Dragonfly: Western energy sector targeted by sophisticated attack group

Summary: Resurgence in energy sector attacks, with the potential for sabotage, linked to re-emergence of Dragonfly cyber espionage group.

Author: Symantec Security Response

The energy sector in Europe and North America is being targeted by a new wave of cyber attacks that could provide attackers with the means to severely disrupt affected operations. The group behind these attacks is known as Dragonfly. The group has been in operation since at least 2011 but has re-emerged over the past two years from a quiet period following exposure by Symantec and a number of other researchers in 2014. This "Dragonfly 2.0" campaign, which appears to have begun in late 2015, shares tactics and tools used in earlier campaigns by the group.

The energy sector has become an area of increased interest to cyber attackers over the past two years. Most notably disruptions to Ukraine's power system in 2015 and 2016 were attributed to a cyber attack and led to power outages affecting hundreds of thousands of people. In recent months, there have also been media reports of attempted attacks on the electricity grids in some European countries, as well as reports of companies that manage nuclear facilities in the U.S. being compromised by hackers.

The Dragonfly group appears to be interested in both learning how energy facilities operate and also gaining access to operational systems themselves, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so. Symantec customers are protected against the activities of the Dragonfly group.

Dragonfly 2.0

Symantec has evidence indicating that the Dragonfly 2.0 campaign has been underway since at least December 2015 and has identified a distinct increase in activity in 2017.

Symantec has strong indications of attacker activity in organizations in the U.S., Turkey, and Switzerland, with traces of activity in organizations outside of these countries. The U.S. and Turkey were also among the countries targeted by Dragonfly in its earlier campaign, though the focus on organizations in Turkey does appear to have increased dramatically in this more recent campaign.

As it did in its prior campaign between 2011 and 2014, Dragonfly 2.0 uses a variety of infection vectors in an effort to gain access to a victim's network, including malicious emails, watering hole attacks, and Trojanized software.

The earliest activity identified by Symantec in this renewed campaign was a malicious email campaign that sent emails disguised as an invitation to a New Year's Eve party to targets in the energy sector in December 2015.

The group conducted further targeted malicious email campaigns during 2016 and into 2017. The emails contained very specific content related to the energy sector, as well as some related to general business concerns. Once opened, the attached malicious document would attempt to leak victims' network credentials to a server outside of the targeted organization.

In July, Cisco blogged about email-based attacks targeting the energy sector using a toolkit called Phishery. Some of the emails sent in 2017 that were observed by Symantec were also using the Phishery toolkit (Trojan.Phisherly), to steal victims' credentials via a template injection attack. This toolkit became generally available on GitHub in late 2016,

As well as sending malicious emails, the attackers also used watering hole attacks to harvest network credentials, by compromising websites that were likely to be visited by those involved in the energy sector.

The stolen credentials were then used in follow-up attacks against the target organizations. In one instance, after a victim visited one of the compromised servers, Backdoor.Goodor was installed on their machine via PowerShell 11 days later. Backdoor.Goodor provides the attackers with remote access to the victim's machine.

In 2014 Symantec observed the Dragonfly group compromise legitimate software in order to deliver malware to victims, a practice also employed in the earlier 2011 campaigns. In the 2016 and 2017 campaigns the group is using the evasion framework Shellter in order to develop Trojanized applications. In particular Backdoor.Dorshel was delivered as a trojanized version of standard Windows applications.

Symantec also has evidence to suggest that files masquerading as Flash updates may be used to install malicious backdoors onto target networks—perhaps by using social engineering to convince a victim they needed to download an update for their Flash player. Shortly after visiting specific URLs, a file named "install_flash_player.exe" was seen on victim computers, followed shortly by the Trojan.Karagany.B backdoor.

Typically the attackers will install one or two backdoors onto victim computers to give them remote access and allow them to install additional tools if necessary. Goodor, Karagany.B, and Dorshell are examples of backdoors used, along with Trojan.Heriplor.

Strong links with earlier campaigns

There are a number of indicators linking recent activity with earlier Dragonfly campaigns. In particular the Heriplor and Karagany Trojans used in Dragonfly 2.0 were both also used in the earlier Dragonfly campaigns between 2011 and 2014.

Trojan.Heriplor is a backdoor that appears to be exclusively used by Dragonfly, and is one of the strongest indications that the group that targeted the western energy sector between 2011 and 2014 is the same group that is behind the more recent attacks. This custom malware is not available on the black market, and has not been observed being used by any other known attack groups. It has only ever been seen being used in attacks against targets in the energy sector.

Trojan.Karagany.B is an evolution of Trojan.Karagany, which was previously used by Dragonfly, and there are similarities in the commands, encryption, and code routines used by the two Trojans. Trojan.Karagny.B doesn't appear to be widely available, and has been consistently observed being used in attacks against the energy sector. However, the earlier Trojan.Karagany was leaked on underground markets, so its use by Dragonfly is not necessarily exclusive.

