SOPHOS
Security made simple.

The Rotten Tomato Campaign

By **Gabor Szappanos**, Principal Researcher, SophosLabs Hungary

A SophosLabs technical paper – October 2014

Contents

Overview

Malware authors are not shy about borrowing ideas. One of the most typical cases is the Tomato Garden case,[1] where several different groups used the same zero-day Microsoft Word exploit. The term "used" means that they somehow get hold of a document that exploited the vulnerability, and then left the exploiting document part and the shellcode intact, only changed the appended encrypted executable at the end, and immediately they had what needed.

Something very similar happened just recently, in August and September of 2014.

I always wanted to know how the malware writing groups worked. I mean the really serious ones, the ones behind Chinese state-sponsored APT attacks, or the groups behind high profile common malware, like Zeus.

This case offers another piece of insight. There must have been a staff meeting, where the manager prompted that, in the next malware distribution campaign they should not only use the aging CVE-2012-0158 vulnerability, but the newer CVE-2014-1761 as well. The rest of the document will detail how some of the groups coped with this task.

Clearly, the malware authors took a sample somehow and started the implementation process. I wasn't there, of course, so what follows is an educated guess based on the samples.

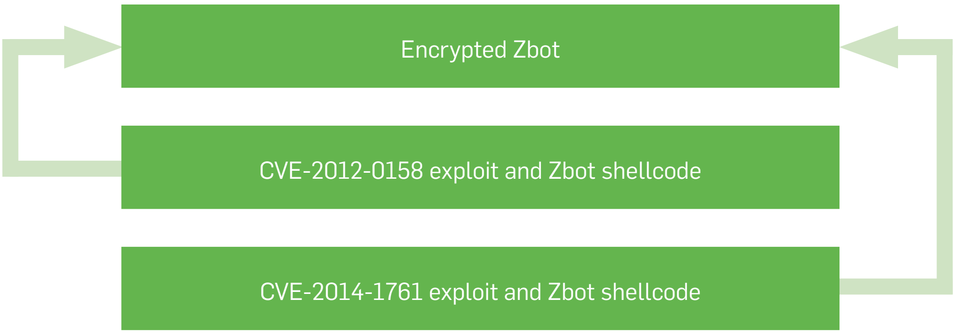
Template 1: CVE-2012-0158 + CVE-2014-1761 Combo

Recently we saw a lot of samples that exploit both CVE-2012-0158 and CVE-2014-1761, and usually either download or drop a Zbot variant.

The document starts with the RTF header stuff, followed by the encrypted second stage.

This is followed by the embedded object exploiting the CVE-2012-0158 vulnerability with the shellcode. Following it is a block exploiting the CVE-2014-1761 with a shellcode of its own, as illustrated in the image below.

The color scheme I will use in the rest of the document is the following: green represents the properly used components; yellow the unused components; and red the incorrectly used components.


Encrypted Zbot
CVE-2012-0158 exploit and Zbot shellcode
CVE-2014-1761 exploit and Zbot shellcode

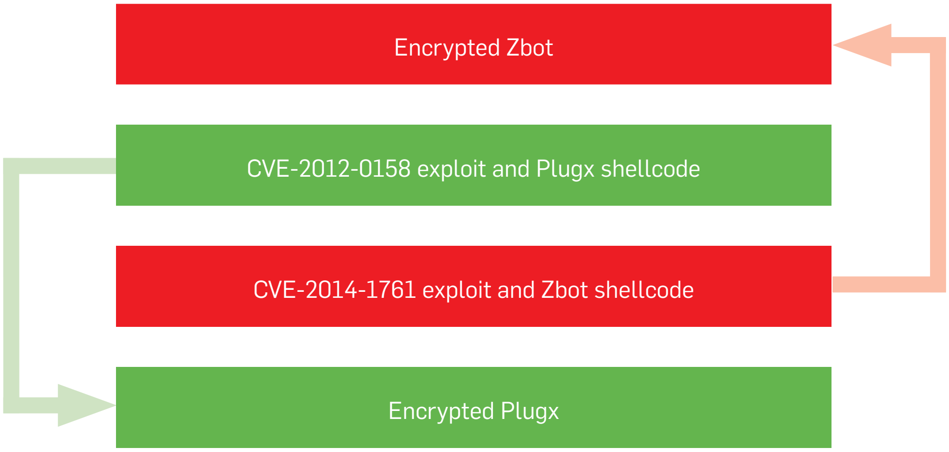
Regardless of the particular exploit used, both shellcodes performed the memory egg-hunting for the memory markers of the second stage (as described in[2]), and decrypted it when found. The second stage could be either a downloader shellcode or a Win32 executable.

One of these samples was SHA1: c3a7cb43ec13299b758cb8ca25eace71329939f7, which contained an encrypted Zbot variant[3] at the beginning of the RTF. It looks very likely that this sample was used as a development template for the other malware writing groups.

First attempt: Plugx

The first attempt must have come from the group deploying Plugx. They took the above mentioned sample, and made some modifications to it.

The result looks like this one:


Encrypted Zbot
CVE-2012-0158 exploit and Plugx shellcode
CVE-2014-1761 exploit and Zbot shellcode
Encrypted Plugx

I can only guess that they didn't understand the CVE-2014-1761 component, and thought that there was only one shellcode, in the CVE-2012-0158 segment. So they appended the encrypted Plugx executable, and replaced the first shellcode with their own. This shellcode contains the hardcoded offset of the embedded executable, and decrypts from there.

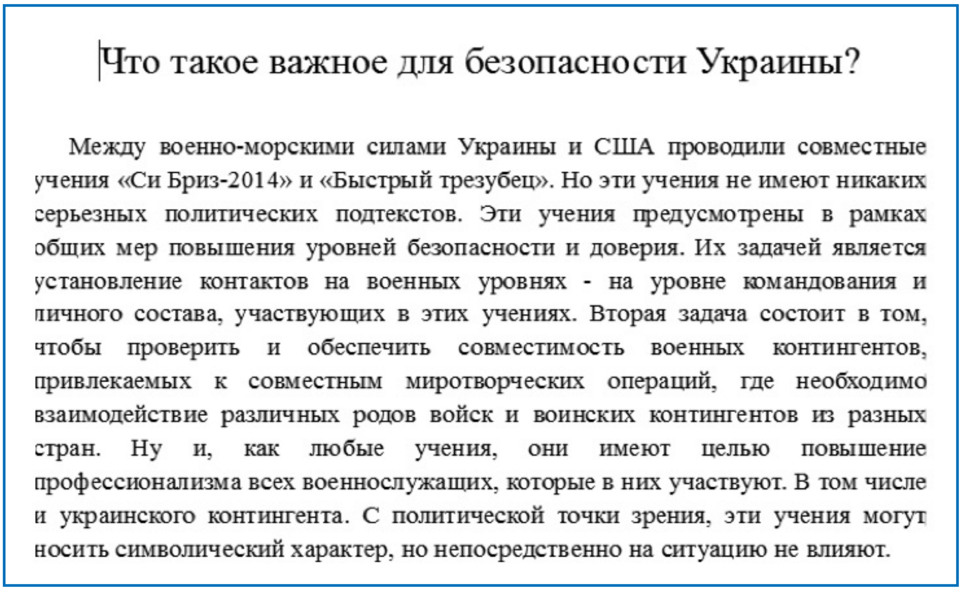
However, they left intact the encrypted Zbot executable at the beginning of the file and the second vulnerability, making this sample a real dual weapon: not only that it exploits two vulnerabilities, but contains two totally different payloads. However, Word can only be exploited once: during the exploitation procedure the current instance of Word exits, and a new one is started that displays the decoy document. So this creates a race condition: whichever vulnerability is triggered first (or gets lucky in an environment where the other one is patched) will have the chance to run its own payload.

13effaca957cc362bdcbfdd05b5763205b53d9ca
Original name: **N/A**

System activity

Dropped to C:\Documents and Settings\All Users\DRM\AShld\drmupgds.exe (clean loader digitally signed by Microsoft) and C:\Documents and Settings\All Users\DRM\AShld\BlackBox.DLL (malware loader) and C:\Documents and Settings\All Users\DRM\AShld\BlackBox.BOX (payload); registered in HKLM\SYSTEM\CurrentControlSet\Services\BlackBox → ImagePath

The payload is next-generation Plugx,[4] plugin function creation dates are 0x20130810.



Что такое важное для безопасности Украины?

Между военно-морскими силами Украины и США проводили совместные учения «Си Бриз-2014» и «Быстрый трезубец». Но эти учения не имеют никаких серьезных политических подтекстов. Эти учения предусмотрены в рамках общих мер повышения уровней безопасности и доверия. Их задачей является установление контактов на военных уровнях - на уровне командования и личного состава, участвующих в этих учениях. Вторая задача состоит в том, чтобы проверить и обеспечить совместимость военных контингентов, привлекаемых к совместным миротворческих операций, где необходимо взаимодействие различных родов войск и воинских контингентов из разных стран. Ну и, как любые учения, они имеют целью повышение профессионализма всех военнослужащих, которые в них участвуют. В том числе и украинского контингента. С политической точки зрения, эти учения могут носить символический характер, но непосредственно на ситуацию не влияют.

