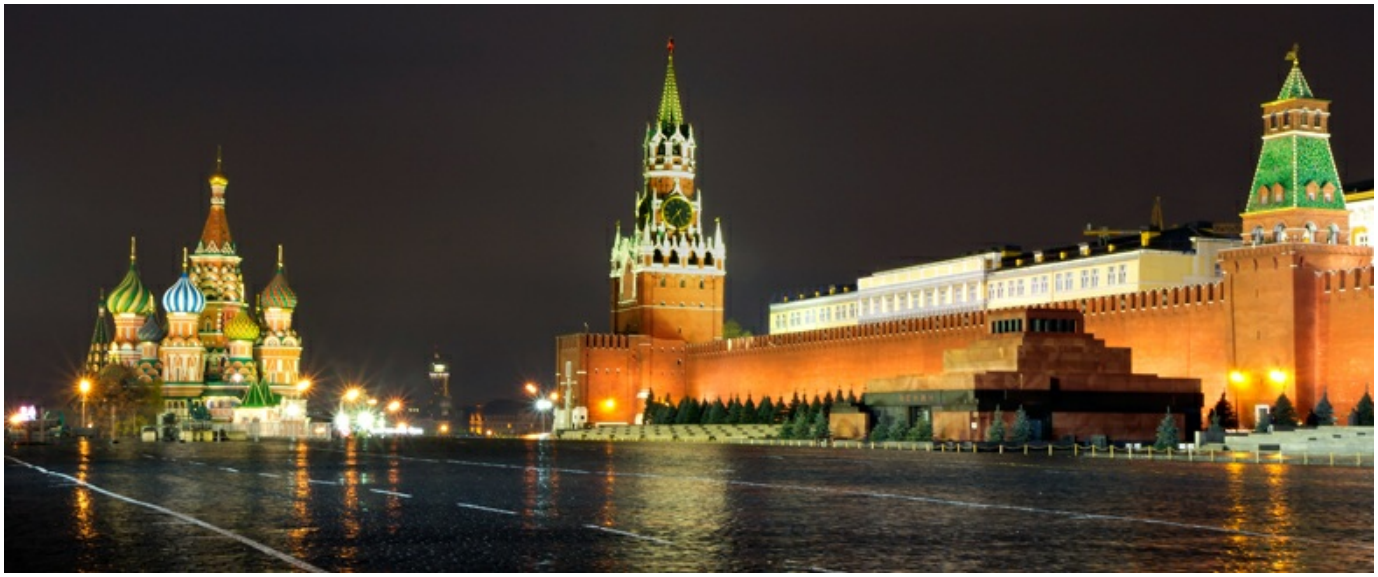
NetTraveler APT Targets Russian, European Interests

proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests



Overview

Throughout 2016, Proofpoint researchers tracked a cyber-espionage campaign targeting victims in Russia and neighboring countries. The actor utilizes spear phishing campaigns to deliver NetTraveler, also known as TravNet. First observed as early as 2004, NetTraveler is a Trojan used widely in targeted attacks. We believe that this attacker operates out of China. In addition to Russia, targeted regions include neighboring countries such as Mongolia, Belarus, and other European countries. The spear-phishing campaigns we detected use links to RAR-compressed executables and Microsoft Word attachments that exploit the CVE-2012-0158 vulnerability.

This particular APT is targeting organizations that include weapons manufacturers, human rights activists, and pro-democracy groups, among others.

Background

Previously we described activity by the same actor "In Pursuit of Optical Fibers and Troop Intel" [2] in which this group utilized PlugX malware to target various telecommunication and military interests in Russia. Since January 2016, this group switched to using NetTraveler and varied its targets, but otherwise left most of its tools, techniques, and procedures (TTPs) unchanged. It is worth noting that this and other China-based espionage groups have reduced their reliance on PlugX for unknown reasons, with only a few major incidents involving PlugX this year [5].

