Master in Cybersecurity

Universidad Carlos III de Madrid

Advanced persistent threats and information leakage

Turla, DragonFly (incl. 2.0), Quedagh

Author

Sarvmetal

90n20

Sc4reCr0w

Fare9

Date May 31, 2020

Abstract

Russia is one of the world's most resourceful superpowers that lives in a continuous alert state with the rest of the countries. This was more pronounced during the Cold War, where Russia fund different intelligence agencies for improving their capabilities in espionage, counterintelligence and interception mechanisms; Russia considers information as a dangerous weapon as it is cheap, easy to access and can traverse Russian borders without any problem. Russia founded agencies as *KGB* or the military unit *GRU* and in 1991 the *FAPSI* (derived from different Directors of the *KGB*). Finally, due to the power that some of these agencies had, they were divided into different agencies, so the *FAPSI* was divided into *SVR*, *FSB* and *FSO*. These agencies control different aspects of the cyber security spectrum or as Russian calls it the *Information warfare*.

These years Russia has also been very active in a kind of warfare after the Cold War that involves the manipulation of information in social networks and forums (using the known as *Web brigades*). Moreover, some hacking groups, attacks and malware have been attributed to Russia through some of the aforementioned military groups. However, this attribution became a problem because, although they share targets and information needs, no one can accurately state the relationship between the military groups and the so called APT groups (even with the capabilities these groups show).

In this practical assignment we will talk about three different APT groups that have been related to Russia in some ways by the reports and webs we've been studying from different prestigious companies in the field of threat intelligence and malware analysis. These are: *Turla*, *DragonFly* and *Quedagh*.

It is important to note that all assumptions that we could do, as well as the information we present in here, are just reports information or our own opinion and for that reason the text in here is not completely accurate or true.

1 Key findings

1.1 Attribution

The APT set we've chosen for this practical assignment have been attributed mainly to Russia by different intelligence agencies and threat intelligence companies, like ESET (in their research department) or Symmantec.

In the case of Turla, this APT group was attributed to Russia by the National Security Agency (NSA) from US and the National Cyber Security Centre (NCSC) from UK. This attribution has been done, in part, due to the techniques and exploits used by the group. Turla APT group is also known by different alias, like Snake, Venomous Bear, Group 88, WRAITH, Turla Team, Uroburos or Uroboros, Pfinet, KRYPTON or maybe the most known and commonly used by Symantec Waterbug. This list has been extracted from [Millington, 2019] and [Malpedia, b]

Dragonfly and Dragonfly 2.0 are also known by the alias Energetic Bear, Crouching Yeti, Group 24, Koala Team and Anger Bear. Due to the targets of these groups (see subsection 2.2.2 to see targets) US has attributed them to be Russian groups. Sadly, attribution in this case is really difficult because this group uses public tools. It is worth mentioning that they tend to use strings in different languages in their malware, noticing a misuse of Cyrillic and English symbols compared with Turla/Snake or Quedagh. The last attribution problem from Dragonfly comes with the fact that their first attack reported has been inside of Russia [RIA, 2018].

Finally, for Quedagh attribution we have to look over the political background, as this APT group has participated in many politically-oriented attacks, ranging from the confrontation between Russia and Georgia in 2008, to the political crisis in Ukraine, which started at the end of 2013. More will be explained in the subsection 1.2. Quedagh is also known as *Sandworm* (by Trend Micro), *Iron Viking* (by Secure Works), *Vodoo Bear* and *TEMP.Noble*. The list of names has been extracted from [Mitre, 2017], [ThaiCERT, 2019] and [Malpedia, a].

1.2 Political Problems and consequences

All of this APTs seem to have some political intention behind their attacks, focusing them on governments and critical infrastructures.

Turla, for instance, targeted several government institutions, embassies and even pharmaceutical companies with espionage purposes. An interesting fact related to Turla, as explained in [Majumder, 2019], involves a series of attacks to Iranian computers already infected by APT34 [Cytomic, 2019], stealing their tools (**Neuron** and **Nautilus**) and showing a warfare between APT groups sponsored by different states.

Dragonfly took advantage over political problems between different countries in order to launch their campaigns as we saw at Ukrainian outage during 2015. This is one of their most known activities, which affected thousands of people and it is believed to be one of the firsts successful attacks to a power grid infrastructure.