C&C servers

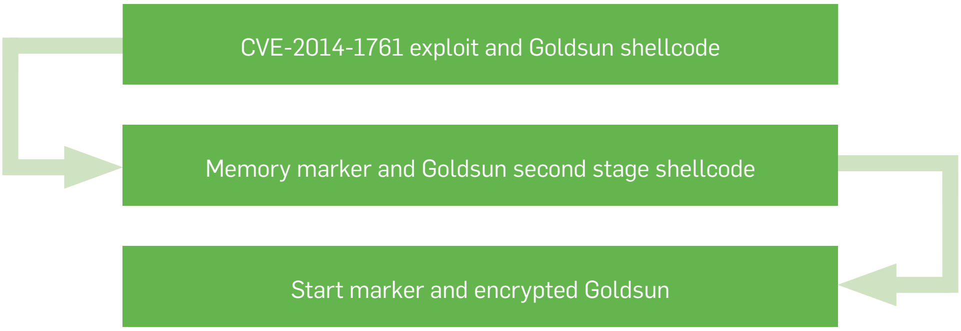
chromeupdate.authorizeddns.org
Dynamic DNS service

googlesupport.proxydns.com
Dynamic DNS service

Template 2: Goldsun

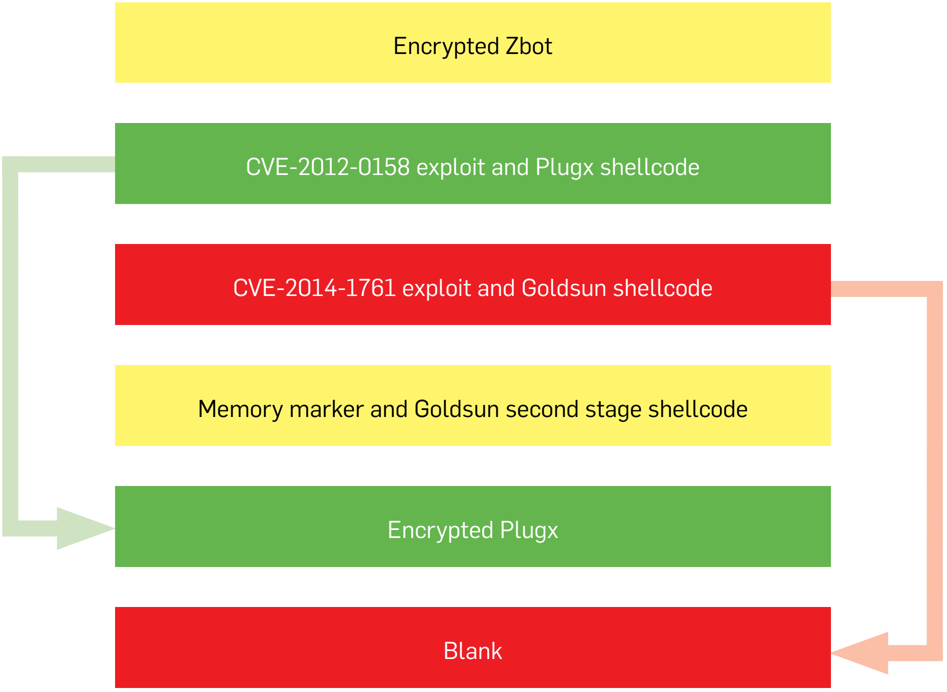
At some point they must have realized that it was wrong and tried to fix the CVE-2014-1761 part. For that, they took another recent sample, something similar to those that drop Goldsun Trojans (like this SHA1: e2474cc0da5a79af876771217eb81974e73c39e5)

In this case, the RTF only contains the CVE-2014-1761 vulnerability, with an appended executable. The vulnerability expects the second stage shellcode at a fixed file offset, checks a marker string there ("p!11"), and jumps to the second stage, which then decrypts and executes the final Win32 payload.


CVE-2014-1761 exploit and Goldsun shellcode
Memory marker and Goldsun second stage shellcode
Start marker and encrypted Goldsun

Second attempts

A large group of samples were created by a sort of a fusion of the Zbot and the Goldsun samples, resulting in a structure like this one:


Encrypted Zbot
CVE-2012-0158 exploit and Plugx shellcode
CVE-2014-1761 exploit and Goldsun shellcode
Memory marker and Goldsun second stage shellcode
Encrypted Plugx
Blank

So now there are two different shellcodes. The first, from Plugx, reads the length of the embedded decoy document and Win32 payload from the end of the file, and using this info locates and decrypts the appended payload. This shellcode identifies the host document by checking if the last dword is the same as the dword before that rotated by 3. And the same holds for another two dwords before that. These dwords also store the length of the appended PE payload and decoy document lengths. This structure makes it possible to swap the payload without changing the exploit and shellcode part.

The shellcode from Goldsun executes the second stage code from a fixed offset.

There are a couple of problems with this implementation. First, the defunctional encrypted Zbot remains in these files, with no purpose at all. But the real problem is with the Goldsun style CVE-2014-1761 block. It was snatched from the CVE-2014-1761 exploiting document, and pasted after the existing Zbot+CVE-2012-0158 combo. Clearly, the offset where the second stage code would be shifted with the different prepended content, but it never happened. As a result, the CVE-2014-1761 exploitation doesn't work, despite all the efforts of the malware authors.

A couple of distinct malware groups were identified that use these schematics.

Plugx

All of these samples are Plugx v2 samples.[4] Most of the time they use Russian related themes in the decoy document.

21b3e540746816c85e5270a1b8bb58bf713ff5f5

Original name: **N/A**

The dropped decoy document doesn't contain anything, it is only blank page.

System activity

Dropped to C:\Documents and Settings\All Users\DRM\usta\usha.exe (clean loader, digitally signed by Kaspersky) and C:\Documents and Settings\All Users\DRM\usta\ushata.dll (malware loader) and C:\Documents and Settings\All Users\DRM\usta\ushata.dll.avp (payload); registered for startup as a service in HKLM\SYSTEM\CurrentControlSet\Services\usta → ImagePath

The payload is next generation Plugx,[4] plugin function creation dates are 0x20130810

C&C servers

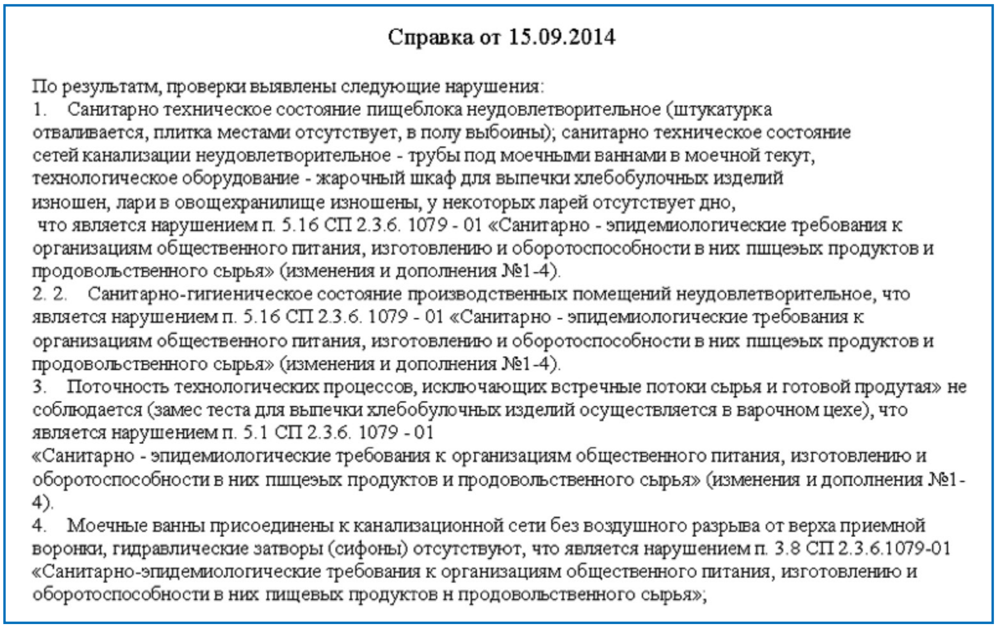
www.notebookhk.net

Registry Registrant ID:
Registrant Name: lee stan
Registrant Organization: lee stan
Registrant Street: xianggangdiqu
Registrant City: xianggangdiqu
Registrant State: xianggang

Registrant Postal Code: 796373
Registrant Country: HK
Registrant Phone: +0.04375094543
Registrant Fax: +0.04375094543
Registrant Email: stanlee@gmail.com

80f965432ce872fc3592d9f907d5a4f66ab07f9c

Original name: **Справка от 16.09.2014.doc**



Справка от 15.09.2014

По результатм, проверки выявлены следующие нарушения:

1. Санитарно техническое состояние пищеблока неудовлетворительное (штукатурка отваливается, плитка местами отсутствует, в полу выбоины); санитарно техническое состояние сетей канализации неудовлетворительное - трубы под моечными ваннами в моечной текут, технологическое оборудование - жарочный шкаф для выпечки хлебобулочных изделий изношен, лари в овощехранилище изношены, у некоторых ларей отсутствует дно, что является нарушением п. 5.16 СП 2.3.6. 1079 - 01 «Санитарно - эпидемиологические требования к организациям общественного питания, изготовлению и оборотоспособности в них пщцеэых продуктов и продовольственного сырья» (изменения и дополнения №1-4).

2. 2. Санитарно-гигиеническое состояние производственных помещений неудовлетворительное, что является нарушением п. 5.16 СП 2.3.6. 1079 - 01 «Санитарно - эпидемиологические требования к организациям общественного питания, изготовлению и оборотоспособности в них пщцеэых продуктов и продовольственного сырья» (изменения и дополнения №1-4).