Moreover, there are some indications that this or a closely related group utilized Saker, Netbot, DarkStRat, and LURK0 Gh0st in its espionage activities. We previously mentioned this in our 2015 publication on PlugX. Palo Alto Networks also demonstrated links via tools and infrastructure used in these attacks in their MNKit [4] research, as did Kaspersky [1] and ESET [3] in their respective publications.

Spear-Phishing

One of this actor's favorite techniques is to register news and military lookalike sites and use them for Command and Control (C&C) and for payload hosting. Days prior to launching a wave of spear-phishing, the actor selects a victim-relevant news topic such as nuclear energy, military training, or geopolitics. The actor then finds a news article on the topic and uses it as a basis for the phishing lure, including file names, relevant decoy documents, image files, and email content.

For example, the actor emailed the URL www.info-spb[.]com/analiz/voennye_kommentaria/n148584.rar to potential victims in early February. The URL links to a RAR file which contains the executable “Нападение на американские космические системы очень дорого обойдется.scr” (“Attacking the American space systems will be very costly.scr”) and two benign decoy documents. One of these documents is shown in Figure 1 below:

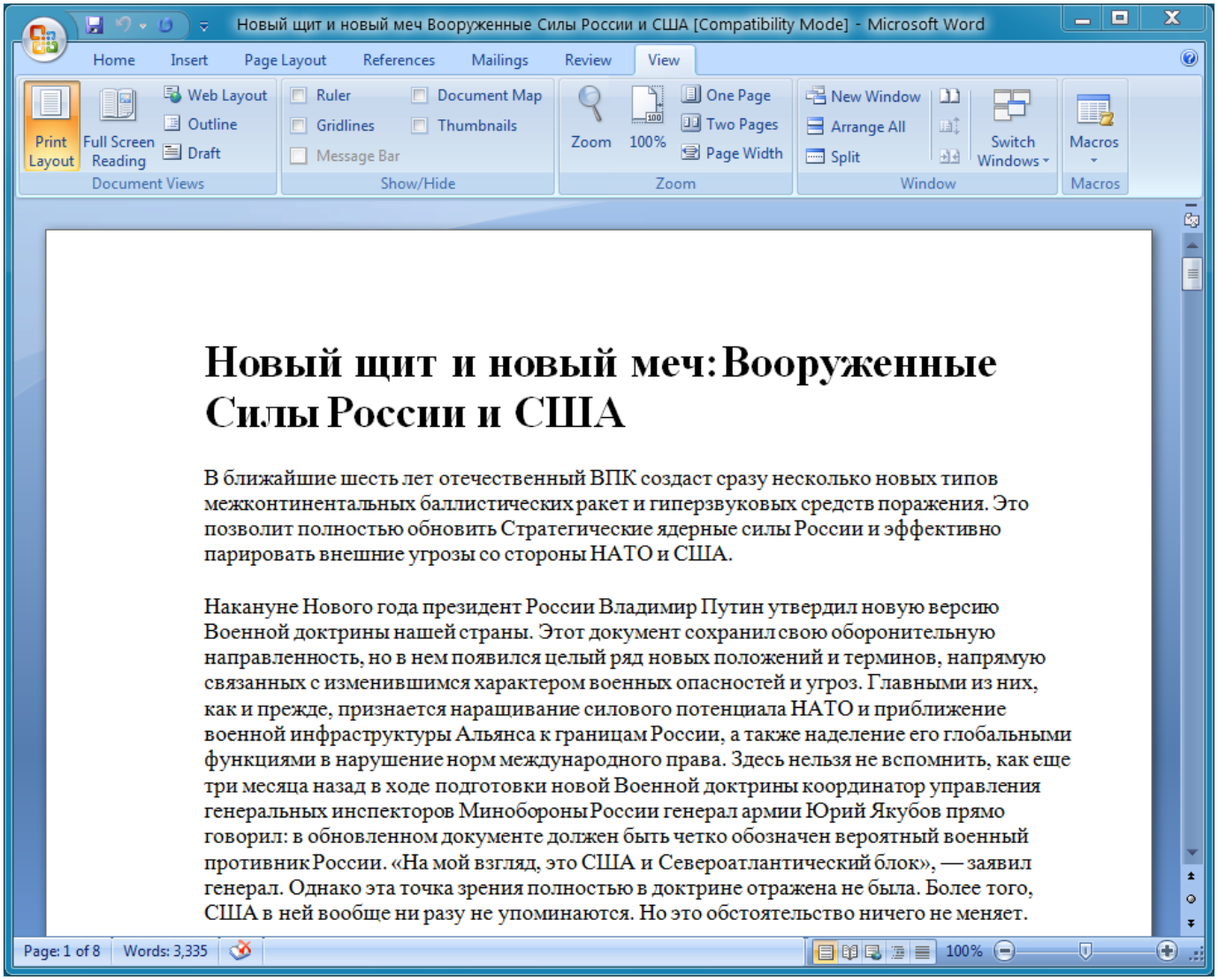


Figure 1: One of the decoy documents, “Новый щит и новый меч Вооруженные Силы России и США.doc” (“New Shield and Sword Armed forces of Russia and USA.doc”)

Figure 2 shows the legitimate news story that served as the basis for the spear-phishing lure.

