350 federal agencies, organizations, and Native American tribal governments. In FY10, approximately 98.9M transactions were made and $30.2B were charged using the GSA SmartPay charge cards, creating $325.9M in refunds."

"Eligibility for the program is determined by the GSA SmartPay Contracting Officer. Federal agencies, departments, tribal organizations, and approved non-federal entities can apply to obtain charge card services under the GSA SmartPay program."

If we take a look at the malicious files we will find that it was exploiting CVE-2012-1889 in the background:

During the exploitation it will load the following files as well:

www[.]gsasmartpay[.]org/cardholders/login/movie[.]swf?apple=AA969692D8CDCD959595CC859183918F83909692839BCC8D9085CD83868D808784CC919584E2E2E2E2

www[.]gsasmartpay[.]org/cardholders/login/deployJava[.]js

www[.]gsasmartpay[.]org/cardholders/login/faq[.]htm

We are not going to show how this vulnerability is exploited since we have showed it in previous blog posts, you can find a good description here.

searching-job.net is another domain registered by the Sykipot actors (registered by thomas7610@yahoo.com on 06-20-2012) that was also serving the same exploit at that time:

www[.]searching-job[.]net/list/verification/deployJava[.]js

www[.]searching-job[.]net/list/verification/faq[.]htm

www[.]searching-job[.]net/list/verification/index[.]htm

www[.]searching-job[.]net/list/verification/movie[.]swf?
apple=AA969692D8CDCD959595CC91878390818A8B8C85CF888D80CC8C8796CD848B8E878E8B9196CC868396E2E2E2E2

www[.]searching-job[.]net/account_list/verification/index[.]htm

Apart from gsasmartpay.org we have found several domains registered by the Sykipot actors that they have probably used to phish users in the last few months. Some of the most suspicious ones are detailed below:

- aafbonus.com registered by janagreen2000@yahoo.com on 06-19-2012

Probably related to American Advertising Federation - http://www.aaf.org/

- nceba.org registered by jimgreen200088@yahoo.com on 07-24-2012

Probably related to U.S. BANKRUPTCY ADMINISTRATOR - http://www.nceba.uscourts.gov/

- pdi2012.org registered by alcott.churchill@yahoo.com on 08-18-2011

Probably related to PDI 2012, the premier training event hosted by the American Society of Military Comptrollers

- hudsoninst.com registered by alcott.churchill@yahoo.com on 11-26-2012

Probably related to the Hudson Institute - http://www.hudson.org/

Hudson Institute is a nonpartisan, independent policy research organization dedicated to innovative research and analysis that promotes global security, prosperity, and freedom.

**CVE-2012-4969 - Internet Explorer**

In September last year, the Sykipot actors registered several domains to exploit a vulnerability in Internet Explorer (CVE-2012-4969).

- resume4jobs.net registered by james.wade1@yahoo.com on 03-08-2012

URL's involved:

http://www[.]resume4jobs[.]net/account/1024486[.]html

http://www[.]resume4jobs[.]net/account/embed[.]htm

http://www[.]resume4jobs[.]net/jobs[.]exe Sykipot malware that uses info[.]resume4jobs[.]net as the C&C

- paypal1.dns1.us - Dynamic DNS provider

URL's involved:

http://paypal1[.]dns1[.]us/account/1024486[.]html

http://paypal1[.]dns1[.]us/account/embed[.]htm

- pollingvoter.org registered by jimgreen200088@yahoo.com on 06-11-2012

URL's involved:

http://www[.]pollingvoter[.]org/ne2012/vote/embed[.]htm

http://www[.]pollingvoter[.]org/life[.]exe Sykipot malware that uses www[.]betterslife[.]com as the C&C

- skyruss.net registered by joneluxara@yahoo.com on 04-17-2012

URL's involved:

http://social[.]sns[.]skyruss[.]net/variety/index[.]html

http://forum[.]skyruss[.]net/articles/embed[.]htm

**CVE-2012-1723 - Java 7**

In August, they were exploiting a vulnerability in Java (CVE-2012-1723) to gain access to the victim's systems. It seems they were using the Metasploit version of the exploit.

