Operation Dragonfly Analysis Suggests Links to Earlier Attacks

By Christiaan Beek (https://securingtomorrow.mcafee.com/author/christiaan-beek/) and Raj Samani (https://securingtomorrow.mcafee.com/author/raj-samani/) on Dec 17, 2017 (https://securingtomorrow.mcafee.com/2017/12/)

On September 6, Symantec published details of the Dragonfly campaign, which targeted dozens of energy companies throughout 2017. This attack was effectively Dragonfly 2.0, an update to a campaign that began in 2014.

Moving beyond our 2014 analysis of Dragonfly, (https://securingtomorrow.mcafee.com/mcafee-labs/operation-dragonfly-imperils-industrial-protocol/) our current focus looks at the attack's indicators to determine whether we can glean any further information regarding the source and possible motivations of those behind the campaign. The campaign targets energy companies around the world by leveraging spear-phishing emails that, once successful, allow the attackers to download Trojan software. The Trojans provide access to the victims' systems and networks.

Going Beyond Energy

Although initial reports showed Dragonfly attacks targeting the energy sector, investigations by McAfee Labs and the Advanced Threat Research team uncovered related attacks targeting the pharmaceutical, financial, and accounting industries. Everything about this campaign points to a well-prepared assault that carefully considers each target, and conducts reconnaissance before taking any measures to exploit compromised targets.

We saw the group use several techniques to get a foothold in victims' networks, including spear phishing, watering holes, and exploits of supply-chain technologies via previous campaigns. By compromising well-established software vulnerabilities and embedding within them "backdoor" malware, the victims think they are installing software from a trusted vendor, while unaware of the supply-side compromise.

Once the attackers have a foothold, they create or gain user accounts to operate stealthily. Using the remote-desktop protocol to hop among internal or external systems, they connect either to a control server if the risk is minimal or use an internal compromised server to conduct operations.

The last wave of attacks used several backdoors and utilities. In analyzing the samples, we compared these with McAfee's threat intelligence knowledge base of attack artifacts.

One of the starting points was a Trojan in the 2017 campaign with the following hashes:

- MD5: da9d8c78efe0c6c8be70e6b857400fb1
- SHA-256: fc54d8afd2ce5cb6cc53c46783bf91d0dd19de604308d536827320826bc36ed9

Comparing this code, we discovered another sample from the group that was used in a July 2013 attack (https://cdn.securelist.com/files/2014/07/Kaspersky_Lab_crouching_yeti_appendixes_eng_final.pdf):

- MD5: 4bfdda1a5f21d56afdc2060b9ce5a170
- SHA-256: 07bd08b07de611b2940e886f453872aa8d9b01f9d3c61d872d6cfe8cde3b50d4
- Filename: fl.exe