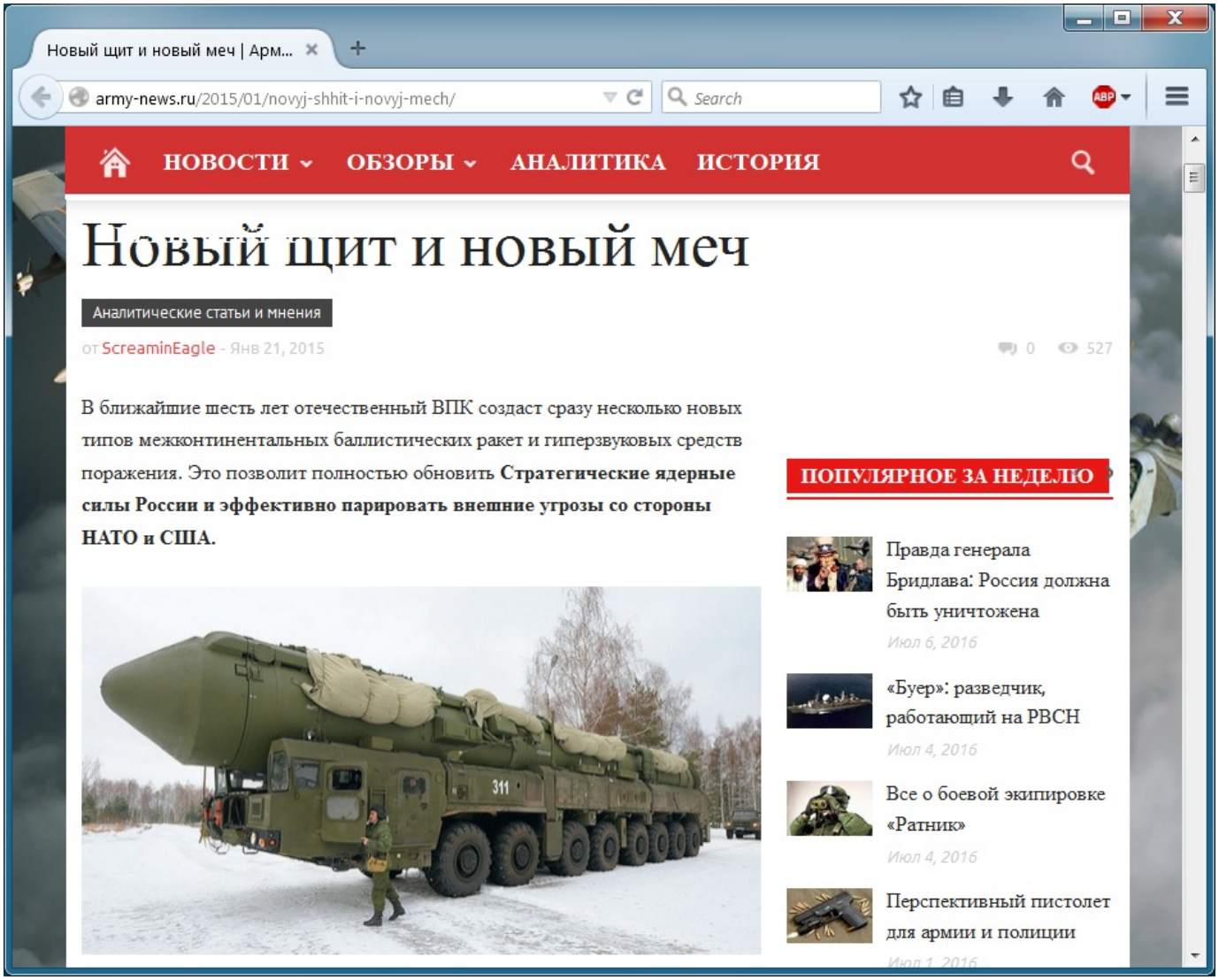


Figure 2: The decoy document copies the text of this legitimate news article that describes new Russian ICBMs [9]

The RAR archives hosted on look-alike domains always contain RAR SFX-packaged executables that drop and load NetTraveler. A sampling of the various filenames used for executables is provided below:

Indicators of Compromise (IOC)

Embedded Filename	Translation
Сервисное обслуживание и ремонт военной техники связи.scr	Service and repair of military communication equipment.scr
Нападение на американские космические системы очень дорого обойдется.scr	Attacking american space systems will be costly.scr
Текст приветствия Главы государства.scr	Text of speech of head of state.scr
Пятнадцатое заседание Коллегии Евразийской экономической комиссии.scr	Fifteenth session of Eurasian economic commission.scr
Совместное антитеррористическое учение «Антитеррор-2016».scr	Joint anti-terrorism training “Antiterror 2016”.scr
Встреча НГШ с Бордюжа.scr	Meeting of Chief of General Staff with Bordyuzh.scr
Изменения в списке аффилированных лиц по состоянию на 20.04.2016 г.scr	Changes to the list of affiliated persons for 20.04.2016.scr

Table 1: File names of executables inside RAR archives and their English translations

In some cases, instead of sending URLs in the spear-phishing emails, the attackers sent Microsoft Word attachments utilizing CVE-2012-0158 to exploit the client and install NetTraveler. These documents were built with MNKit, described in detail here [4] [6]. For example, the