Some examples are:

- slashdoc.org registered by jessantt@gmail.com on 05-21-2012

URL's involved:

http://www[.]slashdoc[.]org/default[.]jar

http://www[.]slashdoc[.]org/index[.]html

The index.html page loads the malicious Java applet and it passes the payload they want to execute using the data parameter (the value is hex encoded):


In this case the host www[.]photosmagnum[.]com was used as the C&C server.

- nceba.org registered by jimgreen200088@yahoo.com on 07-24-2012

URL's involved:

http://www[.]nceba[.]org/newsroom/article/news201207240251[.]html

http://www[.]nceba[.]org/newsroom/article/default[.]jar

Using www[.]betterslife[.]com as the C&C server.

- milstars.org registered by slyan8024@gmail.com on 06-20-2012

URL's involved:

http://milstars[.]org/view/default[.]jar

**CVE-2013-0640 - PDF Exploit targeting Japanese victims**

We found the Sykipot actors using the latest Adobe Acrobat exploit (CVE-2013-0640) a few weeks ago.

The version of the exploit is the same that we found in our latest blog post:

- Latest Adobe PDF exploit used to target Uyghur and Tibetan activists

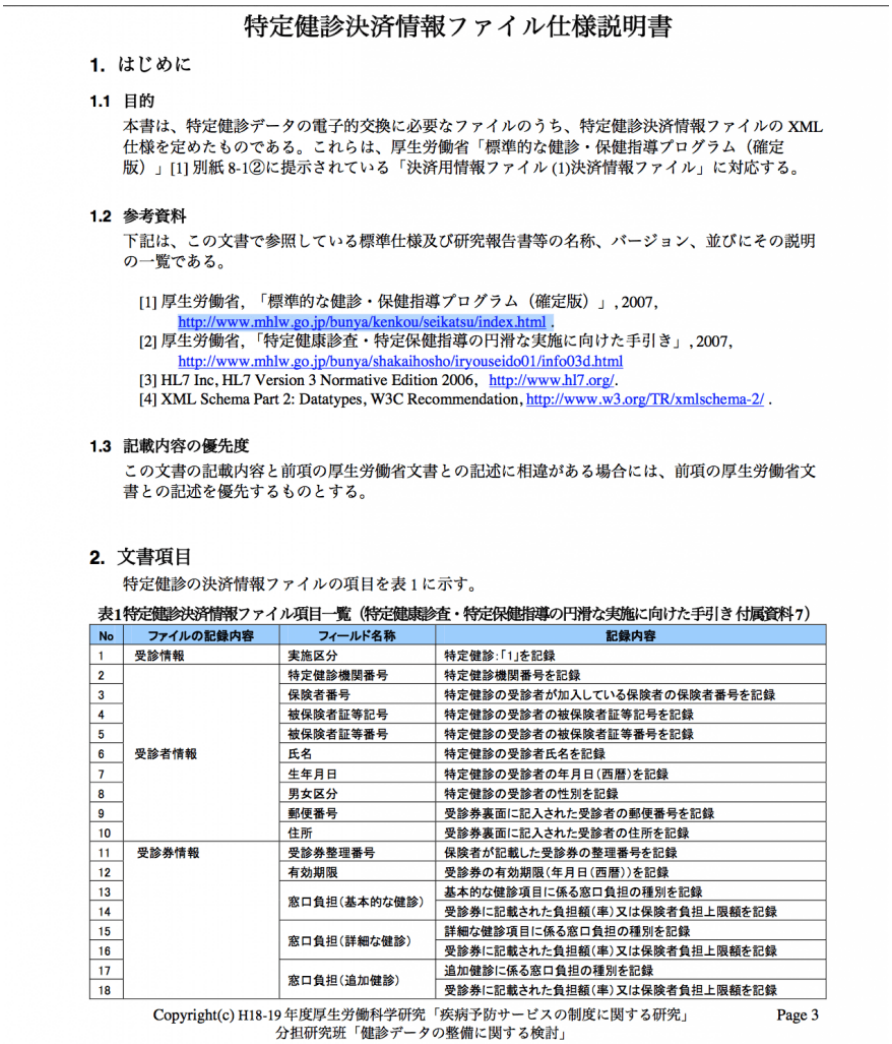
The Javascript code inside the PDF file is very similar to the one found in the Itaduke samples but part of the initial variables and the obfuscation has been removed from the original one.

