Advanced Persistent Threat

Lalisha Sanduwara

IT19130026

Content Page

Abstract

In the modern digitally connected world, prolonged and targeted cyber attacks became one of the most serious threats to the modern computer systems or organizations. This "**Advanced Persistent Threat**" is currently on top of the most serious threats considering the information security concept. The main goal of **Advanced Persistent Threats** is achieving and maintaining the ongoing access to the targeted network or the system without being undetected and steal or gather information for a long period. It collects data by exploiting the vulnerabilities in the system or the network using diverse techniques. Many researchers researched to find approaches and solutions against theses malicious software and threats. But a very few of them were focused on this **Advanced Persistent Threat.** This report is focused on explaining what is Advanced Persistent Threat, how Advanced Persistent Threat works, History of Advanced Persistent Threat, what are the examples for Advanced Persistent Threat, how to detect and prevent Advanced Persistent Threat, what can happen to Advanced Persistent Threat in future. This paper also includes some Advanced Persistent Threat attacks.

Introduction

What is Advanced Persistent Threat?

An Advanced Persistent Threat is a prolonged and targeted attack which is unauthorized users gain access to a system or a network and remain undetected for a period of time. Attackers usually use these Advanced Persistent Threat attacks to monitor networks activities and steal data more than damage to the network or the system.

Advanced Persistent Threat attacks usually target the organizations or systems in sectors such as **National Defense**, **Financial**, **Manufacturing** because these organizations or the systems deal with high-value information such as Military plans, Highly classified intel or sensitive data from government and organizations.

The main focus of Advanced Persistent Threat attack is to achieve and maintain ongoing access to the targeted network or the system rather than getting in and getting out as quickly as possible.

Because of Advanced Persistent Threat attacks cost a great deal of effort, time and resources, hackers target high-value targets with the ultimate goal of stealing information for a long period.

Advanced Persistent Threat attackers use advanced attack techniques such as advanced exploits of zero-day vulnerabilities, spear phishing and social engineering and also use methods such as re-writing the malicious code to avoid the detection and to maintain the access without being discovered.

How an Advanced Persistent Threat works?

These are the main 5 Steps of how Advanced Persistent Treat works

Gain access:

ATP groups gain access to the targeted systems by phishing emails, compromised networks or via an application vulnerability.

Establish a foothold:

when the attackers gaining access to the targeted system, they begin to exploit the malware probes for additional communicate with command-on-control or establish the additional points of compromise to ensure that the attack can continue if one point is closed.

Move laterally:

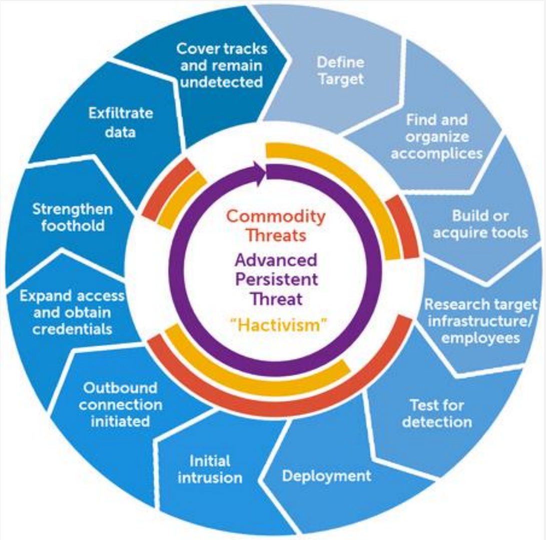
once the attackers gain the access to the targeted systems with the admin rights, they can attempt to take over other servers and other secured areas.

Take the data:

attackers can retrieve data from the system

Stay Undetected until the job is done:

remove the evidence of the attack (foot prints) and create a backdoor to access the system anytime in the same point.


Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
"Hactivism"

History of Advanced Persistent Threat

In 2005 United Kingdome and United State CRET organizations published warnings against the targeted, socially engineered emails dropping trojans to steal sensitive information. This method was used from early 1990s and but it doesn't account for APT. The term "Advanced Persistent Threat" has been cited by US air force Colonel Greg Rattray in 2006.