attachment “ПЛАН РЕАЛИЗАЦИИ ПРОЕКТА.doc” (which translates to “Plan of realization of project.doc”) was sent to potential victims in January 2016. As shown in Figure 3, various builder artifacts are visible in the document indicating the use of a builder.

```
<o:DocumentProperties>
 <o:Author>User123</o:Author>
 <o:LastAuthor>User123</o:LastAuthor>
 <o:Revision>4</o:Revision>
 <o:TotalTime>2</o:TotalTime>
 <o:Created>2012-05-01T14:08:00Z</o:Created>
 <o:LastSaved>2012-05-01T14:12:00Z</o:LastSaved>
 <o:Pages>44</o:Pages>
 <o:Words>17</o:Words>
 <o:Characters>101</o:Characters>
 <o:Lines>1</o:Lines>
 <o:Paragraphs>1</o:Paragraphs>
 <o:CharactersWithSpaces>117</o:CharactersWithSpaces>
 <o:Version>11.9999</o:Version>
</o:DocumentProperties>
```

Figure 3: MNKit builder artifacts in the exploit document, including a LastAuthor value of “User123”

Other Targeted Countries

Besides targeting Russia with NetTraveler, the actor also appears to have interests in Mongolia. While we do not have spear-phishing emails for these samples, we found certain payloads using Mongolian lures and decoys. For example, the file 13_11.rar found on March 11 contains a NetTraveler payload with a Mongolian file name “НИЙГМИЙН ДААТГАЛЫН ЕРӨНХИЙ ГАЗАР.exe” (“Social Insurance General Gazar.exe”) and a decoy PDF file with the same name. The C&C for this sample, www.mogoogle[.]com, resolved to the IP address 103.231.184[.]164, where the last octet of the IP is only 1 number larger than the IP address used for NetTraveler payloads with Russian targeting.