The fact is that, over the last years, energy sector has become a precious target for state-sponsored hackers due to the number of critical infrastructures operated by companies in the industry. Taking this into account, we can infer that Dragonfly might be a state-sponsored group. [Pavel Polityuk, 2017]

Quedagh, like Turla, is found to be participating in many politically-oriented campaigns, being its first first appearance related with Georgia massive DDos attacks in 2008, which anticipated the Russian invasion of the region.

Although it is not confirmed, the group campaigns have solid links to the well-known attacks against energy facilities, blinding system dispatchers, making unwanted changes to the distribution infrastructure and also wiping SCADA servers in an attempt to slow down the recovery from the situation. It is known that this campaign is also related to some attacks against NATO and some European companies.

As per [Waldman and Cordona, 2019] information, the group has also relations with the NotPetya attacks in 2016 and the ransomware BadRabbit in 2017.

2 Activity Details

2.1 Timeline

We've summarized the most remarkable events involved in these APT groups in Figure 1 trying to show their activity throughout the years. Turla is the oldest APT group from this set as spotted in [Millington, 2019], then we have to move until 2008 to see the first Quedagh operation and the Turla's attack to the US Department of Defense [Knowlton, 2010]. Two years later appeared Dragonfly when Trojan.Karagany's source code was leaked.

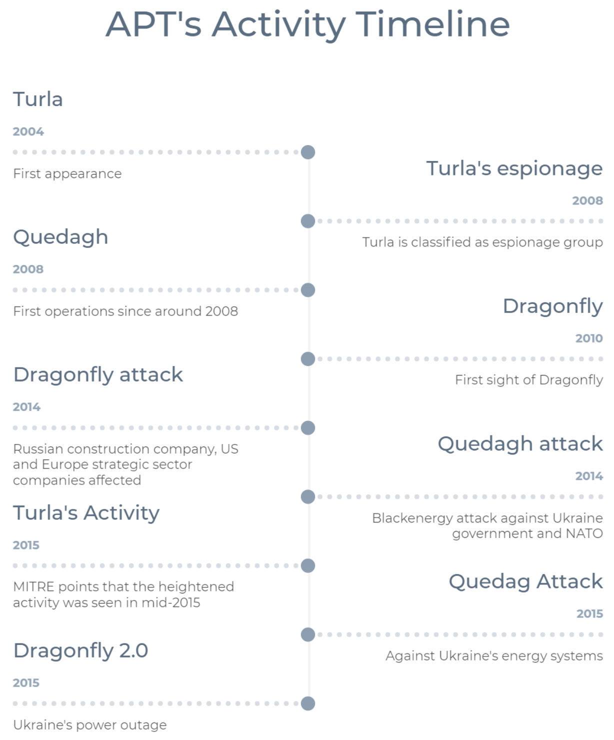
APT's Activity Timeline
Turla
2004
First appearance
Turla's espionage
2008
Turla is classified as espionage group
Quedagh
2008
First operations since around 2008
Dragonfly
2010
First sight of Dragonfly
Dragonfly attack
2014
Russian construction company, US and Europe strategic sector companies affected
Quedagh attack
2014
Blackenergy attack against Ukraine government and NATO
Turla's Activity
2015
MITRE points that the heightened activity was seen in mid-2015
Quedag Attack
2015
Against Ukraine's energy systems
Dragonfly 2.0
2015
Ukraine's power outage

Figure 1: APTs Timeline

2.2 Targets

The similarity in targets between these tree groups is very extensive. Next we list targets individually for each group and then we summarize them in a brief description.

2.2.1 Turla

The type of targets are classified in the next list (this list can be verified with the analysis from the NCSC [NCNS, 2018]): Governments, Embassies, Military, Education, Research and Pharmaceutical Companies

2.2.2 Dragonfly (incl. 2.0)

According to [Kaspersky, 2018], the main targets of these groups are: Construction, Education, Industrial/machinery, Information technology, Manufacturing and Pharmaceutical

2.2.3 Quedagh

This group has a wide diversity of targets including Education, Energy, Government and Telecommunications

After a cross-check verification, we can observe that entities in the strategic sector as well as Governments are of special interest for these groups which focus their efforts in sabotage, espionage and data collection/destruction.

Victims are spread across the world but we can identify a very tight focus in US, Europe and CIS countries. For instance, these APTs attacked countries that, for historical reasons, have been the preferred target for some East Countries, those are Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyztan, Armenia, Lithuania, Ukraine and Russia. Furthermore, some European countries such as Spain, France, Italy, Germany, Poland, Romania, Greece and some others like Saudi Arabia, Serbia, Iran and Israel have been strongly affected by these actors.

