+7
7 Votes

Symantec Official Blog

Dragonfly: Western Energy Companies Under Sabotage Threat

Cyberespionage campaign stole information from targets and had the capability to launch sabotage operations.

By: **Symantec Security Response (/connect/user/symantec-security-response)** SYMANTEC EMPLOYEE

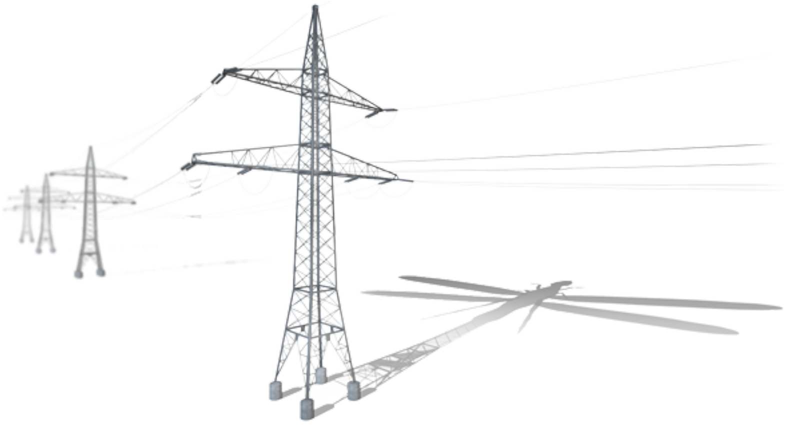
Created 30 Jun 2014 | 0 Comments

: Français (/connect/fr/blogs/dragonfly-les-entreprises-occidentales-du-secteur-de-lenergie-face-un-risque-de-cyber-sabotage), Deutsch (/connect/de/blogs/dragonfly-westliche-energieunternehmen-durch-sabotage-bedroht), Italiano (/connect/blogs/dragonfly-le-aziende-energetiche-occidentali-sotto-la-minaccia-di-sabotaggio), 日本語 (/connect/ja/blogs/dragonfly-0), 한국어 (/connect/blogs/dragonfly), Português (/connect/blogs/dragonfly-empresas-de-energia-ocidentais-sob-ameaca-de-sabotagem), Русский (/connect/blogs/dragonfly-zapadnye-energeticheskie-kompanii-nakhodyatsya-pod-ugrozoi-sabotazha), Español (/connect/es/blogs/dragonfly-amenaza-de-sabotaje-dirigida-empresas-de-servicios-energeticos-occidentales), Türkçe (/connect/blogs/dragonfly-batili-enerji-sirketleri-sabotaj-tehdidi-altinda)

0 64

(http://en-us.reddit.com/submit?url=http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear)

(/connect/forward?path=node/3187841)



An ongoing 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 energy supplies in affected countries.

Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

The Dragonfly group is well resourced, with a range of malware tools at its disposal and is capable of launching attacks through a number of different vectors. Its most ambitious attack campaign saw it compromise a number of industrial control system (ICS) equipment providers, infecting their software with a remote access-type Trojan. This caused companies to install the malware when downloading software updates for computers running ICS equipment. These infections not only gave the attackers a beachhead in the targeted organizations' networks, but also gave them the means to mount sabotage operations against infected ICS computers.

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

In addition to compromising ICS software, Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Backdoor.Oldrea (http://www.symantec.com/security_response/writeup.jsp?docid=2013-052817-2105-99) and Trojan.Karagany (http://www.symantec.com/security_response/writeup.jsp?docid=2010-121515-0725-99). The former appears to be a custom piece of malware, either written by or for the attackers.

Prior to publication, Symantec notified affected victims and relevant national authorities, such as Computer Emergency Response Centers (CERTs) that handle and respond to Internet security incidents.

Background

The Dragonfly group, which is also known by other vendors as Energetic Bear, appears to have been in operation since at least 2011 and may have been active even longer than that. Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus mainly to US and European energy firms in early 2013.