3. Поточность технологических процессов, исключающих встречные потоки сырья и готовой продутая» не соблюдается (замес теста для выпечки хлебобулочных изделий осуществляется в варочном цехе), что является нарушением п. 5.1 СП 2.3.6. 1079 - 01 «Санитарно - эпидемиологические требования к организациям общественного питания, изготовлению и оборотоспособности в них пщцеэых продуктов и продовольственного сырья» (изменения и дополнения №1-4).

4. Моечные ванны присоединены к канализационной сети без воздушного разрыва от верха приемной воронки, гидравлические затворы (сифоны) отсутствуют, что является нарушением п. 3.8 СП 2.3.6.1079-01 «Санитарно-эпидемиологические требования к организациям общественного питания, изготовлению и оборотоспособности в них пищевых продуктов н продовольственного сырья»;

System activity

Dropped to C:\Documents and Settings\All Users\DRM\AShld\AShld.exe (clean loader, digitally signed by McAfee) and C:\Documents and Settings\All Users\DRM\AShld\AShldRes.DLL (malware loader) and C:\Documents and Settings\All Users\DRM\AShld\AShldRes.DLL.asr (payload); registered for startup as a service in HKLM\SYSTEM\CurrentControlSet\Services\AShld → ImagePath

The payload is next generation Plugx,[4] plugin function creation dates are 0x20130810.

C&C servers

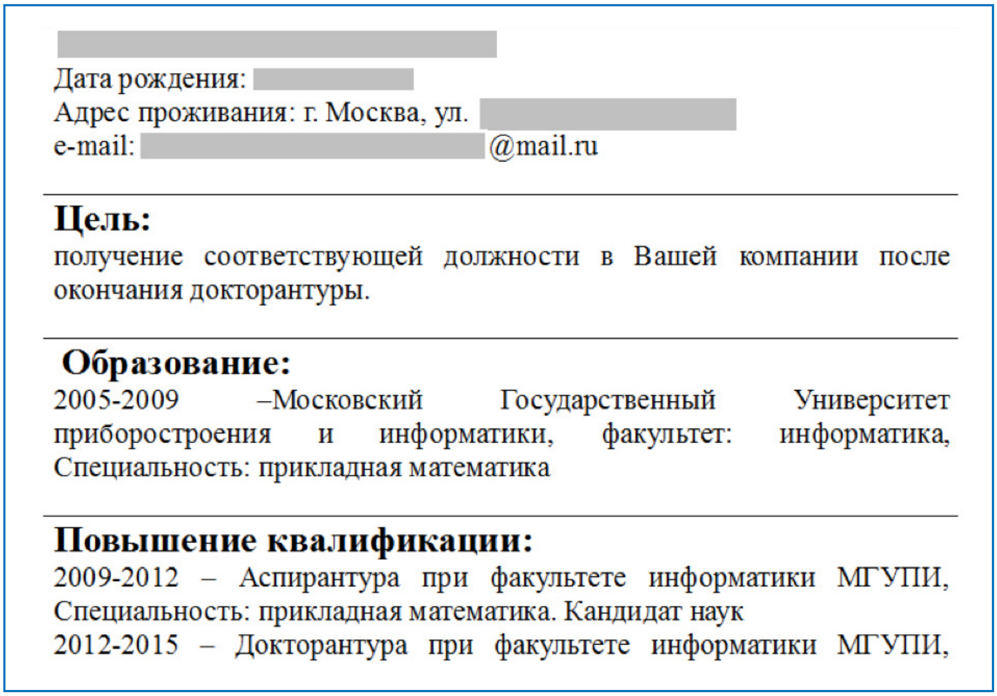
dwm.dnsedc.com

Registry Registrant ID:
Registrant Name: qiuping liu
Registrant Organization: huajiyoutian
Registrant Street: beijing
Registrant City: Beijing
Registrant State/Province: BJ
Registrant Postal Code: 100191

Registrant Country: CN
Registrant Phone: +86.1052810955
Registrant Phone Ext:
Registrant Fax: +89.1052810955
Registrant Fax Ext:
Registrant Email: yuminga1@126.com

Two of the Plugx samples turned out to be very new developments. Similar samples were just recently encountered from the list generated by a researcher.[5]

176273806e6fe338123ff660e70145935bac77c3
Original name: **РЕЗЮМЕ.doc**



[redacted]
Дата рождения: [redacted]
Адрес проживания: г. Москва, ул. [redacted]
e-mail: [redacted]@mail.ru

Цель:

получение соответствующей должности в Вашей компании после окончания докторантуры.

Образование:

2005-2009 –Московский Государственный Университет приборостроения и информатики, факультет: информатика, Специальность: прикладная математика

Повышение квалификации:

2009-2012 – Аспирантура при факультете информатики МГУПИ, Специальность: прикладная математика. Кандидат наук
2012-2015 – Докторантура при факультете информатики МГУПИ,

System activity

Dropped to C:\Documents and Settings\All Users\DRM\KavSky\msinfo.exe (clean loader by Kaspersky) and C:\Documents and Settings\All Users\DRM\KavSky\msi.dll (malware loader) and C:\Documents and Settings\All Users\DRM\KavSky\msi.dll.eng (payload); registered in for startup as a service in HKLM\SYSTEM\CurrentControlSet\Services\KavSky → ImagePath

The payload is next generation Plugx [4], plugin function creation dates are 20140719 (and interestingly, decimal and not hexadecimal, as generally seen in Plugx). Additionally, it has some internal function names not seen in earlier Plugx versions: ZX, ZXWT, JP1, JP2, JP3, JP4, JP5, JAP0, JAP1

C&C servers

futuresgolda.com

Registry Registrant ID:
Registrant Name: qiuping liu
Registrant Organization: huajiyoutian
Registrant Street: beijing
Registrant City: Beijing
Registrant State/Province: BJ
Registrant Postal Code: 100191

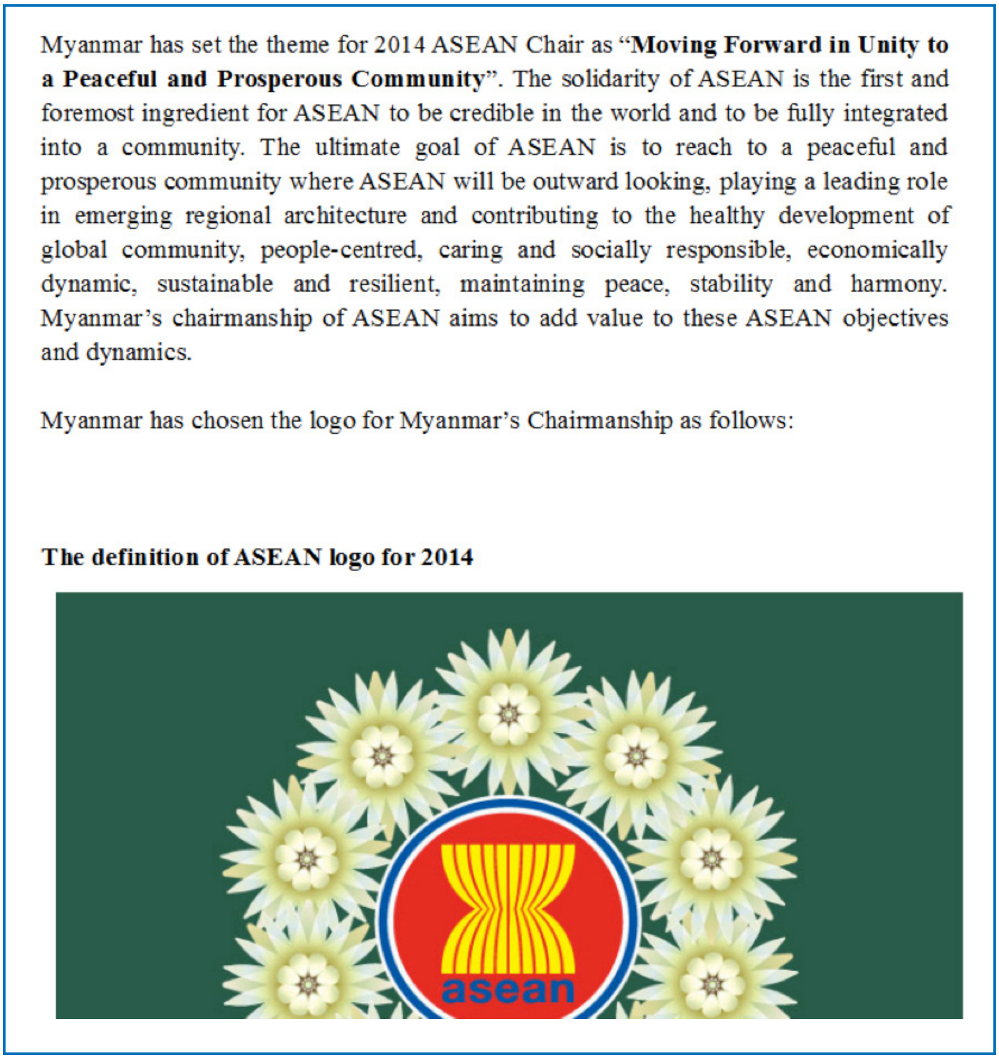
Registrant Country: CN
Registrant Phone: +86.1052810955
Registrant Phone Ext:
Registrant Fax: +89.1052810955
Registrant Fax Ext:
Registrant Email: yuminga1@126.com

adobeflashupdate.dynu.com
Dynamic DNS service

systemupdate5.dtdns.com
Dynamic DNS service

4ad76ce333b38c5bdd558e3d76640fa322e3cca6

Original name: **2014 Chairmanship_end.doc**



Myanmar has set the theme for 2014 ASEAN Chair as "**Moving Forward in Unity to a Peaceful and Prosperous Community**". The solidarity of ASEAN is the first and foremost ingredient for ASEAN to be credible in the world and to be fully integrated into a community. The ultimate goal of ASEAN is to reach to a peaceful and prosperous community where ASEAN will be outward looking, playing a leading role in emerging regional architecture and contributing to the healthy development of global community, people-centred, caring and socially responsible, economically dynamic, sustainable and resilient, maintaining peace, stability and harmony. Myanmar's chairmanship of ASEAN aims to add value to these ASEAN objectives and dynamics.