Iran's nuclear program computer hardware were targeted by a malware called Stuxnet Computer Worm and the Iranian might consider that the Stuxnet creators to be an Advanced Persistent Threat.

This term is always used in reference to a prolonged pattern of sophisticated computer network exploitations which targeted the governments, companies and political activities.

Many sources have alleged with that some Advanced Persistent Threat groups are connected with or agents of governments of sovereign states.

The business or the organizations with the large number of sensitive data are at high risk of being attacked by Advanced Persistent Threat including below sectors.

- Higher education
- Energy
- Technology
- Manufacturing
- Agriculture
- Financial organizations
- Transportation

Advanced Persistent Threat Groups

There are many Advanced Persistent Threat groups in the world wide. These are some examples for these Advanced Persistent Threat groups.

China:

- PLA Unit 61398 (APT1, Comment Crew, Comment Panda, Byzantine Candor)

  Is the military unit undercover designator of a people's liberation army APT unit which has been a source of Chinese computer hacking attack.

  APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the ability and intent to steal dozens of organizations at once. The group focuses on reaching consensus across a wide range of industries in English-speaking countries. The size of the infrastructure of APT1 means a large organization with at least a dozen, but possibly hundreds of human operators.

- Red Apollo (APT 10, Menu Pass, Stone Panda, POTASSIUM)

  They were a group which is sponsored by the government, linked in to the Tianjin field office of the Ministry of Salute Security since 2006.

This continuous APT10 operation involves both access to the casualty system through traditional Lance phishing and monitoring specialist co-ops.

The APT10 skewer phishes are not moderately modern, using duplicate .lnk documents, double-enlargement reports (for example [reshaped] _group_matting_document_20170222_doc_.exe) and sometimes deviate from the initially unrecognizable designation. Launch reports and similar pernicious launches. In spite of spear phishing, Fire Eye Threat Intelligence has tracked how APT10 accessing victims through organizations around the world.

- PLA Unit 31486(APT 2)
- Buckeye (APT 3)
- Codoso Team (APT 19)
    - Target Sectors: Legal and Investment
    - Associated Malware: BECON, COBALTSTRIKE
    - Attack Vectors: In 2017, APT19 used three clear procedures to try to reach bargaining targets. RTF connections that misused Microsoft Windows vulnerability as depicted in CVE 2017-0199 used phishing bait in early May. At the end of May, APT19 shifted to using full-fledged Microsoft Excel (XLSM) records. In the latest variants, APT19 added a white listing application to the XLSM archive.
- Wocao (APT 20)

- PLA Unit 78020(APT 30)
    - Target Sectors: Financial, Government, Energy, Chemical
    - Associated Malware: SHIPSHAPE, SPACESHIP, FLESHFLOOD
    - Attack Vectors: APT30 downloaders use a set of tools designed to traverse aerospace networks for infecting and stealing data on back doors, central controllers and removable drives. APT30 constantly registers its own DNS domains for malware CnC activity.

- Periscope Group (APT 40)
  - Target Sectors: Aviation, Government, Education, Chemical, Technology organizations
  - Associated Malware: this has been using over 51 different code families
  - Attack Vectors: APT40 usually functions as an outstanding person. This includes claiming to be a writer, exchange distributor, or a relevant military association or non-administrative association (NGO). In some cases, the collection has recently been used to underestimate email deliveries.

- Double Dragon (APT 41)
  - Target Sectors: Healthcare, Telecoms, Hight-Tech Sector
  - Associated Malware: this has been using at least 46 different code families and tools
  - Attack Vectors: APT41 regularly relies on LinkedIn Skywire phishing messages, for example, ordering HTML (.chm) documents to be trafficked initially. Once you go to an accident association, APT41 can use more advanced TTP and carry additional malware. For example, in a business that has been running for nearly a year, APT41 has compromised with hundreds of systems and used nearly 150 unique malware including back doors, credential stealers, keyboards and rootkits. APT41 has deployed Rootkit and Master Boot Record (MBR) boot kits on a limited basis to hide their malware and maintain the integrity of selected victims' systems.