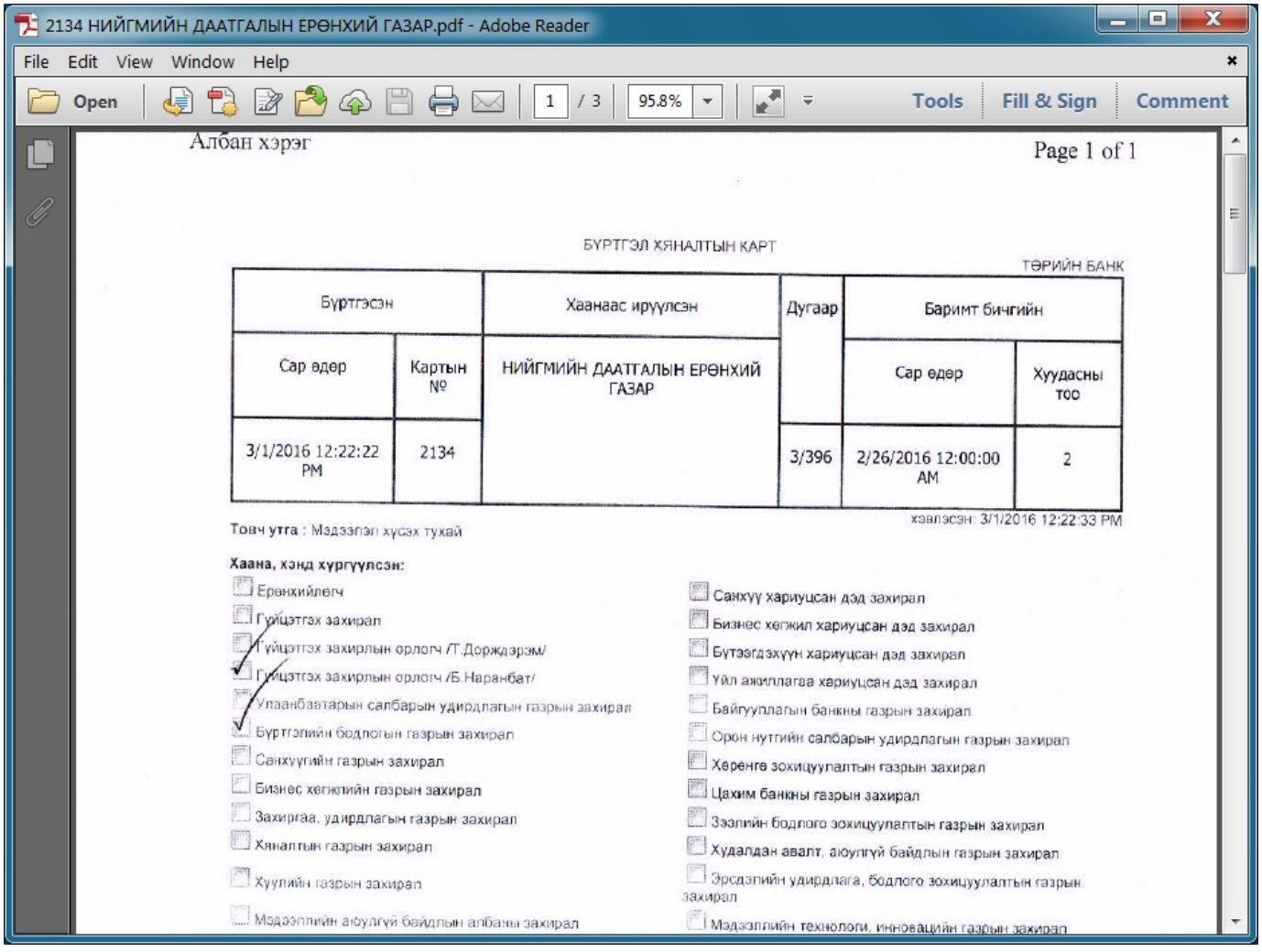


Figure 4: Decoy PDF used with the Mongolian-targeting NetTraveler payload

Another sample found April 20 with a Russian filename “Главный редактор Sputnik–Турция в среду вернется в Москву.rar” (“Main editor of Sputnik-Turkey will return to Moscow on Wednesday.doc.scr”) containing a NetTraveler payload with a decoy JPG file. The image file is a picture of a Turkish-language “Unacceptable forms of passenger information” form. This sample reuses the C&C domain www.mogoogle[.]com. The decoy in this sample was based on an RIA (a Russian language news agency) news article that appeared on the same day describing how the editor for the Turkish branch of a major Russian news source, Sputnik, was not allowed to enter Turkey during the height of the Russia-Turkey plane-downing dispute [7]. This payload could have been sent to Russian or Turkish individuals.