Myanmar has chosen the logo for Myanmar's Chairmanship as follows:

The definition of ASEAN logo for 2014

System activity

Dropped to C:\Documents and Settings\All Users\DRM\KavSky\m.exe (clean loader, digitally signed by Kaspersky) and C:\Documents and Settings\All Users\DRM\KavSky\msi.dll (malware loader) and C:\Documents and Settings\All Users\DRM\KavSky\msi.dll.eng (payload); registered in for startup as a service in HKLM\SYSTEM\CurrentControlSet\Services\KavSky → ImagePath

The payload is next generation Plugx,[4] plugin function creation dates are 20140719 decimal. Additionally, it has some internal function names not seen in earlier Plugx versions: ZX, ZXWT, JP1, JP2, JP3, JP4, JP5, JAP0, JAP1

This sample used a Myanmar related decoy theme, likely part of a separate distribution campaign.

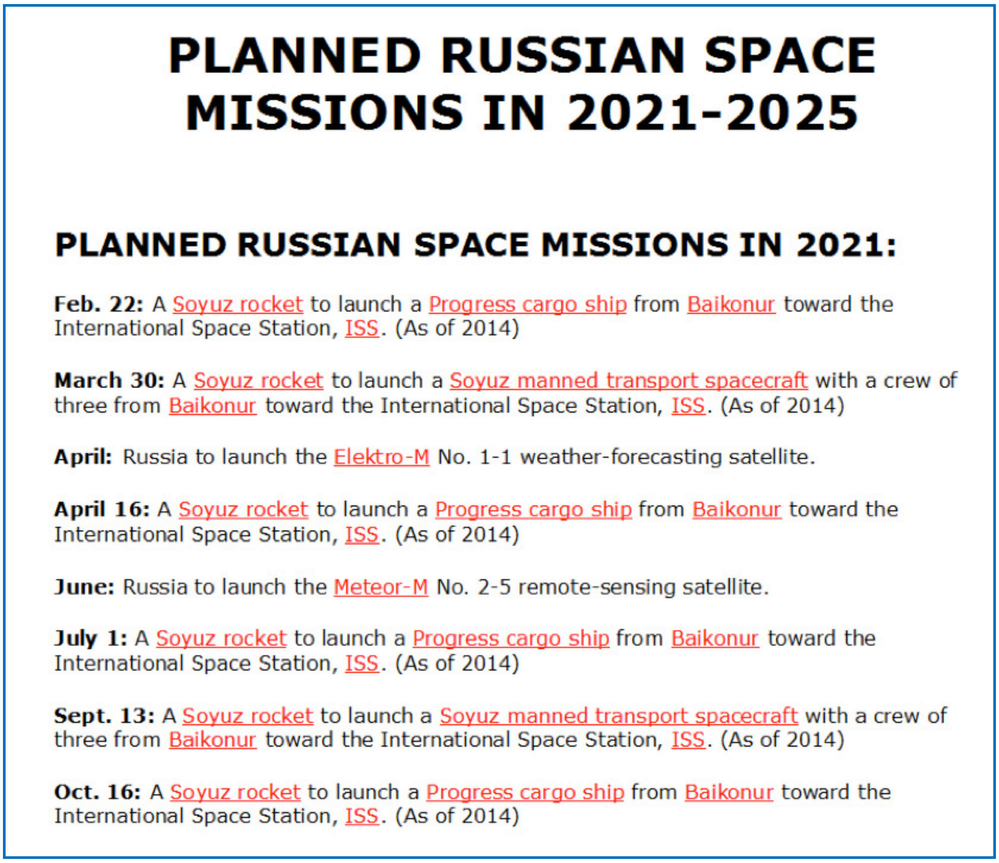
C&C servers

indiasceus.jetos.com Dynamic DNS service	**indiasceus.justdied.com** Dynamic DNS service

Appat

These are new Trojans. Not connected to Plugx at code level, but the overlap between the C&C servers, the same domain registration contact (yuminga1@126.com), and the similar Russian theme indicates that the same group deployed them.

0dfd883c1f205f0740d50688683f1869bcc0e9d7
Original name: **План космической деятельности на 2021-2025 год.doc**



PLANNED RUSSIAN SPACE MISSIONS IN 2021-2025

PLANNED RUSSIAN SPACE MISSIONS IN 2021:

Feb. 22: A Soyuz rocket to launch a Progress cargo ship from Baikonur toward the International Space Station, ISS. (As of 2014)

March 30: A Soyuz rocket to launch a Soyuz manned transport spacecraft with a crew of three from Baikonur toward the International Space Station, ISS. (As of 2014)

April: Russia to launch the Elektro-M No. 1-1 weather-forecasting satellite.

April 16: A Soyuz rocket to launch a Progress cargo ship from Baikonur toward the International Space Station, ISS. (As of 2014)

June: Russia to launch the Meteor-M No. 2-5 remote-sensing satellite.

July 1: A Soyuz rocket to launch a Progress cargo ship from Baikonur toward the International Space Station, ISS. (As of 2014)

Sept. 13: A Soyuz rocket to launch a Soyuz manned transport spacecraft with a crew of three from Baikonur toward the International Space Station, ISS. (As of 2014)

Oct. 16: A Soyuz rocket to launch a Progress cargo ship from Baikonur toward the International Space Station, ISS. (As of 2014)

System activity

Dropped to %WINDOWS%\AppPatch\AcProtect.dll (SHA1: 994be9c340f57ba8cbb20b7ceedad49b00294f3e) and %WINDOWS%\AppPatch\msimain.mui (separate payload file).

Registered for startup with unusual autostart method, briefly touched in.[7]

A Microsoft patch file is dropped to %WINDOWS%\AppPatch\Custom\{099BF1AE-6A93-493D-0C48-2453E7FBC801}.sdband registered to load in HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB. That file loads AcProtect.dll as a library component.

The dumped payload shows similar functionality to what Plugx (or any other general purpose backdoor) has, but on a code level it is very different.

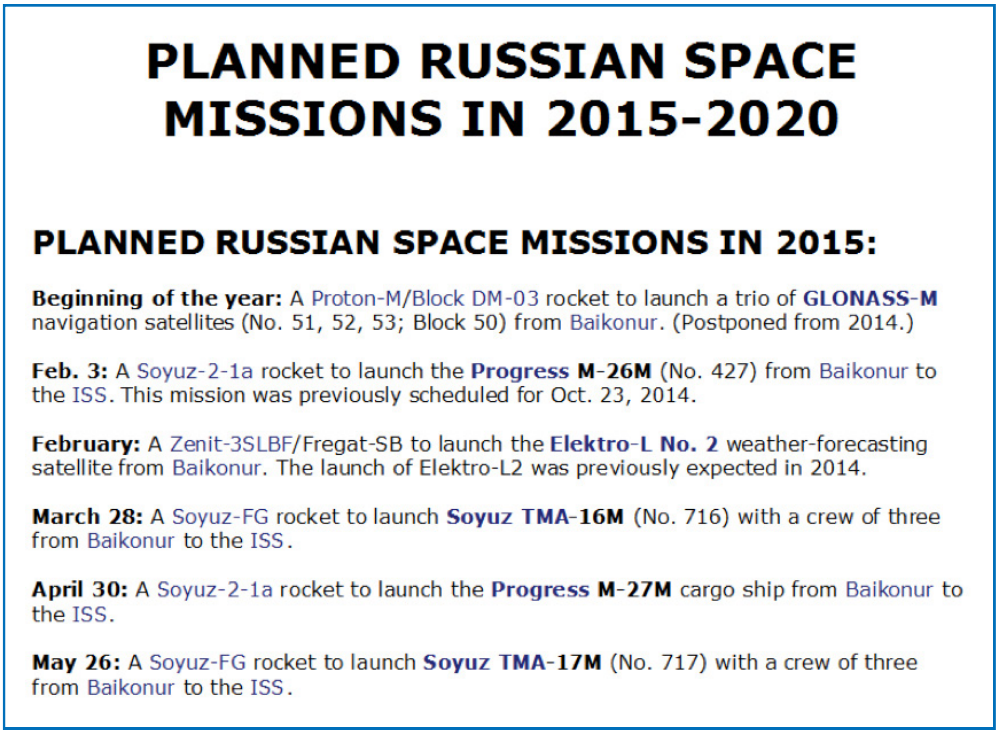
C&C servers

adobeflashupdate.dynu.com
Dynamic DNS service

transactiona.com
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: qiuping liu
Registrant Organization: huajiyoutian
Registrant Street: beijing
Registrant City: Beijing
Registrant State/Province: BJ
Registrant Postal Code: 100191
Registrant Country: CN
Registrant Phone: +86.1052810955
Registrant Phone Ext:
Registrant Fax: +89.1052810955
Registrant Fax Ext:
Registrant Email: yuminga1@126.com

systemupdate5.dtdns.com
Dynamic DNS service

9bc128f120996677d3c4f7c1d7506315b232e49e
Original name: **План космической деятельности на 2015-2020 год.doc**



PLANNED RUSSIAN SPACE MISSIONS IN 2015-2020

PLANNED RUSSIAN SPACE MISSIONS IN 2015:

Beginning of the year: A Proton-M/Block DM-03 rocket to launch a trio of **GLONASS-M** navigation satellites (No. 51, 52, 53; Block 50) from Baikonur. (Postponed from 2014.)