Iran:

- Elfin Team (APT 33, Refined Kitten, Magnallium, Holmium)
    - Target Sectors: Aerospace, Energy
    - Associated Malware: SHAPESHIFT, DROPSHOT, TURNEDUP, NANOCORE, NETWIRE, ALFA Shell
    - Attack vector: Lance phishing messages have been sent to workers identified with the APT33 flight business. These messages included bait themed baits and associated with harmful HTML applications (.hta) documents.

      The .hta reports contained a wide range of responsibilities and contacts for real job postings in well-known workplaces that are relevant to the public.

- Helix Kitten (APT 34)
    - Target Sectors: Financial, Government, Energy, Chemical
    - Associated Malware: POWBAT, POWRUNER, BONDUPDATER
    - Attack vector: APT34 in its latest Crusade, POWRUNER and BONDUPDATER used the now defunct Microsoft Office CVE-2017-11882 to communicate.

- Charming Kitten (APT 35, Phosphorus, Ajax Security, NewsBeef)

- APT 39
    - Target Sectors: Financial, Government, Energy, Chemical
    - Associated Malware: The spread of APT39 has received worldwide attention, and its exercises are packaged in the Middle East. APT39 has organized the media communications field, focusing on businesses and IT companies and the industries that support it.

- Attack vectors: Fire Eye Intelligence has exposed the impact of APT39 with deadly links to start trading, as well as hyperlinks that usually bring about POWBAT corruption. Email accounts that have tended to misuse the natural load and increase the dangers of a fuller attack have now become redundant. APT39 repeatedly registers and utilizes spaces that look like genuine web administrations and associations relevant to the proposed goal. Moreover, this meeting distinguished and misused unauthorized web servers from associations focused on introducing web shells, for example, Antac and ASPXP, and taking bargains to remote-facing Outlook Web Access (WA) assets. Used genuine certificates. We have not looked at the risk of APT39 abuse.

Russia:

- Fancy Bear (APT 28, Pawn Storm, Sofacy Group, Sednit, STRONTIUM, Tsar Team, ThreatGroup-4127)
  SOURFACE DOWNLOADER FOR DEVICES USED BY APT28, Its second stage indirect access includes a set of entries named EVILTOSS and CHOPSTICK. APT28 has been used to protect RSA encryption records and move data from the casualty system to the controller. It's been a long and dedicated improvement effort since 2007, when the SOURFACE downloader and its surroundings have been gradually and systematically altered.
- Cozy Bear (APT 29, Office Monkeys, Cozy Car, The Dukes, CozyDuke)
  - Target Sectors: Western European Governments, foreign policy groups
  - Associated Malware: POWBAT, POWRUNER, BONDUPDATER
  - Attacked Vectors: APT29 has used web-based life destinations, for example Twitter or GitHub, like distributed store administrations, to transfer orders and concentrate information from non-traded systems. The meeting rotates orders through pictures that contain enclosed and encoded information. Data is extracted from an underestimated system and documents are transferred to distributed storage administrations.

- Voodoo Bear
- Venomous Bear

North Korea:

- Ricochet Chollima (APT 37)
    - Target Sectors: Chemical, Electronics, Manufacturing, Aerospace, automotive
    - Associated Malware: POWBAT, POWRUNER, BONDUPDATER
    - Attack Vectors: Social planning strategies are custom-tailored to the desired goals, using public web bargaining of targeted digital secret activities and flood-sharing sites to make malware more seamless. Abuse vulnerabilities in Adobe Flash as well as Hangul Word Processor (HWP). The meeting demonstrated access to zero-day risks (CVE-2018-0802) and demonstrates their ability to link activities.

- Lazarus Group (APT 38, Gods Apostles, Gods Disciples, Guardian of Peace, Zinc, Whois Team, Hidden Cobra)
    - Target Sectors: Financial institutions world-wide
    - Associated Malware: backdoors, tunnelers, dataminers
    - Attack Vectors: APT38 has operated more than 16 associations at any one time in 11 countries. This meeting is cautious, determined, and requires the continuation of access to accidents for any period of time important to understand the system architecture, necessary agreements and frameworks to achieve its objective. APT38 Interestingly, they are not hesitant to forcibly suppress evidence or formulate injuries as a key component of their activities.

