Symantec

# SECURITY RESPONSE

# Dragonfly: Cyberespionage Attacks Against Energy Suppliers

**Symantec Security Response**

Version 1.21: July 7, 2014, 12:00 GMT

> “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.”

Follow us on Twitter
@threatintel

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

Symantec

# 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

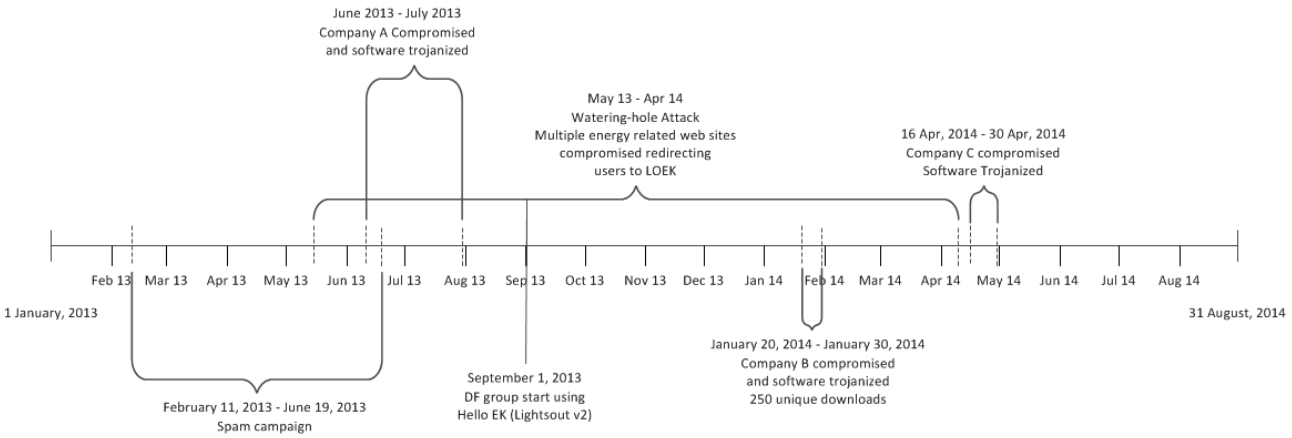


*Figure 1. Timeline of Dragonfly operations*

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.

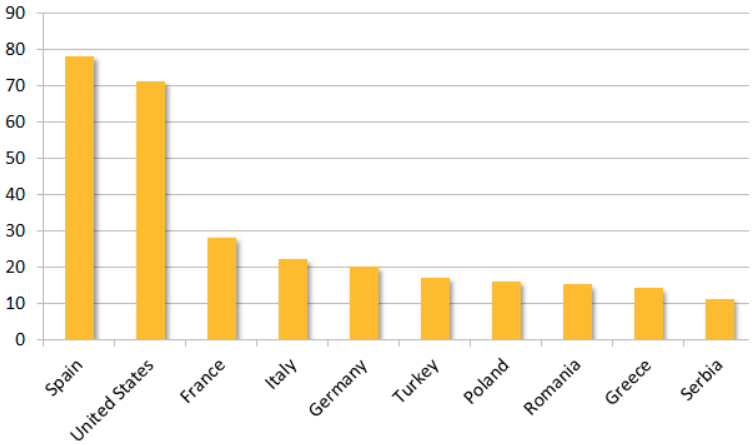


*Figure 2. Top 10 countries by active infection*

The most active infections, as in Figure 2, are

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.

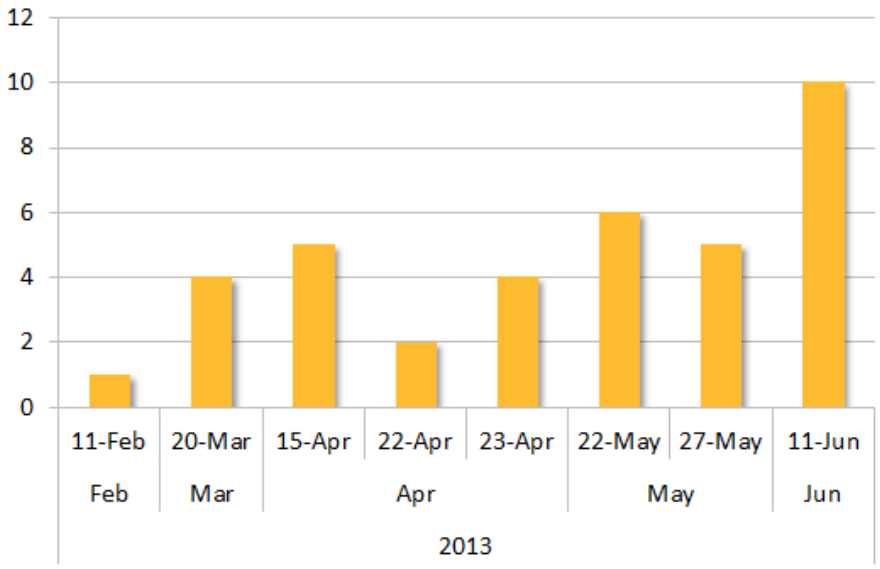


*Figure 3. Spam campaign activity from mid-February 2014 to mid-June 2013*

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.