It's not a surprise to see that, with the help of countries like Cuba and Venezuela, which supports and encourage Russian activities around the globe, the US is tagged as one of the most affected countries and suffered the most successful attacks from the APTs side. We can even find that some Latin American countries have been impacted by these activities, including Brazil, Ecuador and Mexico.

This enforces the idea of state-sponsored authors behind these groups due to the targets high value.

3 Technical details

In this section we will explain different techniques used by the APT groups from the set 3 we will separate the common infection techniques in different steps, ranging from the techniques used to create a first entry point on the system, to the installation of more complex tools. Russia is known for using some specific techniques and use different exploits (mainly for Microsoft Windows targets), but as we saw at class, the term "Advanced" in APT does not always mean complex but how they propagate, their goals and their targets.

3.1 First contact to target system

As pointed by [Peter Apps, 2014] Russian government backed "hackers" are known for being highly disciplined, adept at hiding their tracks, extremely effective at maintaining control of infected networks and more selective in choosing targets. They also commonly exploit the human factor for getting a first foot hold in target systems. The most common used techniques are: *spearphishing*, *watering hole attacks* and *trojanized installers.*

This is used together with different exploits in order to be able to install a first tool inside of the system and to bypass most protections, specially if these are zero-days running payloads during programs' start. Another strategy is the use of embedded *VBA macros* to download a next phase for the attack. Watering hole attacks (used by Turla and Dragonfly) are based on the infection of the web servers commonly visited by the targets with the same purpose than spearphishing attacks.

Finally, the trojanized installers, at the same time that they install a legitimate software, also run the piece of malware in background (Quedagh and Turla APTs used fake updates of Adobe Flash Player). This can be read in [Symantec, 2016] [Paganini, 2020] [Research, 2018] and [Labs, 2016]

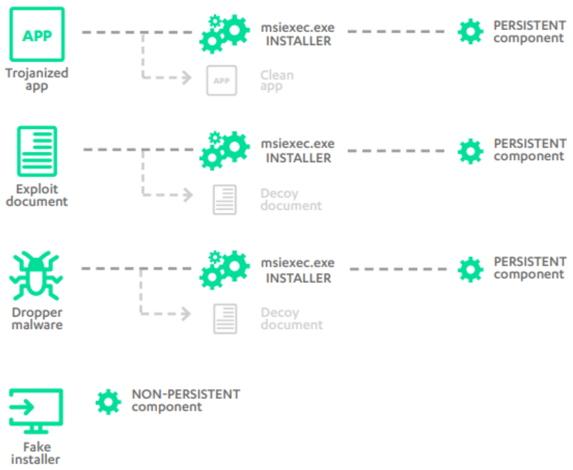

Figure 2: Quedagh different types of infection techniques

3.2 After a successful breakthrough

One important characteristic of any APT is *persistence* and these groups are not, of course, very different from the others. In order to gain such important characteristic, the main strategy is using stealthy backdoors. There is a significant number of tools used and if we gather all these groups backdoors in one, we can see a clear pattern in the pieces of code. The first approach is to recollect data and exfiltrate information that could be useful for next phase, following with manipulation and destruction of data or scanning network connections, among others. It's important to mention and briefly describe some used backdoors in order to give an idea of the sophistication and advance technical capabilities of these authors.

3.2.1 Turla

This group splits the backdoor installation in two stages. In the first seen attacks, they used malware named as Tavdig or Skipper but then moved to open source tools as meterpreter (one of metasploit payloads) obfuscated with the *shikata ga nai* toolkit. This first backdoor allows them to do a reconnaissance phase in order to proceed or not with the next installation.

If the system becomes to be a target of interest, another backdoor will be downloaded and installed. This time it will be a more sophisticated tool compared with the previous one, like Uroburos/Uroboros/Snake/Turla (related to *Agent.BTZ*, both linked to the well known malware

Red october) composed by different modules for 32 and 64 bits and a special driver also for 32 and 64 bits. Another possible backdoor is Carbon [Research, 2017] which would be like a lite version of Uroburos but doesn't include the driver module, so complexity decrease with this version. Finally, another backdoor that can be installed is mosquito [Research, 2018].