Feb. 3: A Soyuz-2-1a rocket to launch the **Progress M-26M** (No. 427) from Baikonur to the ISS. This mission was previously scheduled for Oct. 23, 2014.

February: A Zenit-3SLBF/Fregat-SB to launch the **Elektro-L No. 2** weather-forecasting satellite from Baikonur. The launch of Elektro-L2 was previously expected in 2014.

March 28: A Soyuz-FG rocket to launch **Soyuz TMA-16M** (No. 716) with a crew of three from Baikonur to the ISS.

April 30: A Soyuz-2-1a rocket to launch the **Progress M-27M** cargo ship from Baikonur to the ISS.

May 26: A Soyuz-FG rocket to launch **Soyuz TMA-17M** (No. 717) with a crew of three from Baikonur to the ISS.

System activity

Dropped to %PROFILE%\Local Settings\Temp\3.tmp; 64 bit malware components, refer to the same files names that are used by 0dfd883c1f205f0740d50688683f1869bcc0e9d7

C&C servers: N/A

Others

There were a few other samples, but all single.

Kamics :712df1f1f11f63e2154eb9023d584be62ef100b8

Original name: **N/A**

The dropped decoy document is a password protected Word file, content is not visible in the lack of the correct password.

System activity

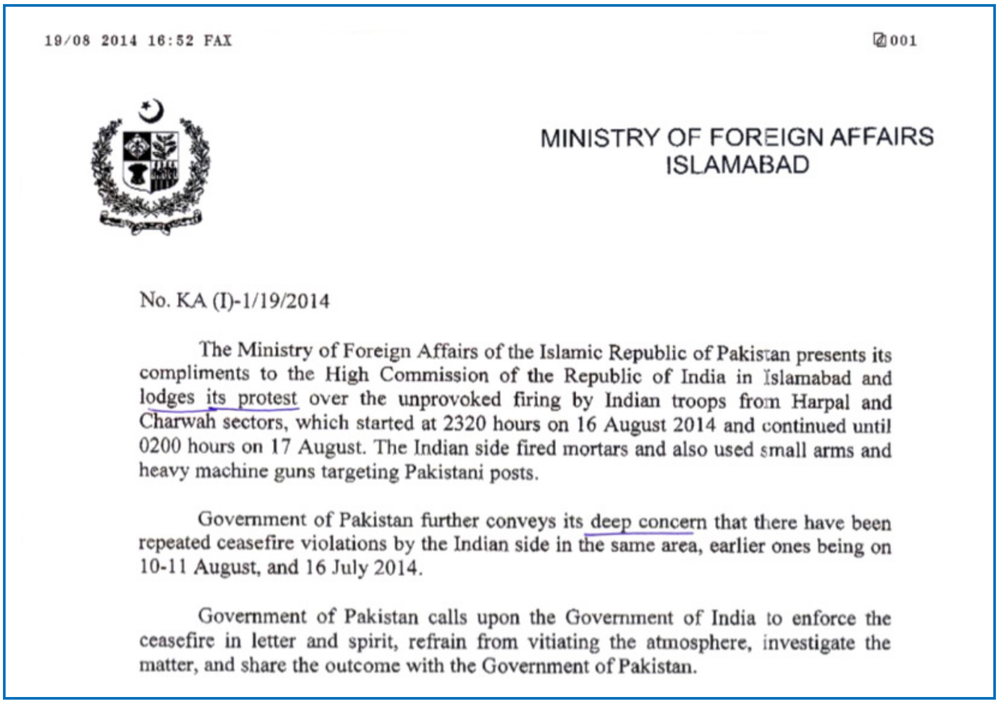
Dropped to %PROFILE%\Local Settings\Temp\msvcpdl100.dll (SHA1: 51346d70ea97a7aaef80f98c4891526443b2696c) and C:\MsBuild\Microsoft\Windows\System32\svchost.exe (SHA1: 2196770391bdbdd15bce5895427ec99b1bef0868); registered for startup in HKCU\Software\Microsoft\Windows\CurrentVersion\Run → Kaspersky Internet Security

C&C servers

buglaa.sportnewsa.net

Farfli: 960ac7329a6e80682959d6da0469921f8167e79a

Original name: **MoFA Note- Verbale on 19.8.14.doc**



19/08 2014 16:52 FAX 001

MINISTRY OF FOREIGN AFFAIRS
ISLAMABAD

No. KA (I)-1/19/2014

The Ministry of Foreign Affairs of the Islamic Republic of Pakistan presents its compliments to the High Commission of the Republic of India in Islamabad and lodges its protest over the unprovoked firing by Indian troops from Harpal and Charwah sectors, which started at 2320 hours on 16 August 2014 and continued until 0200 hours on 17 August. The Indian side fired mortars and also used small arms and heavy machine guns targeting Pakistani posts.

Government of Pakistan further conveys its deep concern that there have been repeated ceasefire violations by the Indian side in the same area, earlier ones being on 10-11 August, and 16 July 2014.

Government of Pakistan calls upon the Government of India to enforce the ceasefire in letter and spirit, refrain from vitiating the atmosphere, investigate the matter, and share the outcome with the Government of Pakistan.

System activity

Dropped to %PROFILE%\Application Data\winlog.exe (SHA1: 511f2055a56c0f458b1b14cc207730d0fe639df4) and %PROFILE%\Application Data\winlog.dll (SHA1: bb185efd35f7b4892a32e7853e044e94502a36af)

C&C servers

unisers.com

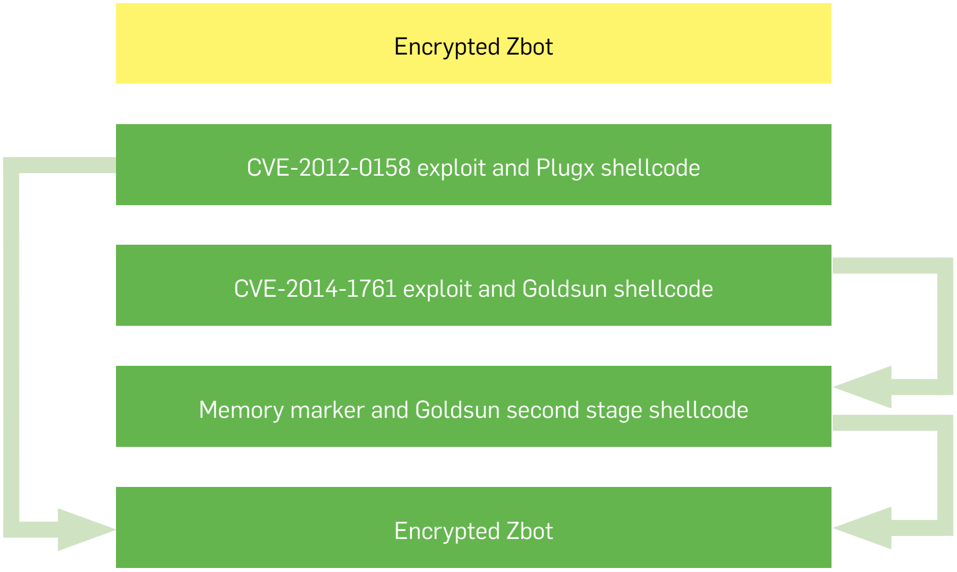
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: wang cheng
Registrant Organization: wang cheng
Registrant Street: BeijingDaguoROAD136
Registrant City: Beijing
Registrant State: Beijing
Registrant Postal Code: 100001
Registrant Country: CN
Registrant Phone: +86.01085452454
Registrant Fax: +86.01085452454
Registrant Email: bitumberls.@163.com

Successful integrations

But not all were failures. There were two samples that followed the above structure, and the Goldsun shellcode offset was fixed.

However, both samples were only dropping and executing a Chinese nationalized version of calc.exe – these are clearly test samples from China.