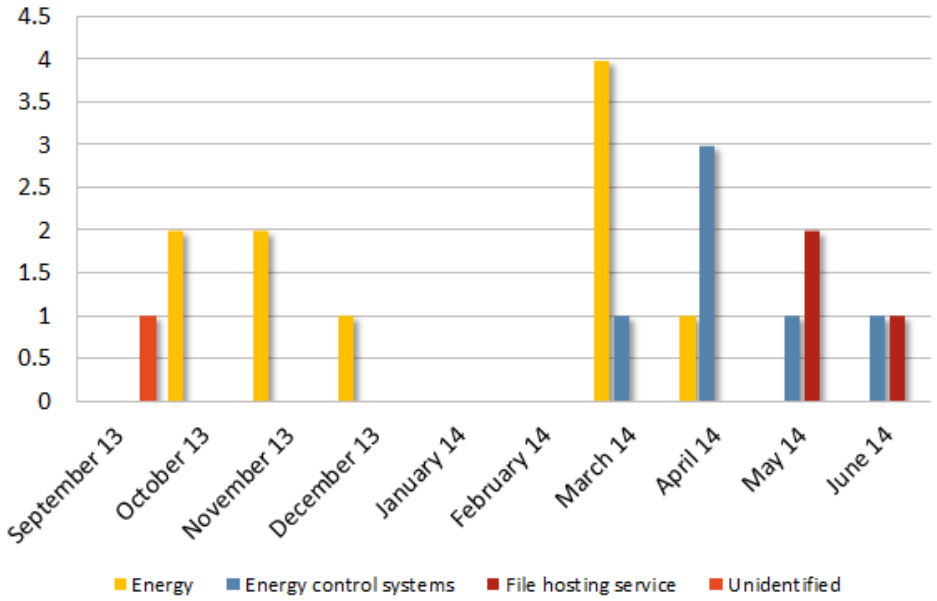


*Figure 4. Targeted industries over time*

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.

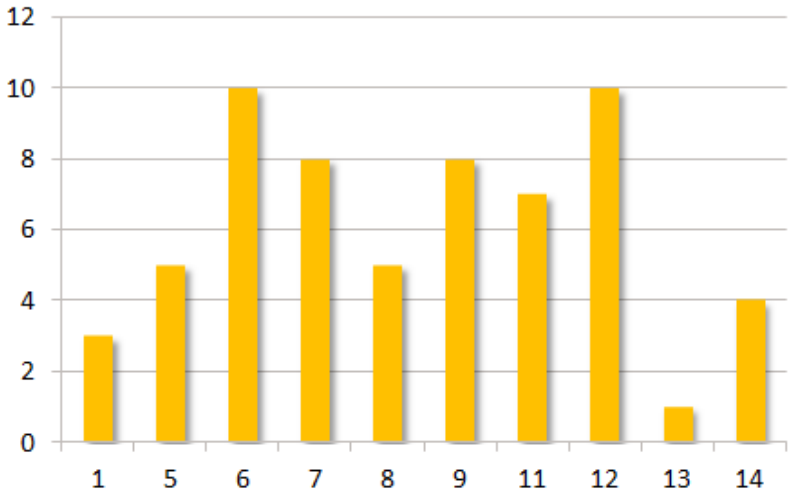


*Figure 5. Number of samples compiled per hour, UTC time zone*

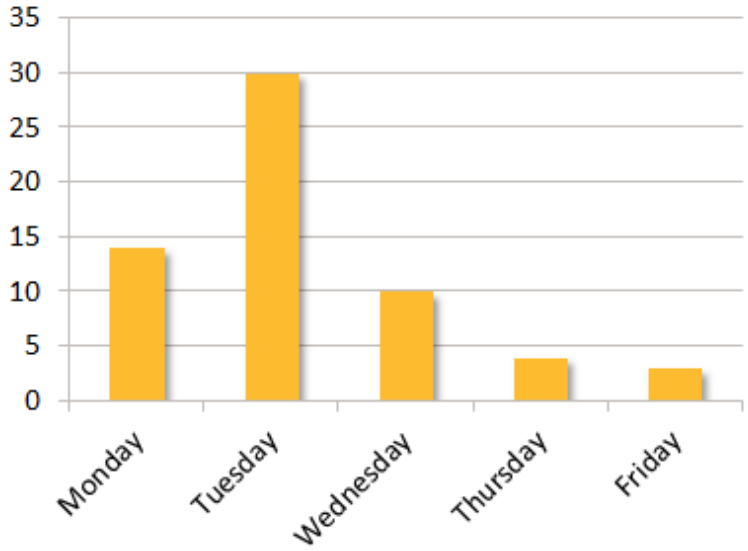


*Figure 6. Number of samples compiled per day, UTC time zone*

# 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.