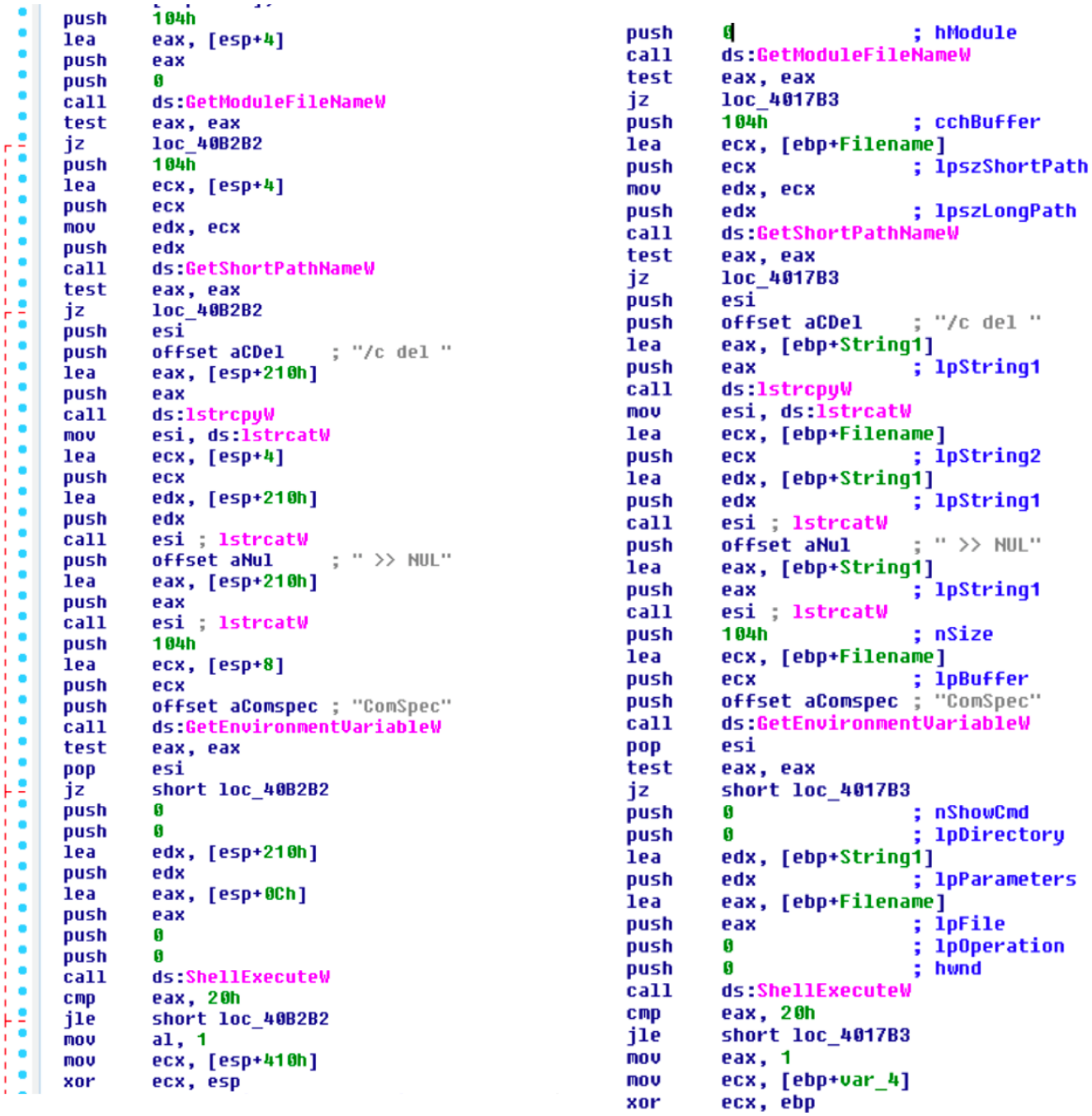
The file was downloaded after a Java exploit executed on the victim's machine, according to the 2013 attack report. After analyzing the 2013 sample, we noticed that some of the executable's resources were in Russian.

Comparing the code, we find the 2017 sample has a large percentage of the same code as the backdoor used in the 2013 attacks. Further, some code in the 2017 backdoor is identical to code in the application TeamViewer, a legitimate remote administration tool used by many around the world. By incorporating the code and in-memory execution, the attackers avoid detection and leave no trace on disk.

The correlating hash we discovered that contained the same TeamViewer code was reported by Crysys, a Hungarian security company. In their report on about "'TeamSpy," (http://www.crysys.hu/teamspy/teamspy.pdf) they mentioned the hash we correlated as well: 708ceccae2c27e32637fd29451aef4a5. This particular sample had the following compile date details: 2011:09:07 – 09:27:58+01:00

The TeamSpy attacks were originally aimed at political and human right activists living in the Commonwealth of Independent States (the former Soviet Union) and eastern European countries. Although the report attributes the attacks to a threat actor or actors and shared tactics and procedures, the motivations behind TeamSpy appear similar to those of the Dragonfly group. With identical code reuse, could the TeamSpy campaign be the work of Dragonfly?

But that's not all of interest. We also discovered that the 2017 sample contained code blocks associated with another interesting malware family: BlackEnergy. Let's look at an example of the code similarities we discovered:



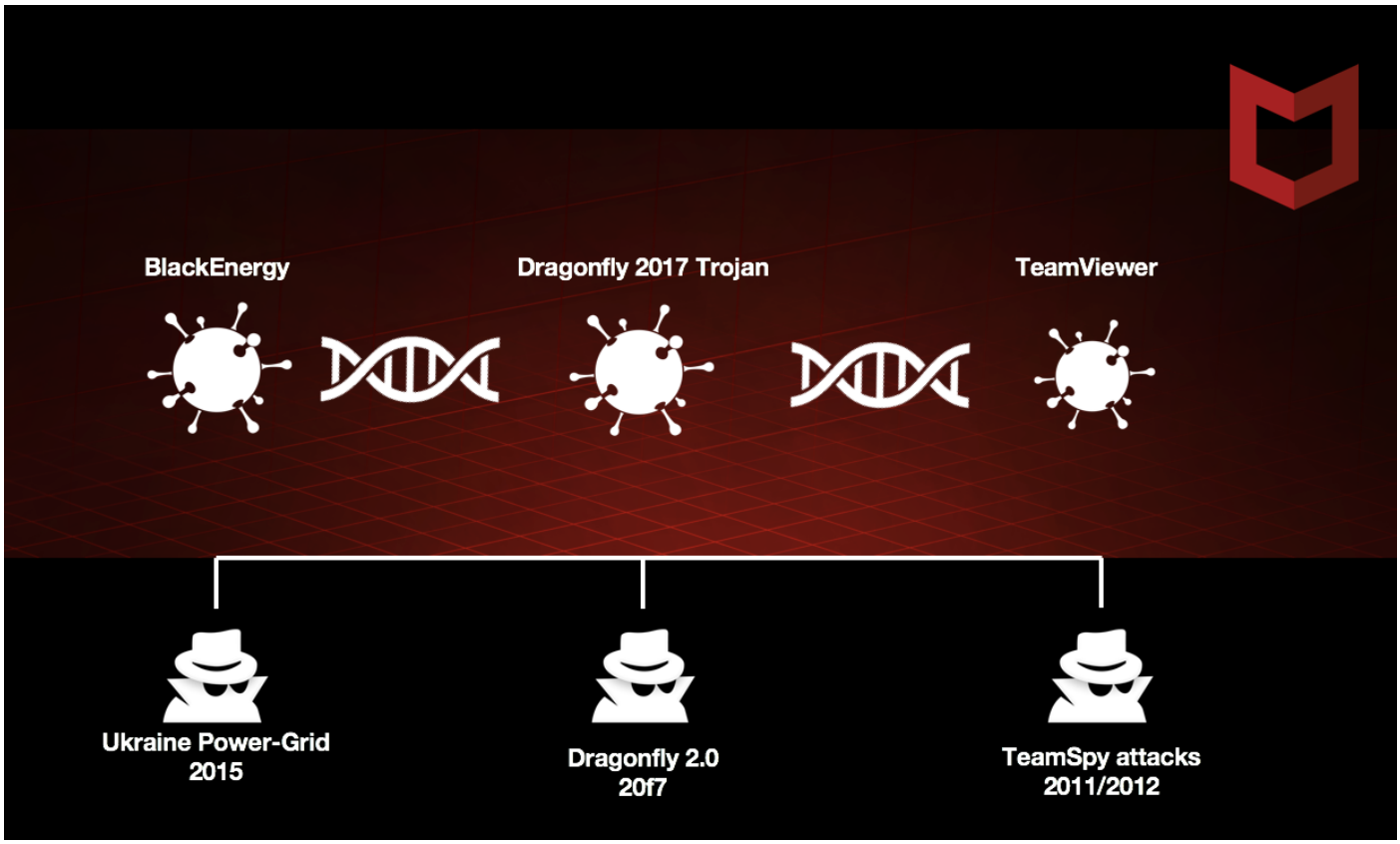
```
push    104h
lea     eax, [esp+4]
push    eax
push    0
call    ds:GetModuleFileNameW
test    eax, eax
jz      loc_40B2B2
push    104h
lea     ecx, [esp+4]
push    ecx
mov     edx, ecx
push    edx
call    ds:GetShortPathNameW
test    eax, eax
jz      loc_40B2B2
push    esi
push    offset aCDel    ; "/c del "
lea     eax, [esp+210h]
push    eax
call    ds:lstrcpyW
mov     esi, ds:lstrcatW
lea     ecx, [esp+4]
push    ecx
lea     edx, [esp+210h]
push    edx
call    esi ; lstrcatW
push    offset aNul     ; " >> NUL"
lea     eax, [esp+210h]
push    eax
call    esi ; lstrcatW
push    104h
lea     ecx, [esp+8]
push    ecx
push    offset aComspec ; "ComSpec"
call    ds:GetEnvironmentVariableW
test    eax, eax
pop     esi
jz      short loc_40B2B2
push    0
push    0
lea     edx, [esp+210h]
push    edx
lea     eax, [esp+0Ch]
push    eax
push    0
push    0
call    ds:ShellExecuteW
cmp     eax, 20h
jle     short loc_40B2B2
mov     al, 1
mov     ecx, [esp+410h]
xor     ecx, esp
```

```
push    0               ; hModule
call    ds:GetModuleFileNameW
test    eax, eax
jz      loc_4017B3
push    104h            ; cchBuffer
lea     ecx, [ebp+Filename]
push    ecx             ; lpszShortPath
mov     edx, ecx
push    edx             ; lpszLongPath
call    ds:GetShortPathNameW
test    eax, eax
jz      loc_4017B3
push    esi
push    offset aCDel    ; "/c del "
lea     eax, [ebp+String1]
push    eax             ; lpString1
call    ds:lstrcpyW
mov     esi, ds:lstrcatW
lea     ecx, [ebp+Filename]
push    ecx             ; lpString2
lea     edx, [ebp+String1]
push    edx             ; lpString1
call    esi ; lstrcatW
push    offset aNul     ; " >> NUL"
lea     eax, [ebp+String1]
push    eax             ; lpString1
call    esi ; lstrcatW
push    104h            ; nSize
lea     ecx, [ebp+Filename]
push    ecx             ; lpBuffer
push    offset aComspec ; "ComSpec"
call    ds:GetEnvironmentVariableW
pop     esi
test    eax, eax
jz      short loc_4017B3
push    0               ; nShowCmd
push    0               ; lpDirectory
lea     edx, [ebp+String1]
push    edx             ; lpParameters
lea     eax, [ebp+Filename]
push    eax             ; lpFile
push    0               ; lpOperation
push    0               ; hwnd
call    ds:ShellExecuteW
cmp     eax, 20h
jle     short loc_4017B3
mov     eax, 1
mov     ecx, [ebp+var_4]
xor     ecx, ebp
```

