The Rotten Tomato Campaign

By Gabor Szappanos, Principal Researcher, SophosLabs Hungary
# Contents

Overview | 2
---|---
Template 1: CVE-2012-0158 + CVE-2014-1761 Combo | 2
First attempt: Plugx | 3
Template 2: Goldsun | 4
Second attempts | 5
Plugx | 6
Appat | 10
Others | 12
Successful intergrations | 13
Detour: Plugx | 16
Conclusion | 20
References | 20
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.

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.

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, plugin function creation dates are 0x20130810.
The Rotten Tomato Campaign

C&C servers
chromeupdate.authorizeddns.org
Dynamic DNS service

google.support.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 (“pi11”), and jumps to the second stage, which then decrypts and executes the final Win32 payload.
The Rotten Tomato Campaign

**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**
- **Encrypted Plugx**
- **Blank**
- **CVE-2014-1761 exploit and Goldsun shellcode**
- **Memory marker and Goldsun second stage shellcode**
- **Start marker and encrypted Goldsun**

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.
The Rotten Tomato Campaign

There are a couple of problems with this implementation. First, the defunct 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.* 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,* plugin function creation dates are 0x20130810

**C&C servers**

**www.notebookhk.net**

<table>
<thead>
<tr>
<th>Registry Registrant ID:</th>
<th>Registrant Postal Code: 796373</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrant Name: lee stan</td>
<td>Registrant Country: HK</td>
</tr>
<tr>
<td>Registrant Organization: lee stan</td>
<td>Registrant Phone: +0.04375094543</td>
</tr>
<tr>
<td>Registrant Street: xianggangdiqu</td>
<td>Registrant Fax: +0.04375094543</td>
</tr>
<tr>
<td>Registrant City: xianggangdiqu</td>
<td>Registrant Email: <a href="mailto:stanlee@gmail.com">stanlee@gmail.com</a></td>
</tr>
<tr>
<td>Registrant State: xianggang</td>
<td></td>
</tr>
</tbody>
</table>

80f965432ce872fc3592d9f907d5a4f66ab07f9c

Original name: Справка от 16.09.2014.doc
The Rotten Tomato Campaign

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, plugin function creation dates are 0x20130810.

C&C servers
dwm.dnsedc.com
Registry Registrant ID: Registrant Country: CN
Registrant Name: guping liu Registrant Phone: +86.1052810955
Registrant Organization: huajiyoutian Registrant Phone Ext:
Registrant Street: beijing Registrant Fax: +89.1052810955
Registrant City: Beijing Registrant Fax Ext:
Registrant State/Province: BJ Registrant Email: yuminga1@126.com
Registrant Postal Code: 100191

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.

176273806e6fe338123ff660e70145935bac77c3
Original name: P3HOME.doc
The Rotten Tomato Campaign

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

adobeflashupdate.dynu.com systemupdate5.dtdns.com
Dynamic DNS service Dynamic DNS service

4ad76ce333b38e5bd0d559e3d7640fa322e3cca6
Original name: 2014 Chairmanship_end.doc
The Rotten Tomato Campaign

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, 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 indiasceus.justdied.com
Dynamic DNS service Dynamic DNS service
The Rotten Tomato Campaign

**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: 994be9c9c340f57ba8cb20b7ceedad49b00294f3e) 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-0C48-2453E7FCB801}\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 Postal Code: 100191
Registry Registrant ID: Registrant Country: CN
Registry Registrant Name: qiuqing liu Registrant Phone: +86.1052810955
Registry Registrant Organization: huajiyoutian Registrant Phone Ext:
Registry Registrant Street: beijing Registrant Fax: +89.1052810955
Registry Registrant City: Beijing Registrant Fax Ext:
Registry Registrant State/Province: BJ Registrant Email: yuming1@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 Electro-L No. 2 weather-forecasting satellite from Baikonur. The launch of Electro-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 0df08883c1f205f0740d50688683f1869b0cc0e9d7

C&C servers: N/A
The Rotten Tomato Campaign

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\msvcpd110.dll (SHA1: 51346d70ea97a7aef80f98c4891526443b2696c) and C:\MsBuild\Microsoft\Windows\System32\svchost.exe (SHA1: 21967703911bd15bce5895427ec99b1be0888); registered for startup in HKCU\Software\Microsoft\Windows\CurrentVersion\Run → Kaspersky Internet Security

C&C servers

buglaa.sportnewsa.net

Farfl: 960ac7329a6e80682959d6da0469921f8167e79a
Original name: MoFA Note- Verbale on 19.8.14.doc

System activity

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

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: تَعَظِّمَة* يَمِينُ حقَّكَ وَهَذَا هِيَ مُتَحَدِّثَتُهُمْ.doc
The Rotten Tomato Campaign

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 Country: China
Registrant Name: dfhgewy Registrant Phone: +086.0000 00000000
Registrant Organization: dfhgewy Registrant Phone Ext:
Registrant Street: dfhgewy Registrant Fax: +086.0000 00000000
Registrant City: Unknown City Registrant Fax Ext:
Registrant State/Province: Unknown Province Registrant Email: joiupnhs@183.com
Registrant Postal Code: 000000

d05e586251b3a965b9c90f76568eff912e16432f
Original name: كرابملا ىحضالا ديعب ةئنهت.doc
The Rotten Tomato Campaign

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

C&C servers
www.starorder.ezua.com
Dynamic DNS service
pop3.sec-homeland.com

Domain Status: OK
Registry Registrant ID: Registrant Postal Code: 000000
Registrant Name: dfhgewy Registrant Country: China
Registrant Organization: dfhgewy Registrant Phone: +086.0000 00000000
Registrant Street: dfhgewy Registrant Phone Ext:
Registrant City: Unknown City Registrant Fax: +086.0000 00000000
Registrant State/Province: Unknown Province Registrant Fax Ext:
Registrant Email: joiupnhs@183.com

Swrort: fa616b8e2f91810a8d036ba0adco6df50da2ad22
Original name: test.doc
The Rotten Tomato Campaign

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.

6f845ef154a0b456afcf8b562a0387dabf4f5f85
Original name: Indian Cooking Recipe.doc
The Rotten Tomato Campaign

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, plugin function creation dates are 0x20130524

C&C servers
supercat.strangled.net
Free domain sharing

a97827aef54e7969b9cbbec64d9ee81a835f2240
Original name: Calling Off India-Pak Talks.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.
The Rotten Tomato Campaign

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, plugin function creation dates are 0x20130524

C&C servers
nusteachers.no-ip.org
Dynamic DNS service
e8a29bb704d270e61563073725fa5416998325
Original name: Human Rights Violations of Tibet.doc
The Rotten Tomato Campaign

Tibet: Human Rights Violations

Dr. Parasaaran 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,* plugin function creation dates are 0x20130524.

C&C servers
ruchi.mysq1.net
Dynamic DNS service

19e9dfabdb9b10a90b62c12f205f0d1eeef3f14
This is not a Plugx sample, but a Nineblog variant.*
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 shrunk to zero with that sample. We have seen earlier 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:
3. https://www.virustotal.com/en-gb/file/3ba00f684daf0f2c1bef09341af73c7dabd44a13070b164de3e3e0754110aa3/analysis/
5. http://blog.9bplus.com/watching-attackers-through-virustotal/