The campaign against the European and American energy sector quickly expanded in scope. The group initially began sending malware in phishing emails to personnel in target firms. Later, the group added watering hole attacks to its offensive, compromising websites likely to be visited by those working in energy in order to redirect them to websites hosting an exploit kit. The exploit kit in turn delivered malware to the victim's computer. The third phase of the campaign was the Trojanizing of legitimate software bundles belonging to three different ICS equipment manufacturers.

Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability. The group is able to mount attacks through multiple vectors and compromise numerous third party websites in the process. Dragonfly has targeted multiple organizations in the energy sector over a long period of time. Its current main motive appears to be cyberespionage, with potential for sabotage a definite secondary capability.

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. Based on this information, it is likely the attackers are based in Eastern Europe.

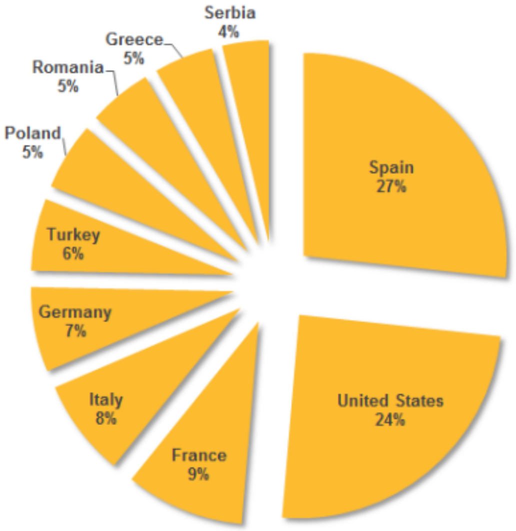


Figure. *Top 10 countries by active infections (where attackers stole information from infected computers)*

Tools employed

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.

Once installed on a victim's computer, Oldrea gathers system information, along with lists of files, programs installed, and root of available drives. It will also extract data from the computer's Outlook address book and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote command-and-control (C&C) server controlled by the attackers.

The majority of C&C servers appear to be hosted on compromised servers running content management systems, indicating that the attackers may have used the same exploit to gain control of each server. Oldrea has a basic control panel which allows an authenticated user to download a compressed version of the stolen data for each particular victim.

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 it for its own use. This version is detected by Symantec as Trojan.Karagany!gen1 (http://www.symantec.com/security_response/writeup.jsp?docid=2014-061601-3811-99).

Karagany is capable of uploading stolen data, downloading new files, and running executable files on an infected computer. It is also capable of running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloging documents on infected computers.

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.

Multiple attack vectors
The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest method was an email 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.

The spam campaign began in February 2013 and continued into June 2013. Symantec identified seven different organizations targeted in this campaign. The number of emails sent to each organization ranged from one to 84.

The attackers then shifted their focus to watering hole attacks, comprising a number of energy-related websites and injecting an iframe into each which redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. Lightsout exploits 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.

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. All three companies made equipment that is used in a number of industrial sectors, including energy.

The first identified Trojanized software was a product used to provide VPN access to programmable logic controller (PLC) type devices. The vendor discovered the attack shortly after it was mounted, but there had already been 250 unique downloads of the compromised software.

The second company to be compromised was a European manufacturer of specialist PLC type devices. In this instance, a software package containing a driver for one of its devices was compromised. Symantec estimates that the Trojanized software was available for download for at least six weeks in June and July 2013.

The third firm attacked was a European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure. Symantec believes that compromised software may have been available for download for approximately ten days in April 2014.

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.