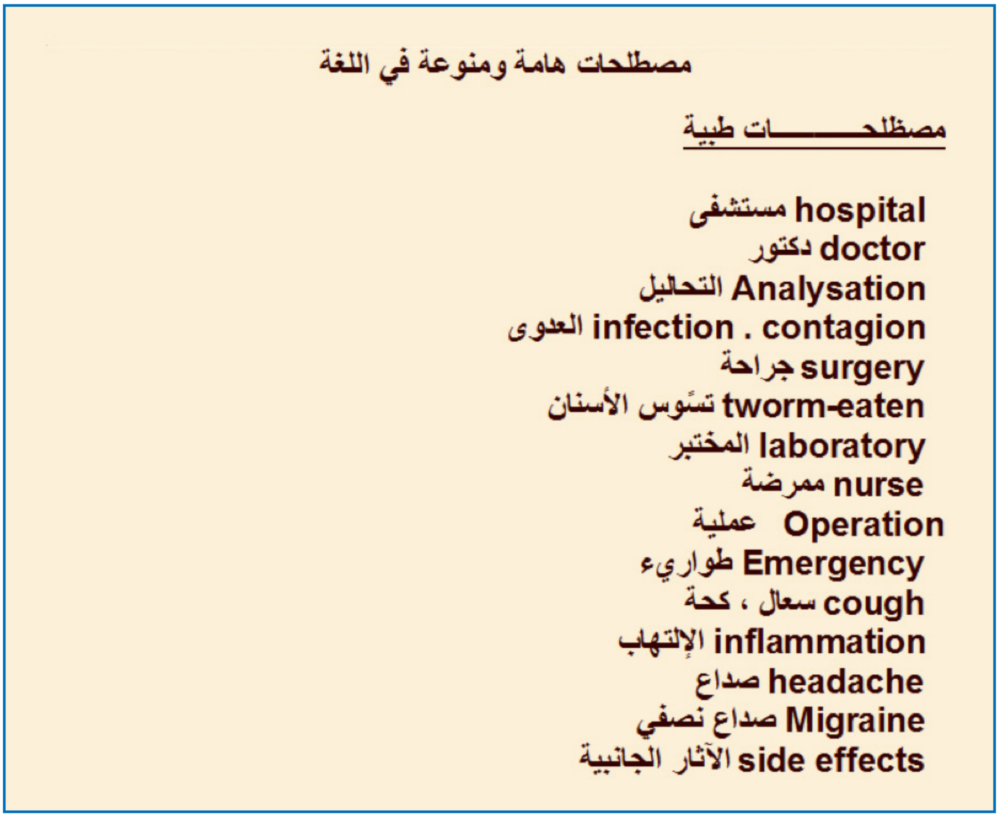
Furthermore, a couple of common malware samples were found with fixed second stage offsets, showing that at least these guys know what they are doing. Still, they kept the inactive encrypted Zbot at the beginning of the document.


Encrypted Zbot
CVE-2012-0158 exploit and Plugx shellcode
CVE-2014-1761 exploit and Goldsun shellcode
Memory marker and Goldsun second stage shellcode
Encrypted Zbot

Zbot

Among the samples conventional Zbots variants were also found. These showed up in Middle Eastern countries, and have Arabic themes as a decoy.

a44308788bbd189e532745a79d126feaf708c3cd
Original name: **مصطلحات عامة ومنوعة في اللغة.doc**



مصطلحات هامة ومنوعة في اللغة

مصطلحـــــــــات طبية

مستشفى	hospital
دكتور	doctor
التحاليل	Analysation
العدوى	infection . contagion
جراحة	surgery
تسَوس الأسنان	tworm-eaten
المختبر	laboratory
ممرضة	nurse
عملية	Operation
طواريء	Emergency
سعال ، كحة	cough
الإلتهاب	inflammation
صداع	headache
صداع نصفي	Migraine
الآثار الجانبية	side effects

System activity

Dropped to %PROFILE%\Application Data\Yhyq\sied.exe (random directory and filename); registered for startup in HKCU\Software\Microsoft\Windows\CurrentVersion\Run → Opagw

C&C servers

www.starorder.ezua.com

Dynamic DNS service

pop3.sec-homeland.com

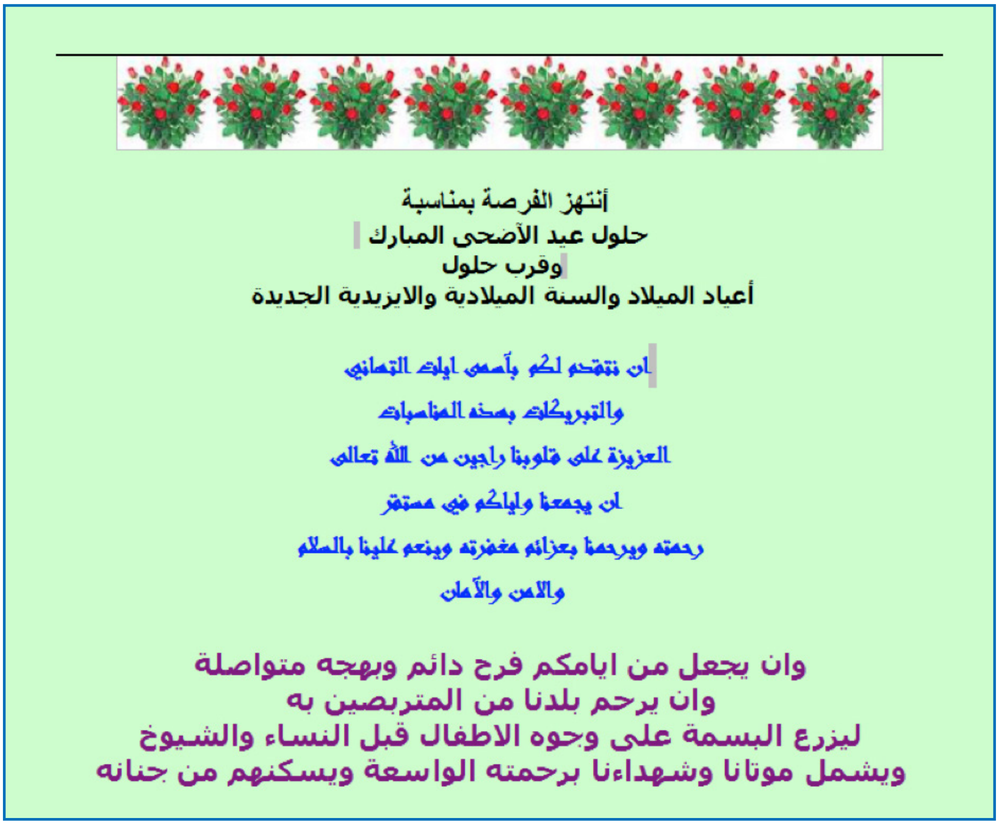
Domain Status: OK

Registry Registrant ID:
Registrant Name: dfhgewy
Registrant Organization: dfhgewy
Registrant Street: dfhgewy
Registrant City: Unknown City
Registrant State/Province: Unknown Province
Registrant Postal Code: 000000

Registrant Country: China
Registrant Phone: +086.0000 00000000
Registrant Phone Ext:
Registrant Fax: +086.0000 00000000
Registrant Fax Ext:
Registrant Email: joiupnhs@163.com

d05e586251b3a965b9c9af76568eff912e16432f

Original name: **تهنئة بعيد الاضحى المبارك.doc**



أنتهز الفرصة بمناسبة
حلول عيد الأضحى المبارك
وقرب حلول
أعياد الميلاد والسنة الميلادية والايزيدية الجديدة

ان نتقدم لكم بأسمى ايات التهاني
والتبريكات بهذه المناسبات
العزيزة على قلوبنا راجين من الله تعالى
ان يجمعنا واياكم في مستقر
رحمته ويرحمنا بعزائم مغفرته وينعم علينا بالسلام
والامن والآمان

وان يجعل من ايامكم فرح دائم وبهجه متواصلة
وان يرحم بلدنا من المتربصين به
ليزرع البسمة على وجوه الاطفال قبل النساء والشيوخ
ويشمل موتانا وشهداءنا برحمته الواسعة ويسكنهم من جنانه

System activity

Dropped to %PROFILE%\Application Data\Hysyt\ydbi.exe (random directory and filename); registered for startup in HKCU\Software\Microsoft\Windows\CurrentVersion\Run → Pecyiqu

C&C servers

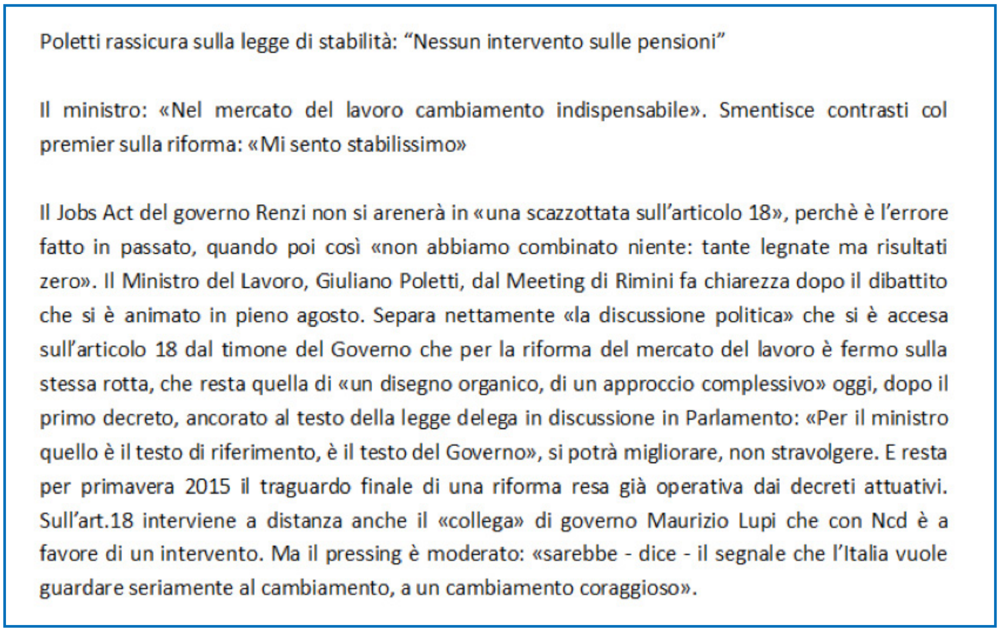
www.starorder.ezua.com

Dynamic DNS service
pop3.sec-homeland.com

Domain Status: OK
Registry Registrant ID:
Registrant Name: dfhgewy
Registrant Organization: dfhgewy
Registrant Street: dfhgewy
Registrant City: Unknown City
Registrant State/Province: Unknown Province