Feature	Dragonfly (2013-2014)	Dragonfly 2.0 (2015-2017)	Link strength
Backdoor.Oldrea	Yes	No	None
Trojan.Heriplor (Oldrea stage II)	Yes	Yes	Strong
Trojan.Karagany	Yes	Yes (Trojan.Karagany.B)	Medium-Strong
Trojan.Listrix (Karagany stage II)	Yes	Yes	Medium-Strong
"Western" energy sector targeted	Yes	Yes	Medium
Strategic website compromises	Yes	Yes	Weak
Phishing emails	Yes	Yes	Weak
Trojanized applications	Yes	Yes	Weak

Table 1. Links between current and earlier Dragonfly cyber attack campaigns.

Potential for sabotage

Sabotage attacks are typically preceded by an intelligence-gathering phase where attackers collect information about target networks and systems and acquire credentials that will be used in later campaigns. The most notable examples of this are Stuxnet and Shamoon where previously stolen credentials were subsequently used to administer their destructive payloads.

The original Dragonfly campaigns now appear to have been a more exploratory phase where the attackers were simply trying to gain access to the networks of targeted organizations. The Dragonfly 2.0 campaigns show how the attackers may be entering into a new phase, with recent campaigns potentially providing them with access to operational systems, access that could be used for more disruptive purposes in future.

The most concerning evidence of this is in their use of screen captures. In one particular instance the attackers used a clear format for naming the screen capture files, [machine description and location].[organization name]. The string "cntrl" (control) is used in many of the machine descriptions, possibly indicating that these machines have access to operational systems.

Clues or false flags?

While Symantec cannot definitively determine Dragonfly's origins, this is clearly an accomplished attack group. It is capable of compromising targeted organizations through a variety of methods; can steal credentials to traverse targeted networks; and has a range of malware tools available to it, some of which appear to have been custom developed. Dragonfly is a highly focused group, carrying out targeted attacks on energy sector targets since at least 2011, with a renewed ramping up of activity observed in the last year.

Some of the group's activity appears to be aimed at making it more difficult to determine who precisely is behind it:

- The attackers used more generally available malware and "living off the land" tools, such as administration tools like PowerShell, PsExec, and Bitsadmin, which may be part of a strategy to make attribution more difficult. The Phisherly toolkit became available on Github in 2016, and a tool used by the group—Screenutil—also appears to use some code from CodeProject.
- The attackers also did not use any zero days. As with the group's use of publicly available tools, this could be an attempt to deliberately thwart attribution, or is could indicate a lack of resources,
- Some code strings in the malware were in Russian. However, some were also in French, which indicates that one of these languages may be a false flag.

Conflicting evidence and what appear to be attempts at misattribution make it difficult to definitively state where this attack group is based or who is behind it.

What is clear is that Dragonfly is a highly experienced threat actor, capable of compromising numerous organizations, stealing information, and gaining access to key systems. What it plans to do with all this intelligence has yet to become clear, but its capabilities do extend to materially disrupting targeted organizations should it choose to do so.

Protection

Symantec customers are protected against Dragonfly activity, Symantec has also made efforts to notify identified targets of recent Dragonfly activity.

Symantec has the following specific detections in place for the threats called out in this blog:

- Trojan.Phisherly
- Backdoor.Goodor
- Trojan.Karagany.B
- Backdoor.Dorshell
- Trojan.Heriplor
- Trojan.Listrix
- Trojan.Karagany

Symantec has also developed a list of Indicators of Compromise to assist in identifying Dragonfly activity:

FAMILY	MD5	COMMAND & CONTROL
Backdoor.Dorshell	b3b5d67f5bbf5a043f5bf5d079dbcb56	hxxp://103.41.177.69/A56WY
Trojan.Karagany.B	1560f68403c5a41e96b28d3f882de7f1	hxxp://37.1.202.26/getimage/622622.jpg
Trojan.Heriplor	e02603178c8c47d198f7d34bcf2d68b8	
Trojan.Listrix	da9d8c78efe0c6c8be70e6b857400fb1	
Hacktool.Credrix	a4cf567f27f3b2f8b73ae15e2e487f00	
Backdoor.Goodor	765fcd7588b1d94008975c4627c8feb6	
Trojan.Phisherly	141e78d16456a072c9697454fc6d5f58	184.154.150.66
Screenutil	db07e1740152e09610ea826655d27e8d	

Best Practices

- Dragonfly relies heavily on stolen credentials to compromise a network. Important passwords, such as those with high privileges, should be at least 8-10 characters long (and preferably longer) and include a mixture of letters and numbers. Encourage users to avoid reusing the same passwords on multiple websites and sharing passwords with others should be forbidden. Delete unused credentials and profiles and limit the number of administrative-level profiles created. Employ two-factor authentication (such as Symantec VIP) to provide an additional layer of security, preventing any stolen credentials from being used by attackers.
- Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.
- Implement and enforce a security policy whereby any sensitive data is encrypted at rest and in transit. Ensure that customer data is encrypted as well. This can help mitigate the damage of potential data leaks from within an organization.
- Implement SMB egress traffic filtering on perimeter devices to prevent SMB traffic leaving your network onto the internet.
- Educate employees on the dangers posed by spear-phishing emails, including exercising caution around emails from unfamiliar sources and opening attachments that haven't been solicited. A full protection stack helps to defend against emailed threats, including Symantec Email Security.cloud which can block email-borne threats and Symantec Endpoint Protection, which can block malware on the endpoint. Symantec Messaging Gateway's Disarm technology can also protect computers from threats by removing malicious content from attached documents before they even reach the user.