United States:

- Equation group

Uzbekistan:

- Sand Cat

Vietnam:

- Ocean Lotus
  - Target Sectors: Foreign companies which are investing Vietnam’s manufacturing, hospitality and consulting
  - Associated Malware: SOUNDBITE, WINDSHIELD, PHOREAL, BEACON, KOMPROGO
  - Attacked Sectors: APT32 entertainers influence activism reports to empower injured macros using social planning strategies. Once activated, the installed document will usually download a large number of malpractice payments from a remote server. APT32 entertainers bring revenge links via Lance Phishing Messages. Proof has been shown that some have been sent via Gmail.

There is another Undisclosed APT Group called APT 5

- Target Sectors: Telecommunication, technology companies, satellite communication information.
- Associated Malware: LEOUNCIA
- Attack Vectors:
  Every account seems to be a huge risk cluster consisting of a few schedules. Assembling Media Broadcasting Organizations use malicious software with typing capabilities to clearly target the corporate systems, workers and officials.

How can we detect Advanced Persistent Threat?

Network Monitoring

This can expose the suspicious activities which alert Advanced Persistent Threat. Payloads can be detected done by using Advanced Persistent Threat detection solutions.

1. Increase in log-ons at late at night

   Advanced Persistent Threats increase from compromising one computer to take over many computers or whole computer network within few hours.to perfume that attacker read authentication databases, steal user credentials and reuse them. So, they go through multiple servers and we can notice a high volume of upraised log-ons in the mid night.
2. Unusual information flows

   Unexpected flows of large information from internal origination point to another internal pc or to an external pc. (server to server, server to client, network to network)
3. Unexpected data files.

   Attackers create data bundles which are ready transfer to the attackers' computer. We can notice large size files compressed in archive formats appear in unusual places.

User behavior analytics

Monitor and analyze how users work with the information systems or organizations. Then the systems can detect unusual behaviors.

Deception technology

Fool the attackers by leading to attack to a fake server, networks and other resources. Security researchers can study the attacking methods and techniques which are use by the attacker while the attackers wasting their time and their strength for trying to retrieve data from fake servers or databases.

How to prevent Advanced Persistent Threat

Install a Firewall

When firewall is up, it will be the first defense against the Advanced Persistent Threat.

Install a web application firewall

By installing a web application firewall, user can detect the attacks coming through web by looking at the HTTP traffic.

Install an Antivirus software

Trojans, malware and viruses which are used by Advanced Persistent Threat attackers to exploit the system can be detected by Antivirus software.

Install a Virtual Private Network (VPN)

Wi-Fi hotspots are easy opportunities for attackers. VPN provides a secure encrypted tunnel which can access without being attacked by the attackers.

Educate all the employees about Spear Phishing

Train the employees to what should they do, what they should not do and to whom they should inform about this.

Make sure all the security patches are installed

If you are not installing patches on time, your computer is more vulnerable to attacks.

The future of Advanced Persistent Threat

The rise of sovereign information laws shows how armed information has become. Information is being developed step by step through the development of 5G, Internet of Things (IoT), Industry 4.0, smart cities and systems. This rise in information has brought a big buzz to Edge innovations, distributed storage arrangements, and informational lakes. All of this is an attempt to handle the enormous amount of data that is being generated every second, in an effort to limit the resources required by organizations around the world. The World Economic Forum predicts that by 2025, 463 Exabytes of data will be created globally every day.

Our information may include personally identifiable information (PII) for example, locations and government disability numbers, geographical areas, your investigation history or your political interests). This information is important to many individuals and associations, from promoting / displaying viewpoints, to ideological groups that seek to influence the consequences of a clear sexual orientation, age gap, or general political decision. The persistence of Netflix's Great Hack and the impact of Cambridge Analytica directly impacts the viewpoints of a large number of people.