Registrant Postal Code: 000000
Registrant Country: China
Registrant Phone: +086.0000 00000000
Registrant Phone Ext:
Registrant Fax: +086.0000 00000000
Registrant Fax Ext:
Registrant Email: joiupnhs@163.com

Swrort: fa616b8e2f91810a8d036ba0adca6df50da2ad22
Original name: **test.doc**



Poletti rassicura sulla legge di stabilità: "Nessun intervento sulle pensioni"

Il ministro: «Nel mercato del lavoro cambiamento indispensabile». Smentisce contrasti col premier sulla riforma: «Mi sento stabilissimo»

Il Jobs Act del governo Renzi non si arenerà in «una scazzottata sull'articolo 18», perchè è l'errore fatto in passato, quando poi così «non abbiamo combinato niente: tante legnate ma risultati zero». Il Ministro del Lavoro, Giuliano Poletti, dal Meeting di Rimini fa chiarezza dopo il dibattito che si è animato in pieno agosto. Separa nettamente «la discussione politica» che si è accesa sull'articolo 18 dal timone del Governo che per la riforma del mercato del lavoro è fermo sulla stessa rotta, che resta quella di «un disegno organico, di un approccio complessivo» oggi, dopo il primo decreto, ancorato al testo della legge delega in discussione in Parlamento: «Per il ministro quello è il testo di riferimento, è il testo del Governo», si potrà migliorare, non stravolgere. E resta per primavera 2015 il traguardo finale di una riforma resa già operativa dai decreti attuativi. Sull'art.18 interviene a distanza anche il «collega» di governo Maurizio Lupi che con Ncd è a favore di un intervento. Ma il pressing è moderato: «sarebbe - dice - il segnale che l'Italia vuole guardare seriamente al cambiamento, a un cambiamento coraggioso».

System activity

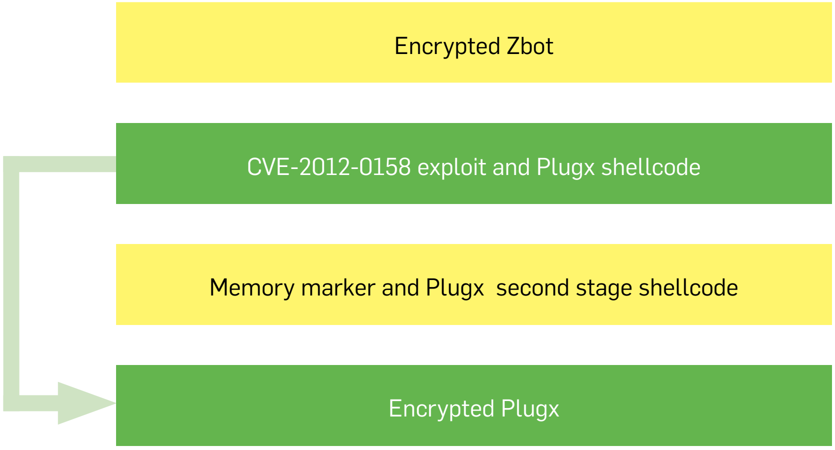
Dropped to %PROFILE%\Local Settings\Temp\3.tmp

C&C servers

Detour: Plugx

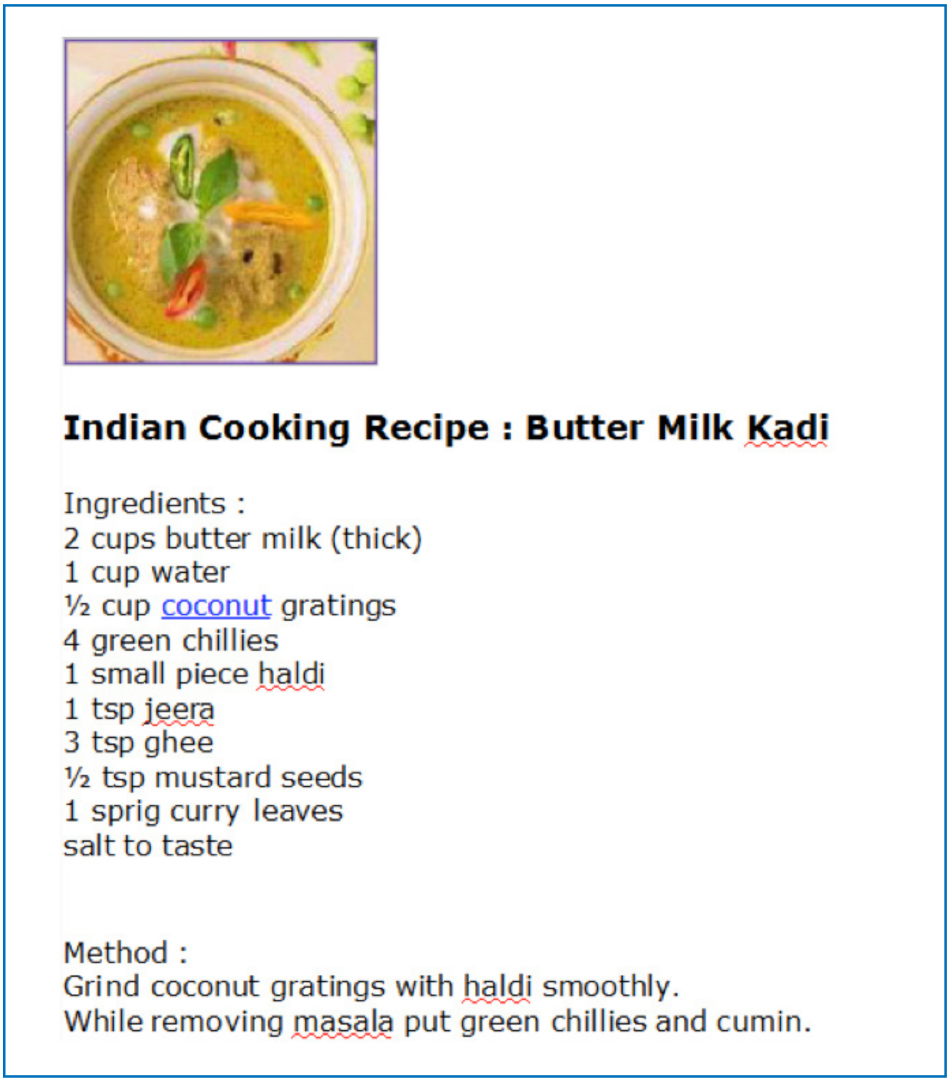
During the analysis of this campaign we ran into a handful of samples that have nothing to do with CVE-2014-1761, but they contained some of the encrypted Zbot at the beginning of the file. The end of encrypted PE is truncated, and the CVE-2012-0158 code is replaced with the Plugx shellcode.

Interestingly, there is another shellcode, which is starts with the same marker ("p!11") as the Goldsun second stage code, but the execution logic is the same as the Plugx shellcode. However, this shellcode just hangs in the air, no execution path leads to it. It is not clear, where these samples fit in the development path, could be that after the failure to integrate CVE-2014-1761, the corresponding part was simply ditched from the samples.


Encrypted Zbot
CVE-2012-0158 exploit and Plugx shellcode
Memory marker and Plugx second stage shellcode
Encrypted Plugx

6f845ef154a0b456afcf8b562a0387dabf4f5f85

Original name: **Indian Cooking Recipe.doc**



Indian Cooking Recipe : Butter Milk Kadi

Ingredients :
2 cups butter milk (thick)
1 cup water
½ cup coconut gratings
4 green chillies
1 small piece haldi
1 tsp jeera
3 tsp ghee
½ tsp mustard seeds
1 sprig curry leaves
salt to taste

Method :
Grind coconut gratings with haldi smoothly.
While removing masala put green chillies and cumin.