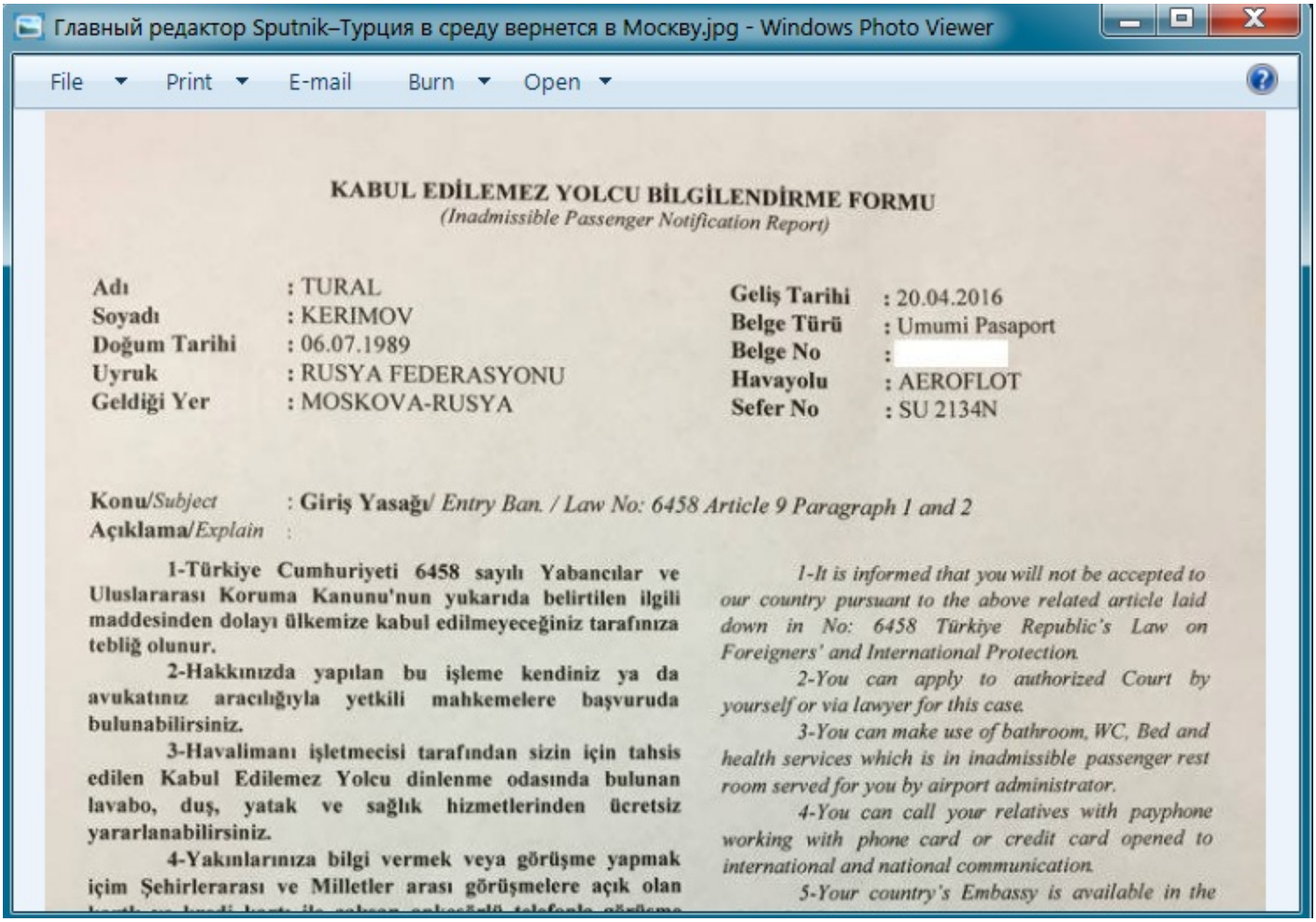


Figure 5: Decoy JPG used with the Russia/Turkey NetTraveler payload

Another sample found on March 13 included a Russian file name “Совместное антитеррористическое учение «Антитеррор-2016».rar” (“Joint anti-terrorism training “Antiterror 2016”.scr”) and contains a NetTraveler payload with C&C www.voennovosti[.]com. The file name for this sample capitalizes on a Belarusian news article [8] describing anti-terror exercises in Minsk, Belarus, by participating Commonwealth of Independent States countries (CIS). This payload could have been sent to a national of participating countries such as Belarus, Russia, or Ukraine.

Infrastructure

The following table summarizes the C&C and payload hosting domains used throughout the year.

Infection Site	Registrant Email	Legitimate Site Mimicked
www.tassnews[.]net	ghjksd@gmail.com	tass.ru (Major Russian news agency)
www.interfaxru[.]com	ganh@gmail.com	www.interfax.ru (Russian non-government news agency)
www.riaru[.]net	fjknge@yahoo.com	Ria.ru (State-operated domestic Russian news agency)
www.voennovosti[.]com	ukdf@gmail.com	voennovosti.ru (Military news of Russia)
www.info-spb[.]com	kefj0943@yahoo.com	Unknown (Possibly an acronym for St. Petersburg, a major city in Russia)
www.mogoogle[.]com	rubiya@163.com	Unknown (Possibly a word combination of Mongolia and Google)

All the domains (except mogoogle[.]com) were set up with the same registrar in Beijing referred to as “Shanghai Meicheng Technology Information Development Co., Ltd.”. Other than the emails, information used for registration was randomized. On the infrastructure side, the similarities to the 2015 PlugX campaign we described in “In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia” include:

- Registration using “Shanghai Meicheng Technology Information Development Co., Ltd.”
- Use of 4 - 6 letter Yahoo or Gmail registrant accounts