Consider this from the point of view of today's enemies, especially in the case of high-profile threats (APT) that have their own advantages, such as money gains, political upheaval in a nation for the misuse of an uprising, or the support that a political agent can have.
Moreover, the traditional requirements for surveillance, damage and theft are echoed through the APT as a convincing factor.

It is simple to see why information is regularly referred to as the new oil, and why it places a high importance on resistive capacity, and the reduction of the all-inclusive current custom cavity. Moreover, legislation is enacted to ensure sovereign and business premiums, as well as associations and offices that utilize resources effectively to develop and safeguard their information.

Whatever it is, how does this effect push APT meetings forward? Where do APT meetings go? Do they change their objectives? Will they be united or increasingly collective to overcome the new difficulties they face?

The future of Advance Persistent Threats includes Capability, Capacity and Cost.

Capability

Capabilities are fundamentally broader nowadays, and gradually more powerful and competent process innovations, equipment, and programs are being rolled out into practice every day. This improvement in innovation empowers APTs to improve their current capabilities in the same way that they try to misuse new ones.

For example, the incorporation of Industry 4.0 and Smart City will soon provide unlimited opportunities for teams to join IoT gadgets and sensor APT meetings.
This can be misused to register a confusing volume of artificial intelligence (AI) as a single form.

Although unexpected, the gadget is essentially made of scars or insecurities, for example, weak passwords that cannot be changed, and the mass of gadgets currently available will expand the vulnerability. This will result in more powerful meetings than trying to misuse it.

While the USA presently flaunts the quickest supercomputer on the planet, this was just an ongoing honor subsequent to thumping China off of a multi-year strength at the top-spot. Be that as it may, this has prodded China to put resources into a multi-billion-dollar program planned for overhauling their current abilities throughout the following three years to recapture the title.

In addition, in a Twitter message, the state of Iran states that they will use all the resources to create an all-encompassing supercomputer that can be used by APT33, thus ensuring that they are aware of the development and development of innovation.

However, as these PCs accelerate significantly, it can significantly affect current encryption guidelines, making it less time-consuming. Instead of hundreds of years. This is a prerequisite for new principles of encryption.

With Super PCs, for example, nowadays used in the world, and perhaps the fastest supercomputer in the country of the premier APT meeting, one can rest assured that the digital arms race is ahead.

Capacity

As noted in various outlets around the world over the past year, there is a dearth of digital capabilities worldwide to estimate agency in the range of 1.8 million and 3.5 million by 2022. This should certainly be of concern to anyone working in the digital security industry right now, raising concerns about outstanding work and potential burnout by business experts.

Nevertheless, is it enough to admit that the Advanced Persistent Threat group is facing this kind of shortage and that APT meetings are likewise open their eyes to the digital aptitude hole? As recently noted, a large number of new devices are being introduced through IoT and Industry 4.0, which can be very vulnerable. However, is there an option to focus on these in case APT meetings do not have the personnel employed to direct their activities?

The system can be advanced and robotized tons of times, but in spite of all it requires enough people with full information about the frames they are attacking. The robot meetings do not include the 'content children' we are comfortable with in their likeness of the robot, they have exceptional talents and fully proficient people, or groups that work for the ultimate goal.

Can the offerings continue to expand, the offensive philosophy broadens, and is there any hope that APT meetings have a place of immersion? Where is the lack of assets and labor to further their struggles with different businesses and begin to concentrate more on what they know?

To address the labor problem, there is the possibility of an expansion of APT gathering coordination and joint efforts, for example, risk knowledge sharing networks, where they deliver asset, devices and systems as high as possible. Or a large cash prize. All things considered, there are a few shadowy corners in the shade that are likely to turn out to be more common in the future, with APT gathering and the following becoming significantly closer. The less obvious guard.

Whenever we can earn some money, it is the APT meetings that keep each other's frame and each other's strategies, techniques and procedures (TTPs). This gives an unmistakable impression of the idea that the Internet is now as blocked as it is, and often concerns the Internet's general limit rather than the misuse of the Internet.