System activity

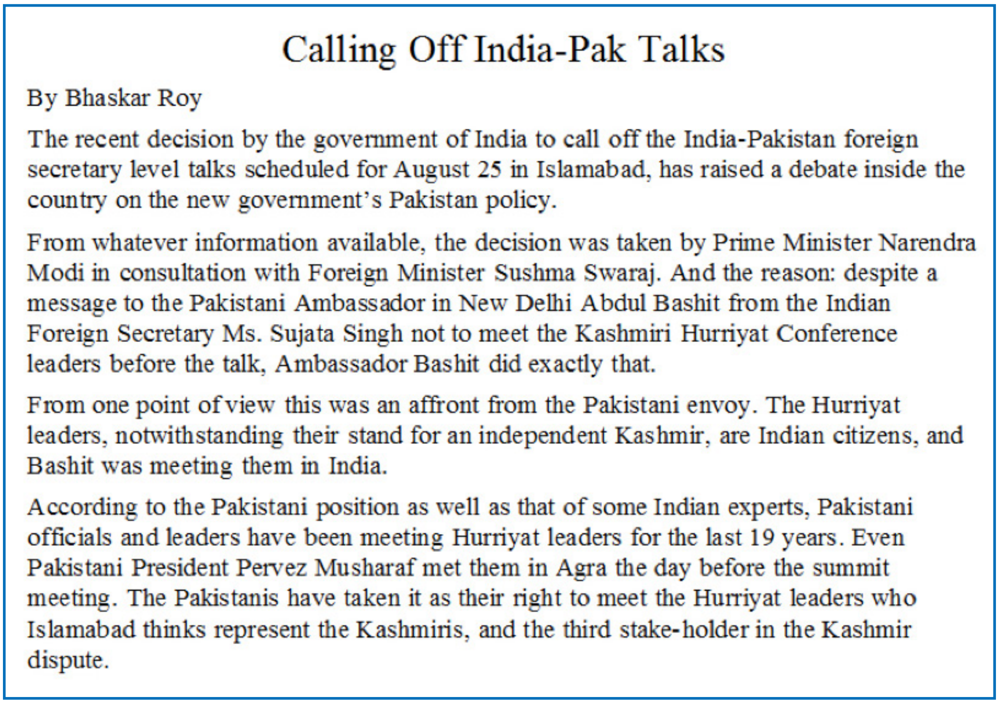
Dropped to C:\Documents and Settings\All Users\RasTls\RasTls.exe (clean loader digitally signed by Symantec), C:\Documents and Settings\All Users\RasTls\RasTls.dll (loader) and C:\Documents and Settings\All Users\RasTls\RasTls.dll.msc (payload); registered in HKLM\SYSTEM\CurrentControlSet\Services\RasTls → ImagePath

The payload is next generation Plugx,[4] plugin function creation dates are 0x20130524

C&C servers

supercat.strangled.net
Free domain sharing

a97827aef54e7969b9cbbec64d9ee81a835f2240
Original name: **Calling Off India-Pak Talks.doc**



Calling Off India-Pak Talks

By Bhaskar Roy

The recent decision by the government of India to call off the India-Pakistan foreign secretary level talks scheduled for August 25 in Islamabad, has raised a debate inside the country on the new government's Pakistan policy.

From whatever information available, the decision was taken by Prime Minister Narendra Modi in consultation with Foreign Minister Sushma Swaraj. And the reason: despite a message to the Pakistani Ambassador in New Delhi Abdul Bashit from the Indian Foreign Secretary Ms. Sujata Singh not to meet the Kashmiri Hurriyat Conference leaders before the talk, Ambassador Bashit did exactly that.

From one point of view this was an affront from the Pakistani envoy. The Hurriyat leaders, notwithstanding their stand for an independent Kashmir, are Indian citizens, and Bashit was meeting them in India.

According to the Pakistani position as well as that of some Indian experts, Pakistani officials and leaders have been meeting Hurriyat leaders for the last 19 years. Even Pakistani President Pervez Musharaf met them in Agra the day before the summit meeting. The Pakistanis have taken it as their right to meet the Hurriyat leaders who Islamabad thinks represent the Kashmiris, and the third stake-holder in the Kashmir dispute.

System activity

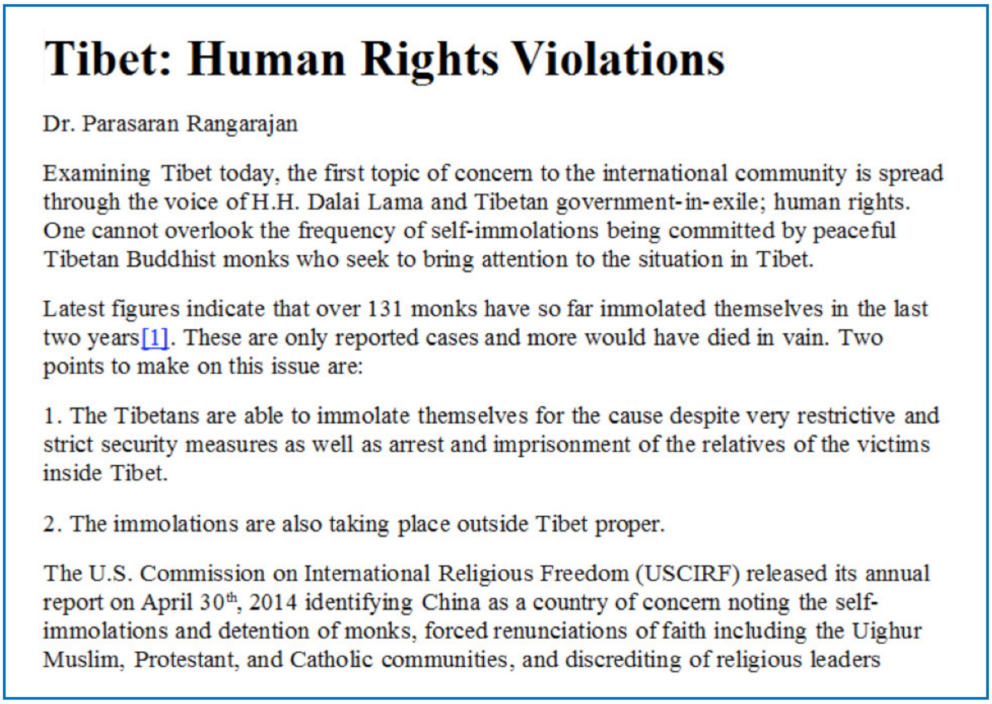
Dropped to C:\Documents and Settings\All Users\RasTls\RasTls.exe (clean loader digitally signed by Symantec), C:\Documents and Settings\All Users\RasTls\RasTls.dll (loader) and C:\Documents and Settings\All Users\RasTls\RasTls.dll.msc (payload); registered in HKLM\SYSTEM\CurrentControlSet\Services\RasTls → ImagePath

The payload is next generation Plugx,[4] plugin function creation dates are 0x20130524

C&C servers

nusteachers.no-ip.org
Dynamic DNS service

e8a29bb90422fa6116563073725fa54169998325
Original name: **Human Rights Violations of Tibet.doc**



Tibet: Human Rights Violations

Dr. Parasaran Rangarajan

Examining Tibet today, the first topic of concern to the international community is spread through the voice of H.H. Dalai Lama and Tibetan government-in-exile; human rights. One cannot overlook the frequency of self-immolations being committed by peaceful Tibetan Buddhist monks who seek to bring attention to the situation in Tibet.

Latest figures indicate that over 131 monks have so far immolated themselves in the last two years[1]. These are only reported cases and more would have died in vain. Two points to make on this issue are:

1. The Tibetans are able to immolate themselves for the cause despite very restrictive and strict security measures as well as arrest and imprisonment of the relatives of the victims inside Tibet.

2. The immolations are also taking place outside Tibet proper.

The U.S. Commission on International Religious Freedom (USCIRF) released its annual report on April 30th, 2014 identifying China as a country of concern noting the self-immolations and detention of monks, forced renunciations of faith including the Uighur Muslim, Protestant, and Catholic communities, and discrediting of religious leaders

System activity

Dropped to C:\Documents and Settings\All Users\RasTls\RasTls.exe (clean loader digitally signed by Symantec), C:\Documents and Settings\All Users\RasTls\RasTls.dll (loader) and C:\Documents and Settings\All Users\RasTls\RasTls.dll.msc (payload); registered in HKLM\SYSTEM\CurrentControlSet\Services\RasTls → ImagePath

The payload is next generation Plugx,[4] plugin function creation dates are 0x20130524.

C&C servers

ruchi.mysq1.net
Dynamic DNS service

19e9dfabdb9b10a90b62c12f205ff0d1eeef3f14

This is not a Plugx sample, but a Nineblog variant.[8]
Original name: ghozaresh amniyati.doc

System activity

Dropped to %PROFILE%\Application Data\Erease.vbe, that connects to the C&C server. The dropped decoy document is bogus, a truncated copy of the exploited document.

C&C servers:

www.freetimes.dns05.com
Dynamic DNS service

Conclusion

Apart from the lesson learned about malware development, what can we learn from this process?

The partially successful Plugx attempt raises a few questions. Should it be considered as a common cybercrime sample (as the dropped Zbot suggests) or as an APT (as Plugx does)? Actually, it depends on the patch level of the targeted computer.

The narrow line between APT and common malware shrank to zero with that sample. We have seen earlier[6] that authors of common malware are getting the idea of document-based exploitation from the APT players. Now it is swinging back – targeted attack players are snatching ideas from the other group. The fact that the attempt was less successful does not deny the fact that a symbiosis exists between the two distinct criminal groups, and ideas are floating in both directions.

References:

1. http://blog.malwaretracker.com/2013/06/tomato-garden-campaign-part-2-old-new.html
2. http://www.securelist.com/en/analysis/204792298/The_curious_case_of_a_CVE_2012_0158_exploit
3. https://www.virustotal.com/en-gb/file/3ba00f684daf0f9f2c1bef0934f1af73c7dabd44a13070b64de34c0754110aa3/analysis/
4. https://nakedsecurity.sophos.com/2014/06/30/from-the-labs-plugx-the-next-generation/
5. http://blog.9bplus.com/watching-attackers-through-virustotal/
6. https://nakedsecurity.sophos.com/2014/03/11/on-the-trail-of-advanced-persistent-threats/
7. http://www.arcticadv.com/free/ebook/pdf/sdb-explorer-exe-black-hat.html
8. http://www.fireeye.com/blog/technical/malware-research/2013/08/the-curious-case-of-encoded-vb-scripts-apt-nineblog.html

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

SOPHOS