Once the PDF is opened the following lure file is displayed to the victim:

Based on the content of the lure document the potential victims seem to be somehow related to the **Japanese Ministry of Health, Labour and Welfare**

Once the infection takes place the following files are created on the system:

DOCUME~1ADMINI~1LOCALS~1Temppfilede.dat 5ED3A94354F27BC7AF0FEF04F89D8EB8



# 特定健診決済情報ファイル仕様説明書

## 1. はじめに

### 1.1 目的

本書は、特定健診データの電子的交換に必要なファイルのうち、特定健診決済情報ファイルの XML 仕様を定めたものである。これらは、厚生労働省「標準的な健診・保健指導プログラム（確定版）」[1] 別紙 8-1②に提示されている「決済用情報ファイル (1)決済情報ファイル」に対応する。

### 1.2 参考資料

下記は、この文書で参照している標準仕様及び研究報告書等の名称、バージョン、並びにその説明の一覧である。

[1] 厚生労働省，「標準的な健診・保健指導プログラム（確定版）」, 2007,
http://www.mhlw.go.jp/bunya/kenkou/seikatsu/index.html .
[2] 厚生労働省，「特定健康診査・特定保健指導の円滑な実施に向けた手引き」, 2007,
http://www.mhlw.go.jp/bunya/shakaihosho/iryouseido01/info03d.html
[3] HL7 Inc, HL7 Version 3 Normative Edition 2006, http://www.hl7.org/.
[4] XML Schema Part 2: Datatypes, W3C Recommendation, http://www.w3.org/TR/xmlschema-2/ .

### 1.3 記載内容の優先度

この文書の記載内容と前項の厚生労働省文書との記述に相違がある場合には、前項の厚生労働省文書との記述を優先するものとする。

## 2. 文書項目

特定健診の決済情報ファイルの項目を表 1 に示す。

表1特定健診決済情報ファイル項目一覧（特定健康診査・特定保健指導の円滑な実施に向けた手引き 付属資料7）

| No | ファイルの記録内容 | フィールド名称 | 記録内容 |
|---|---|---|---|
| 1 | 受診情報 | 実施区分 | 特定健診:「1」を記録 |
| 2 | 受診者情報 | 特定健診機関番号 | 特定健診機関番号を記録 |
| 3 | | 保険者番号 | 特定健診の受診者が加入している保険者の保険者番号を記録 |
| 4 | | 被保険者証等記号 | 特定健診の受診者の被保険者証等記号を記録 |
| 5 | | 被保険者証等番号 | 特定健診の受診者の被保険者証等番号を記録 |
| 6 | | 氏名 | 特定健診の受診者氏名を記録 |
| 7 | | 生年月日 | 特定健診の受診者の年月日（西暦）を記録 |
| 8 | | 男女区分 | 特定健診の受診者の性別を記録 |
| 9 | | 郵便番号 | 受診券裏面に記入された受診者の郵便番号を記録 |
| 10 | | 住所 | 受診券裏面に記入された受診者の住所を記録 |
| 11 | 受診券情報 | 受診券整理番号 | 保険者が記載した受診券の整理番号を記録 |
| 12 | | 有効期限 | 受診券の有効期限（年月日（西暦））を記録 |
| 13 | | 窓口負担（基本的な健診） | 基本的な健診項目に係る窓口負担の種別を記録 |
| 14 | | | 受診券に記載された負担額（率）又は保険者負担上限額を記録 |
| 15 | | 窓口負担（詳細な健診） | 詳細な健診項目に係る窓口負担の種別を記録 |
| 16 | | | 受診券に記載された負担額（率）又は保険者負担上限額を記録 |
| 17 | | 窓口負担（追加健診） | 追加健診に係る窓口負担の種別を記録 |
| 18 | | | 受診券に記載された負担額（率）又は保険者負担上限額を記録 |




DOCUME~1ADMINI~1LOCALS~1mpr.dll 84EFAFF343CF7A34D2A0D847A1E5FD50

DOCUME~1ADMINI~1LOCALS~1setm.ini 00051F392350128BA4DD4CA10F44DDEF

DOCUME~1ADMINI~1LOCALS~1 emp.dll BEA84BE4BFE236652F6A4E382B21A96F

The file setm.ini contains the configuration of Sykipot in this case:

[srv_info]

sleeptime=3600000

url=bassball[.]peocity[.]com (C&C server)

scexe=rsvp.exe

scdll=mpr.dll

runexe=run.exe

mark=0304adbh

The following actions take place in the system:

cmd /c reg add HKCUSOFTWAREMicrosoftWindowsCurrentVersionRun /v start /t REG_SZ /d [sykipot_payload_file].exe -startup /f (persistence)

Several functions are called within the Sykipot's DLL:

[sykipot_payload_file].exe -startupEx

[sykipot_payload_file].exe -startup1

cmd /c [sykipot_payload_file].exe -startup

Then the malicious payload will be injected into Internet Explorer.