- Use of fake C&C domains that mimic major news sites or military forums
- IP address 98.126.38[.]107 resolved to domains used in both 2015 (including patriotp[.]com) and 2016 campaigns (such as www.voennovosti[.]com)

NetTraveler Analysis

NetTraveler implants continue to use a DLL side-loading technique. The payloads described here used the clean, signed executable fsguidll.exe (F-secure GUI component) to sideload fslapi.dll or the clean, signed executable RasTls.exe to sideload rastls.dll.

The configuration file used by NetTraveler uses a known format. For example, the payload dropped by 20160623.doc (See IOC table) uses the following configuration, where U00P is a C&C server, K00P is a DES key composed of a string of repeated As, P00D is sleep time, and F00G is proxy setting. U00P and K00P are encrypted in the file using a simple algorithm. These values are contained in the dropped config.dat file. Additionally, MM1 through MM6 parameters (not shown below) are added after installation.

[OOOOOO]

U00P=hxxp://www.tassnews[.]net/revenge/dk/downloader.asp

K00P=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

P00D=5

F00G=True

Conclusion

Threat actors have been successfully using NetTraveler for cyber-espionage for over 10 years. Targets have ranged from government agencies to nuclear power installations. In this case, it appears that Chinese actors are targeting a variety of interests in Russia and neighboring countries, relying on spear-phishing attacks to drop NetTraveler on vulnerable machines. Regardless of the TTPs, this ongoing APT points to the staying power of NetTraveler and the need for ongoing vigilance and technological protections against advanced persistent threats. Even organizations without direct government ties are potential targets for these types of attacks as smaller agencies or contractors can serve as beachheads in larger campaigns against indirectly related targets.