A BlackEnergy sample from 2016 (at left) alongside a Dragonfly sample from 2017.

Self-deleting code is very common in malware, but it is usually implemented by creating a batch file and executing the batch instead of directly calling the delete command, as we see in the preceding examples.

The BlackEnergy sample used in our comparison was captured in the Ukraine on October 31, 2015, and was mentioned in our post (https://securingtomorrow.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/) on the evolution of the BlackEnergy Trojan. It is remarkable that this piece of code is almost identical in both samples, and suggests a correlation between the BlackEnergy and Dragonfly campaigns.



Actor Sophistication

Our analysis of this attack tells a story about the actors' capability and skills. Their attack precision is very good; they know whom and what to attack, using a variety of efforts. Their focus is on Windows systems and they use well-known practices to gather information and credentials. From our research, we have seen the evolution of the code in their backdoors and the reuse of code in their campaigns.

How well do the actors cover their tracks? We conclude they are fairly sophisticated in hiding details of their attacks, and in some cases in leaving details behind to either mislead or make a statement. We rate threat actors by scoring them in different categories; we have mentioned a few. The Dragonfly group is in the top echelon of targeting attackers; it is critical that those in the targeted sectors be aware of them.

The Dragonfly group is most likely after intellectual property or insights into the sector they target, with the ability to take offensive disruptive and destructive action, as was reported (http://www.silicon.co.uk/security/blackenergy-trojan-ukraine-power-183050?inf_by=5a291109671db830108b4a17) in the 2015 attack on the Ukrainian power grid by a BlackEnergy malware family.

We would like to thank the team at Intezer for their assistance and support during our research.

‹ Previous Article (https://securingtomorrow.mcafee.com/mcafee-labs/looking-into-the-world-of-ransomware-actors-reveals-some-surprises/)

Next Article › (https://securingtomorrow.mcafee.com/consumer/iot-supports-worlds-largest-industries/)

Categories: McAfee Labs (https://securingtomorrow.mcafee.com/category/mcafee-labs/)
Tags: advanced persistent threats (https://securingtomorrow.mcafee.com/tag/advanced-persistent-threats/), cybercrime (https://securingtomorrow.mcafee.com/tag/cybercrime/), malware (https://securingtomorrow.mcafee.com/tag/malware/), Phishing (https://securingtomorrow.mcafee.com/tag/phishing/), Quarterly Threats Report (https://securingtomorrow.mcafee.com/tag/quarterly-threats-report/)

Leave a reply

Facebook Comments (0) Comments (0) G+ Comments

0 Comments Sort by Oldest

Add a comment...

Facebook Comments Plugin

Newsletter Sign Up

First Name

Last name

Email

Subscribe

McAfee on Twitter

Follow us on Twitter (https://twitter.com/McAfee)

mcafee_labs (https://www.twitter.com/mcafee_labs)

Prediction #2 (https://twitter.com/#search?q=2): Ransomware will continue to grow, but the motivations behind these types of attacks will change. Our... https://t.co/HR9XqsKas3 (https://t.co/HR9XqsKas3)

3 days ago (2018/01/13 02:03:05)
Reply (https://twitter.com/intent/tweet?in_reply_to=951998001014366208) · Retweet (https://twitter.com/intent/retweet?tweet_id=951998001014366208) · Favorite (https://twitter.com/intent/favorite?tweet_id=951998001014366208)

mcafee_labs (https://www.twitter.com/mcafee_labs)

Keep your friends close and enemies closer. We went behind enemy lines to learn the tactics and motives of... https://t.co/jbP1DXmVo0 (https://t.co/jbP1DXmVo0)

3 days ago (2018/01/13 00:32:05)
Reply (https://twitter.com/intent/tweet?in_reply_to=951975098935803904) · Retweet (https://twitter.com/intent/retweet?tweet_id=951975098935803904) · Favorite (https://twitter.com/intent/favorite?tweet_id=951975098935803904)