The malware will communicate with the C&C server once in a while using SSL and the well known communication paths of previous Sykipot payloads:

/kys_allow_put.asp?type=

/kys_allow_get.asp?name=

As we showed in the past most of the Sykipot samples used the key "19990817" for encryption.In this sample we have found a new key "20120709" that is also a date.

**Infrastructure**

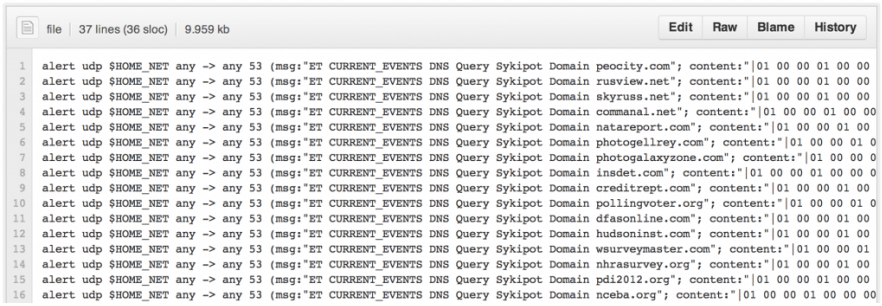
Along with the blog post we are making a list of new domains public that weren't mentioned in previous Sykipot research:

Unique malicious domains:

- peocity.com
- rusview.net
- skyruss.net
- commanal.net
- natareport.com
- photogellrey.com
- photogalaxyzone.com
- insdet.com
- creditrept.com
- pollingvoter.org
- dfasonline.com
- hudsoninst.com
- wsurveymaster.com
- nhrasurvey.org
- pdi2012.org
- nceba.org
- linkedin-blog.com
- aafbonus.com
- milstars.org
- vatdex.com
- insightpublicaffairs.org
- applesea.net
- appledmg.net
- appleintouch.net
- seyuieyahooapis.com
- appledns.net
- emailserverctr.com
- dailynewsjustin.com
- hi-tecsolutions.org
- slashdoc.org
- photosmagnum.com
- resume4jobs.net
- searching-job.net
- servagency.com

- gsasmartpay.org
- tech-att.com

We are releasing Snort rules to detect queries to the malicious domains in your network:




Thanks to EmergingThreats http://www.emergingthreats.net/ [no longer available] for the help. You will find the rules in its ruleset update today as well.

Based in our research, below is the list of unique e-mail addreses used to registered malicious domains:

- 233@lao.com
- Joneluxara@yahoo.com
- alcott.churchill@yahoo.com
- b@bvc.com
- calvin.kliff@yahoo.com
- carrier.fisher@hotmail.com
- conan0557@126.com
- james.wade1@yahoo.com
- janagreen2000@yahoo.com
- jessantt@gmail.com
- jimgreen200088@yahoo.com
- jimgreen20008@yahoo.com
- marialreyna11211919@yahoo.com
- morgan.wale1@yahoo.com
- mskinner62@yahoo.com
- myhog@hotmail.com
- parviz7415@yahoo.com
- slyan8024@gmail.com
- thomas7610@yahoo.com

Apart from the list of new domains you should check out the domains mentioned in the following articles that all related to previous Sykipot's activity but some of them are still being used in Sykipot's operations:

- Sykipot is back - Alienvault Labs

- The Sykipot Attacks - Symantec

- The Sykipot Campaign - TrendMicro

- Hurricane Sandy serves as lure to deliver Sykipot - Verizon

- Insight into Sykipot Operations - Symantec

### Share this with others

Tags: sykipot, cve-2013-0640, cve-2012-1889, cve-2012-4969, cve-2012-1723