Cost

Governments and key industry pioneers who produce interesting information will continue to utilize resources for their secure security capabilities, particularly with the intent of ensuring critical national infrastructure. As these capabilities advance across the globe, the complexity of the objectives for APT meetings will often widen, leading to potential opportunities. Two potential scenarios are:

1. A shift in focus for APT group targets
2. A shift in APT groups alignment

Scenario one should see Meetings where business leaders and the government can adjust their concentrations focus on more of the low-hanging natural product - associations that are still industry pioneers in their important parts, but who are not as keen on their safety and in this way. Turn systematically targeted / unsafe.

Scenario two should see
You can also meet with other APT meetings or criminal meetings that have comparable interests. They begin to work more collaboratively, asset sharing, for example, personal and capabilities, which allows them to handle larger and more frequent attacks on crime. As a result, some of the accounts generated go to legitimate APT meetings to serve their specific purpose.

Given these Scenarios,
The last one is almost certain. Skilled meetings require staff and money to help with their exercises, and by working more closely or in direct coordination with other APTs or crime meetings, they consider everything that is considered, develop their abilities and speculate, along these lines. It is more effective and ensures that the blue groups are subsequently persecuted.

While these are briefly looking at two potential scenarios for APT meetings, the reality of the difficulties they face is much broader. While APT meetings usually seek to misuse political turmoil for their own motivation, the delegation of financial power can also significantly affect their objectives and procedures. Countries that endorse potential exchanges focus on the playground to eliminate potential.

In a summary,

While there are many other points to consider in regards to the fate of APT meetings, the above suggests that they are practically confident that they will achieve their goal. As new security measures are incorporated, there is little doubt that the way they are engaged will change in the future. Let us begin to gain a consistent understanding of the TTP in APT meetings.

Good meetings are now in our systems, our legislatures, and our associations, and they ensure that these systems can be closely connected in order to advance their own matters, whether strategically, financially or insightfully.

Moreover, the states of the country are giving their own motivation to achieve their financial or political matters, and so will the APT meetings as they advance their organizations or innovations to improve their capabilities.

As cyber security professionals
We need to understand that national security strategies, as well as APT meetings supporting the country, follow national regulation. By understanding these, we can begin to get a clearer picture of what the following steps are, in terms of geopolitical situations, and by leveraging digital danger knowledge to our broader digital capabilities.

From a security standpoint, the Internet is becoming increasingly blocked and we must continue to understand APT meetings, as the representation between one APT meeting and the following is always blurred. Keep expanding our understanding of the dangers that lie ahead and coming, but what does the risk scene look like over the next 18 - 24 years?

Conclusion

Advanced Persistent Threats are expanding each year with increasing levels of refinement. With the failure of many unions and governments to recognize and prevent these attacks governments are at huge risk of losing valuable data.

Re-exploring the difficulties of unpacking data frames, APT has identified 12 mitigation strategies by 25 researchers, and it is clear that there is a need to incorporate a portion of the work done and their adequacy-based techniques.

As its researchers have pointed out, the purpose of the use is uniquely affecting additions. Establishing a code of conduct, using relief strategies and realizing techniques will reduce false positives and improve APT mitigation capability.

It is better to increasing of focusing on the anomaly detection and monitor the network, pattern recognition and that will useful to prevent APTs.