In order to avoid being detected by protection mechanisms as firewalls, there are modules used to inject dlls in specific process to connect to Turla's C&Cs.

As part of the set of tools that this APT group uses, many different exploits are delivered, like *CVE-2013-3346* used to elevate privileges and *CVE-2013-5065* to install the second backdoor. Moreover, they also exploit *MS09-025* and *MS10-015* vulnerabilities. At this pont, it is worth to mention an interesting exploit used by this group, that involved a vulnerable VirtualBox driver aimed for version 1.6.2 and 1.6.0. They installed the signed driver VBoxDrv.sys bypassing many security checks and then the vulnerability was exploited in an effort to perform privilege escalation over the affected system.

Even when many of these phases are windows targeted, Turla has also targeted macOS and Linux Systems [Kurt Baumgartner, 2014][newWorld, 2017].

3.2.2 Dragonfly (incl. 2.0)

In the case of Dragonfly, the most relevant malware they used was *Backdoor.Oldrea.* This is a persistent component that reaches the C&C servers performing a GET request, expecting a HTML response page with a base64 encoded string. This string is found between two comments with the text *havex* and the instruction to follow. The backdoor is designed to collect sensitive information such as OS, username, computer's configuration and installed drivers among others. However, the most interesting IOC is the collection of data from Outlook and ICS related software configuration files. All of the gathered data is encrypted and sent back to the C&C server with a HTML POST request [Symantec, 2014].

It is also common to see in their campaigns an installation of the *Karagany* malware, which is used for recon. It installs itself in the affected target in order to download additional content and exfiltrate data. Dragonfly is a recognized group in the use of freely available tools in the wild, as it could be seen in the case of this malware, where they use common packers such as *UPX* and *Aspack*, together with a custom *Delphi* binary packer/protector. Here we have an important attribution flag, as the APT group always use *neosphere* as the key to decrypt the payloads.

Afterwards, when Dragonfly 2.0 was born in 2015, other backdoors where discovered. Typically, they try to install one or two backdoors in the target system, in order to to gain remote access. It is known that *Goodor*, *Karagany.B* and *Dorshel* were used along with *Trojan.Heriplor*.

Looking deeper at the functionality and characteristics of these backdoors, we found some interesting facts: *Goodor* is a tool written in Golang and its main goal is to provide attackers remote access to the target machine; *Karagany.B*, in other side, make crucial changes inside Windows machines, ranging from file corruption and firewall bypass to more advanced techniques, like adding malicious code into Windows Boot Setting, so it can get persistence and run stealthy; Finally, not very different from the others if we speak about the aims, once *Backdoor.Dorshel* is executed, it opens a reverse connection to a pre-defined list of URLs, from where it it may download potential additional files.

Other interesting report from [Kaspersky Research Team, 2014], names backdoors as *Sysmain* and *ClientX*, which are described as RATs that give attackes a wide range of functionalities to control and interact with the target machines. These functionalities include launching additional malware, taking screenshots, updating the RAT itself and loading DLLs.

3.2.3 Quedagh

As different investigations suggest, it seems that Quedagh use a customized version of the widely used *BlackEnergy* toolkit. It was initialy designed to create botnets for using them in DDoS attacks but, since its first appearance around 2007, it has evolved to add more functionalities through plugins.

According to [Labs, 2016], this APT group customizations include, among others, support for proxy servers and the inclusion of techniques to bypass the Windows UAC and driver signing protection over 64 bits systems. Moreover, it seems that they also included the possibility to download malware aimed for SCADA ICS systems, especially those related to *Siemens' Simatic WinCC Systems*. In total, three different versions of this malware have been identified over time, called *BlackEnergy 1*, *BlackEnergy2* and *BlackEnergy3*, being this last one not only amied for Windows, but also for Linux, ARM-based , MIPS-based, SCADA ICS and some Cisco networking devices, as reported by [Check Point, 2016].

After a successful breakthrough, they use a wide variety of exploits to drop the malware installer, like the *CVE-2010-3333*, which affected a bunch of office versions, the *CVE-2014-1761*, which was aimed towards Microsoft Word, or the well-known 0-day *CVE-2014-4414*, a very harmful RCE vulnerability present in Office OLE objects.

The malware only attemps to infect systems whose current user has administration privileges, as it relies in a driver component to achieve persistence. If this is not the case, it will relaunch itself as Administrator, triggering an UAC propmt. Here the filename of the installer gets sense, as the group tend to use *regedt32.exe* in order to temp the user to grant administrative permissions.

