Dragonfly: Energy Companies Under Sabotage Threat

Symantec Security Response
What is Dragonfly?

- Ongoing cyberespionage campaign
- Targeting the energy sector in Europe and US
- Stealing information
- Capable of sabotage
Targets

• Electricity infrastructure
• Electricity generation
• Industrial equipment providers
• Petroleum pipeline operators
Target Locations

- Spain: 27%
- United States: 24%
- Serbia: 4%
- Greece: 5%
- Turkey: 6%
- Germany: 7%
- Italy: 8%
- France: 9%
- Poland: 5%
- Romania: 5%
The Dragonfly group

- In operation since at least 2011
- Initially targeted defense and aviation companies in the US and Canada
- Shifted focus to US and European energy firms in early 2013
- Priorities appear to be:
  - Persistent access to targets
  - Information stealing
  - Sabotage
- Has the hallmarks of state sponsored operation
- Appear to be operating in the UTC +4 time zone
Dragonfly employs three attack vectors

- Spam emails
- Watering hole attacks
- Compromising third party software
Spam campaign

- Generic spam emails sent to senior employees and engineers
- Began in February 2013 and continued into June 2013
- Emails bore one of two subject lines: “The account” or “Settlement of delivery problem”.
- Email disguised malware as PDF attachment
Watering hole attacks

• Group compromised legitimate websites related to energy sector
• Began in May 2013 and continued into April 2014
• Attacks redirected website visitors to other compromised legitimate websites hosting Lightsout Exploit Kit
• These sites dropped malware on to the victim’s computer.
Compromising third party software

• Three ICS equipment providers targeted
• Malware inserted into the software bundles they had made available for download on their websites
• Victims inadvertently downloaded “Trojanized” software when applying software updates
• By targeting suppliers, attackers found “soft underbelly” that provided a path into bigger companies
Timeline of recent attacks

- **February 11, 2013 - June 19, 2013**: Spam campaign
- **June 2013 - July 2013**: Company A compromised and software trojanized
- **May 13 - Apr 14**: Watering-hole Attack. Multiple energy-related websites compromised redirecting users to LOEK
- **January 20, 2014 - January 30, 2014**: Company B compromised and software trojanized. 250 unique downloads
Tools: Backdoor.Oldrea

- Remote access tool (RAT) type malware
- Custom malware, either written by the group itself or created for it
- Favoured tool: used in majority of attacks
- Acts as back door for attackers allowing them to extract data and install further malware
- Also known as Havex
Tools: Trojan.Karagany

- Was available on the underground market.
- Source code leaked in 2010
- Dragonfly appear to have modified it for its own use
- Capable of uploading stolen data, downloading new files and running executable files
- Can run plugins, for collecting passwords, taking screenshots, and cataloging documents on infected computers.
Protection

• Symantec customers are protected from malware variants mentioned in this report. Detections are made by Symantec products using antivirus, Insight and behavioral technologies such as SONAR.

• Symantec customers are protected from any attack using the exploits mentioned in this report when using Symantec products containing network threat protection/IPS technologies.

• Details on Symantec’s protection technologies can be found here: [http://www.symantec.com/page.jsp?id=star](http://www.symantec.com/page.jsp?id=star)
Summary

• Dragonfly is an ongoing threat
• Currently targeting energy sector in Europe and US
• Other sectors not immune, may be used as stepping stone
• Attacker capabilities
  – persistent access to networks
  – Information stealing
  – Sabotage
• Well resourced with a range of technical capabilities
• Likely to be state-sponsored
More Resources

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

Twitter
http://twitter.com/threatintel

Whitepapers
http://www.symantec.com/security_response/whitepapers.jsp
Dragonfly: Western Energy Companies Under Sabotage Threat