References

[1] https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/

[2] https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

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

[4] http://researchcenter.paloaltonetworks.com/2016/06/unit42-recent-mnkit-exploit-activity-reveals-some-common-threads/

[5] http://asia.nikkei.com/Business/Companies/Known-virus-linked-to-China-behind-JTB-data-breach

[6] https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-office-exploit-generators-szappanos.pdf

[7] http://ria.ru/world/20160420/1415455030.html

[8] http://sputnik.by/defense_safety/20160524/1022738965.html

[9] http://army-news.ru/2015/01/novyj-shhit-i-novyj-mech/

Indicators of Compromise (IOC)

IOC	IOC Type	Description
www.interfaxru[.]com	Hostname	NetTraveler C&C and payload hosting site
www.info-spb[.]com	Hostname	NetTraveler C&C and payload hosting site
www.tassnews[.]net	Hostname	NetTraveler C&C
www.riaru[.]net	Hostname	NetTraveler C&C
www.voennovosti[.]com	Hostname	NetTraveler C&C
www.mogoogle[.]com	Hostname	NetTraveler C&C
103.231.184[.]164	IP	NetTraveler C&C
103.231.184[.]163	IP	NetTraveler C&C
98.126.38[.]107	IP	NetTraveler C&C

hxxp://www.interfaxru[.]com/html/rostechnologii/20160420.rar	URL	NetTraveler payload URL
hxxp://www.info-spb[.]com/analiz/voennye_kommentaria/n148584.rar	URL	NetTraveler payload URL
hxxp://www.info-spb[.]com/html/news/cout/Последний%20доклад.rar	URL	NetTraveler payload URL
hxxp://www.info-spb[.]com//worldnews/almaz-antey/no.15.02.2016.rar	URL	NetTraveler payload URL
hxxp://www.info-spb[.]com/worldnews/mfa/ua/2016-02-16.zip	URL	NetTraveler payload URL
hxxp://www.info-spb[.]com/worldnews/mfa/uz/03.02.2016.rar	URL	NetTraveler payload URL
5afcaca6f6dd6fb3bad26585f30870f71462c59e251cc76b0df5851ac2aa17de	SHA256	20160420.rar
67c994ad328cd3d8b954366b2baa5e643b31ed42280548eebbd0c30c53f9e37d	SHA256	Информация о перечне зон деятельности сетевой организации в 2016 г.rar
f3997f8269e4177342aec8816c28cfebaef17a86f22eef15d90b4f9e5b15d8e6	SHA256	20160330.rar
69527b0471c2effab2d21106556ace6bd501daf7758b2ebbf3b2780d6399ecbf	SHA256	Совместное антитеррористическое учение «Антитеррор-2016».rar
8e3e5b12f0964e73e4057610ce7a6aa25607c94536762128dabebf9ccfa667d4	SHA256	13_11.rar
1bcafa596c597868a179fe3d783b8c5bcd1b487d891b99cb90e76e8abd55a599	SHA256	Главный редактор Sputnik–Турция в среду вернется в Москву.rar
409bb7f9faf4b7dc168f71084edb695707f22a83a2e79b810a0b4a27966d78f1	SHA256	Текст приветствия Главы государства.rar
3adacca54c6fe4bb905e233e48dffd8f6d03078d3d2d309d40e2e67a04a70db1	SHA256	n148584.rar
80ba8997067025dd830d49d09c57c0dcb1e2f303fa0e093069bd9cff29420692	SHA256	20160623.doc
60386112fc4b0ddb833fc9a877a9a4f0fe76828ebab4457637b0827106b269fe	SHA256	20160607.doc
b3a5c562e3531fb8be476af4947eaa793a77cc61715284bfb9c380b7048da44a	SHA256	ПЛАН РЕАЛИЗАЦИИ ПРОЕКТА.doc

Select ET Signatures that would fire on such traffic:

2816649 || ETPRO TROJAN Win32.TravNet.C HTTP Checkin