As this could be unsuccesful with experienced users, further versions of the malware include a bypass of the UAC settings, exploiting a backward compatibility on Windows systems, so the user interaction is no longer needed and the installation runs completely into the background. During this time, the installer filename change to *msiexec.exe*, the same as the Windows installer program.

With the arrival of 64 bits systems, the group faced a new change of plans and added support to this technology. Also, they included a bypass to the new driver signing requirement, present at Windows 64 bits systems, through the use of the *TESTSIGNING* option provided by Microsoft to developers. As this adds a watermark to alert the users about this fact, the group removed related strings at *user32.dll.mui*.

The final objective of the malware installer is to inject its dll component, embedded in the driver, into *svchost.exe*. Moreover, it provides some routines for hiding processes using *DKOM* (Direct Kernel Object Manipulation) and to manage rootkit rules directly from memory.

Once deployed, the malware supports the following commands: *rexec* (Download and execute files), *lexec*(Execute commands), *die*(Uninstall), *getpl*(Load plugins), *turnoff*(Exit), *chprt*(Add, remove or set C&C server).

In newer releases, those commands changed, to add even more control over the installed malware: *delete*(Uninstall), *ldplg*(Load plugins), *unlplg*(Unload plugins), *update*(Update main dll), *dexec*(Download and execute files), *exec*(Execute shell commands), *updcfg*(Update configuration data).

This process provides the APT group with a toolkit to maintain botnets without specific functionality, letting them to load customized plugins from a remote C&C server, depending on the target and their desired intentions.

Due to its behaviour it is difficult to determine the uses of this malware implant, but regarding to the group associated campaigns it is clear that their main focus is the steal of information from compromised systems, like accounts, credentials, registered mails..., as well as perform lateral movements and network discovery.

Some other investigations affirmed that the group use other pieces of malware, like *PassKillDisk* [Gilbert Sison, Rheniel Ramos, Jay Yaneza, Alfredo Oliveira, 2018] , a data wiper, and *Gccat* [byt3bl33d3r, 2015], a backdoor that relies in gmail for its C&C communications.

3.3 Summarizing in a table

Table 1 shows the techniques summarized in a table, where a bullet represent that the technique is used by the APT group.

APT Group	Spearphishing	Watering Hole	Fake Installer	Backdoor	Second Backdoor	Zero-Day Exploits
DragonFly (Incl. 2.0)	●	●	●	●		
Turla	●	●	●	●	●	●
Quelagh	●		●	●		●

Table 1: Table with techniques used by the APT's malwares.

References

[byt3bl33d3r, 2015] byt3bl33d3r (2015). gcat A PoC backdoor that uses Gmail as a C&C server. https://github.com/byt3bl33d3r/gcat. [Online; accessed 22-April-2020].

[Check Point, 2016] Check Point (2016). Check Point Threat Alert: BlackEnergy Trojan. https://blog.checkpoint.com/2016/01/14/check-point-threat-alert-blackenergy-trojan/. [Online; accessed 22-April-2020].

[Cytomic, 2019] Cytomic (2019). Turla contra el mundo: así es el grupo terrorista que ha ciberatacado a 35 países. https://www.cytomicmodel.com/es/news/turla-grupo-ciberterrorismo/. [Online; accessed 21-April-2020].

[Gilbert Sison, Rheniel Ramos, Jay Yaneza, Alfredo Oliveira, 2018] Gilbert Sison, Rheniel Ramos, Jay Yaneza, Alfredo Oliveira (2018). New KillDisk Variant Hits Financial Organizations in Latin America. https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/. [Online; accessed 22-April-2020].

[Kaspersky, 2018] Kaspersky (2018). Crouching Yeti. https://apt.securelist.com/#!/threat/976. [Online; accessed 22-April-2020].

[Kaspersky Research Team, 2014] Kaspersky Research Team (2014). Energetic Bear - Crouching Yeti. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf. [Online; accessed 22-April-2020].

[Knowlton, 2010] Knowlton, B. (2010). Military Computer Attack Confirmed. https://www.nytimes.com/2010/08/26/technology/26cyber.html?r=1&ref=technology. [Online; accessed 21-April-2020].