Protection
Symantec has the following detections in place that will protect customers running up to date versions of our products from the malware used in these attacks:

Antivirus detections

- Backdoor.Oldrea (http://www.symantec.com/security_response/writeup.jsp?docid=2013-052817-2105-99)
- Trojan.Karagany (http://www.symantec.com/security_response/writeup.jsp?docid=2010-121515-0725-99)
- Trojan.Karagany!gen1 (http://www.symantec.com/security_response/writeup.jsp?docid=2014-061601-3811-99)

Intrusion Prevention Signatures

- Web Attack: Lightsout Exploit Kit (http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=27413)
- Web Attack: Lightsout Toolkit Website 4 (http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=27421)

For further technical details on the Dragonfly attacks, please read our whitepaper (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

Tags: Security (/connect/search?filters=im_vid_31:691), Endpoint Protection (/connect/product/endpoint-protection-vdi), Security Response (/connect/search?filters=im_vid_51:2261), energy sector (/connect/search?filters=im_vid_111:69971), high availability (/connect/search?filters=im_vid_111:5461), ICS (/connect/search?filters=im_vid_111:82841), sabotage (/connect/search?filters=im_vid_111:70001)

Subscriptions (0)

(/connect/user/symantec-security-response)

Symantec Security Response (/connect/user/symantec-security-response)

View Profile (/connect/user/symantec-security-response)

Login (/connect/user/login?destination=node%2F3187841) or Register (/connect/user/register?destination=node%2F3187841) to post comments.

About Your Community

A Message From Your Community Manager: RGMDonaldson (/connect/user/rgmdonaldson)

(/connect/user/rgmdonaldson)

Welcome to the Security Community on Symantec Connect.

The Security Community covers many different security products from Symantec and provides valuable technical information for each.

Please feel free to contact me via private message with any questions you may have.

I look forward to hearing from you and answering any questions about the Community.

Send a private message to the Community Manager (/connect/messages/new/4100651?destination=user%2F4100651)

Top 5 Contributors: All Time

MEMBER	REWARD POINTS
(/connect/user/riai) 𝓑𝓻í𝓪𝓷 (/connect/user/riai)	129651
(/connect/user/vikram-kumar-sav-sep) Vikram Kumar-SAV to SEP (/connect/user/vikram-kumar-sav-sep)	77376
(/connect/user/mithun-sanghavi) Mithun Sanghavi (/connect/user/mithun-sanghavi)	74094
(/connect/user/rafeeq) Rafeeq (/connect/user/rafeeq)	67639
(/connect/user/pk-1) P_K_ (/connect/user/pk-1)	53536

Top 5 Contributors: Last 30 Days

MEMBER	REWARD POINTS
(/connect/user/riai) 𝓑𝓻í𝓪𝓷 (/connect/user/riai)	775
(/connect/user/morgado) Morgado (/connect/user/morgado)	300
(/connect/user/brycenm) BrycenM (/connect/user/brycenm)	200
(/connect/user/aravind-ghosh) Aravind Ghosh (/connect/user/aravind-ghosh)	175
(/connect/user/dlp-solutions2) DLP Solutions2 (/connect/user/dlp-solutions2)	175

Trusted Advisors

MEMBER	ARTICLES	SOLVED
(/connect/user/mithun-sanghavi) Mithun Sanghavi (/connect/user/mithun-sanghavi)	61	1
(/connect/user/smlatcst) SMLatCST (/connect/user/smlatcst)	1	438
(/connect/user/jjesse) jjesse (/connect/user/jjesse)	24	108
(/connect/user/stephanefichet) stephane.fichet (/connect/user/stephanefichet)	7	151
(/connect/user/riai) 𝓑𝓻í𝓪𝓷 (/connect/user/riai)	25	2

know
Please take a minute to complete our Security Response survey. Click here.

(https://www.surveymonkey.com/r/G7KVZWQ)

Contact Us (/connect/contact) Privacy Policy (http://www.symantec.com/about/profile/policies/privacy.jsp) Earn Rewards (/connect/points) Rewards Terms and Conditions (/connect/blogs/symantec-connect-rewards-program-terms-and-conditions)

(https://twitter.com/symantec) (https://www.facebook.com/Symantec) (https://www.linkedin.com/company/symantec)