References

- https://youtu.be/vXEGWlw8GSs
- https://youtu.be/Sqw_KJDsltA
- SearchSecurity. 2020. *What Is Advanced Persistent Threat (APT)? - Definition From Whatis.Com*. [online] Available at: <https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT> [Accessed 25 April 2020].
- En.wikipedia.org. 2020. *Advanced Persistent Threat*. [online] Available at: <https://en.wikipedia.org/wiki/Advanced_persistent_threat> [Accessed 25 April 2020].
- Platform, H., Instrumentation, V., Forensics, N., Security, E., Security, E., Demand, D., Demand, E., Defense, M., Intelligence, T., Services, F., Systems, I., Assessment, C., Assessments, C., Assessment, R., Assessments, P., Assessment, S., Assessment, R., Exercise, T., Testing, P., Development, C., Services, D., Operations, C., Defense, M., Services, I., Retainer, I., Product, I., Exercise, T., Stories, C., Success, C., Portal, C., Support, C., Programs, S., Notices, S., Products, S., Portal, D., Overview, P., Resellers, F., Partners, T., Partners, C., Providers, G., Locator, P., Center, P., Partner, B., Reports, A., Reports, T., Industry, T., Groups, A., Blogs, R., Security?, W., Platform, O., Email, N., Expertise, O., Magazine, T., Downloads, F., Market, F., Training, E., FireEye?, W., Honors, A., Directors, B., Relations, I., Releases, P., Opportunities, J., FireEye, C. and Threats, A., 2020. *Anatomy Of An APT (Advanced Persistent Threat) Attack* | *Fireeye*. [online] FireEye. Available at: <https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html> [Accessed 25 April 2020].
- Platform, H., Instrumentation, V., Forensics, N., Security, E., Security, E., Demand, D., Demand, E., Defense, M., Intelligence, T., Services, F., Systems, I., Assessment, C., Assessments, C., Assessment, R., Assessments, P., Assessment, S., Assessment, R., Exercise, T., Testing, P., Development, C., Services, D., Operations, C., Defense, M., Services, I., Retainer, I., Product, I., Exercise, T., Stories, C., Success, C., Portal, C., Support, C., Programs, S., Notices, S., Products, S., Portal, D., Overview, P., Resellers, F., Partners, T., Partners, C., Providers, G., Locator, P., Center, P., Partner, B., Reports, A., Reports, T., Industry, T., Groups, A., Blogs, R., Security?, W., Platform, O., Email, N., Expertise, O., Magazine, T., Downloads, F., Market, F., Training, E., FireEye?, W., Honors, A., Directors, B., Relations, I., Releases, P., Opportunities, J., FireEye, C. and Groups, A., 2020. *Advanced Persistent Threat Groups* | *Fireeye*. [online] FireEye. Available at: <https://www.fireeye.com/current-threats/apt-groups.html> [Accessed 25 April 2020].

- Adelaiye, O., Showole, A. and Faki, S., 2020. *Evaluating Advanced Persistent Threats Mitigation Effects:A Review*. [online] Semanticscholar.org. Available at: <https://www.semanticscholar.org/paper/Evaluating-Advanced-Persistent-Threats-Mitigation-Adelaiye-Showole/9c676cc552acd1bee282b106b11c756d20cc4886> [Accessed 25 April 2020].
- Grimes, R., 2020. *What Is An Advanced Persistent Threat (APT)? 5 Signs You've Been Hit*. [online] CSO Online. Available at: <https://www.csoonline.com/article/2615666/5-signs-youve-been-hit-with-an-apt.html> [Accessed 25 April 2020].
- Us, A., Services, O., Collaboration, U., Management, I., Management, N., Services, M., Security, I., Testing, C., Recovery, D. and Us, C., 2020. *Advanced Persistent Threat Protection: 7 Ways To Prevent APT Attacks | Solid State Systems LLC*. [online] Solid State Systems LLC. Available at: <http://solidsystemsllc.com/advanced-persistent-threat-protection/> [Accessed 25 April 2020].
- Threats, H. and Hernandez, P., 2020. *How To Stop Advanced Persistent Threats*. [online] Esecurityplanet.com. Available at: <https://www.esecurityplanet.com/threats/how-to-stop-advanced-persistent-threats.html> [Accessed 25 April 2020].
- Kaspersky.com. 2020. *5 Warning Signs Of Advanced Persistent Threat | Tips To Prevent APT | Kaspersky*. [online] Available at: <https://www.kaspersky.com/resource-center/threats/advanced-persistent-threat> [Accessed 25 April 2020].
  F, R., 2020. *Telesoft Technologies - The APT Series - The Future Of Advanced Persistent Threat Groups*. [online] Telesoft-technologies.com. Available at: <https://www.telesoft-technologies.com/blog/item/the-apt-series-part-3-the-future-of-advanced-persistent-threat-groups> [Accessed 25 April 2020].