[Kurt Baumgartner, 2014] Kurt Baumgartner, C. R. (2014). The 'Penquin' Turla A Turla/Snake/Uroburos Malware for Linux. https://securelist.com/the-penquin-turla-2/67962/. [Online; accessed 21-April-2020].

[Labs, 2016] Labs, F.-S. (2016). BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks. `https://www.f-secure.com/documents/996508/1030745/blackenergywhitepaper.pdf`. [Online; accessed 22-April-2020].

[Majumder, 2019] Majumder, B. G. (2019). Russia-linked hackers attack 35 countries using stolen Iranian malware. `https://www.ibtimes.sg/russia-linked-hackers-attack-35-countries-using-stolen-iranian-malware-33451`. [Online; accessed 21-April-2020].

[Malpedia, a] Malpedia. Sandworm. `https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm`. [Online; accessed 22-April-2020].

[Malpedia, b] Malpedia. Turla Group. `https://malpedia.caad.fkie.fraunhofer.de/actor/turlagroup`. [Online; accessed 21-April-2020].

[Millington, 2019] Millington, E. (2019). MITRE — ATT&CK: Turla. `https://attack.mitre.org/groups/G0010/`. [Online; accessed 21-April-2020].

[Mitre, 2017] Mitre (2017). Sandworm Team. `https://attack.mitre.org/groups/G0034/`. [Online; accessed 22-April-2020].

[NCNS, 2018] NCNS (2018). Turla group malware. `https://www.ncsc.gov.uk/news/turla-group-malware`. [Online; accessed 21-April-2020].

[newWorld, 2017] newWorld (2017). APT Turla - Kazuar (MacOS Version of Uroburos Espionage Rootkit). `http://www.edison-newworld.com/2017/05/apt-turla-kazuar-macos-version-of.html`. [Online; accessed 21-April-2020].

[Paganini, 2020] Paganini, P. (2020). Russia-Linked Turla APT uses new malware in watering hole attacks. `https://securityaffairs.co/wordpress/99518/apt/turla-apt-new-malware.html`. [Online; accessed 21-April-2020].

[Pavel Polityuk, 2017] Pavel Polityuk, Oleg Vukmanovic, S. J. (2017). Ukraine's power outage was a cyber attack: Ukrenergo. `https://www.reuters.com/article/us-`

ukraine-cyber-attack-energy-idUSKBN1521BA. [Online; accessed 21-April-2020].

[Peter Apps, 2014] Peter Apps, J. F. (2014). Suspected Russian spyware Turla targets Europe, United States. https://www.reuters.com/article/us-russia-cyberespionage-insight-idUSBREA260YI20140307. [Online; accessed 21-April-2020].

[Research, 2017] Research, E. (2017). Carbon Paper: Peering into Turla's second stage backdoor. https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/. [Online; accessed 21-April-2020].

[Research, 2018] Research, E. (2018). Diplomats in Eastern Europe bitten by a Turla mosquito. https://www.welivesecurity.com/wp-content/uploads/2018/01/ESETTurlaMosquito.pdf. [Online; accessed 22-April-2020].

[RIA, 2018] RIA (2018). Experts called the possible culprits of hacker attacks on US energy networks. https://ria.ru/20180724/1525259858.html. [Online; accessed 22-April-2020].

[Symantec, 2014] Symantec (2014). Dragonfly: Cyberespionage Attacks Against Energy Suppliers. https://www.yumpu.com/en/document/read/44301001/dragonfly-threat-against-western-energy-supplierspdfutm-contentbuffer4b1c9utm-mediumsocialutm-sourcetwitter. [Online; accessed 22-April-2020].

[Symantec, 2016] Symantec (2016). The Waterbug attack group. https://paper.seebug.org/papers/APT/APTCyberCriminalCampagin/2016/2016.01.14.The.Waterbug.Attack.Group/waterbug-attack-group.pdf. [Online; accessed 21-April-2020].

[ThaiCERT, 2019] ThaiCERT (2019). THREAT GROUP CARDS: A THREAT ACTOR ENCYCLOPEDIA. `https://www.thaicert.or.th/downloads/files/A ThreatActorEncyclopedia.pdf`. [Online; accessed 22-April-2020].

[Waldman and Cordona, 2019] Waldman, J. and Cordona, E. (2019). TOP 25 THREAT ACTORS - 2019 EDITION. `https://sbscyber.com/resources/top-25-threat-actors-2019-edition`. [Online; accessed 22-April-2020].