Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Advanced Persistent Threats

What are they and do they really exist?

Audience: General

Reading Time: 10 Mins

The use of the term Advanced Persistent Threat has been on the rise lately, as more evidence is shared that not only proves they exist, but they are actively attacking targets

Advanced Persistent Threats are being utilised by organised criminals and are often developed/sponsored by nation states for a variety of different reasons. Some nation states encourage hacking activities on an individual and group level, often paying hackers a salary to: steal intellectual property, gather personal data or more simply, reward hackers for successful fraudulent activities designed to re-appropriate wealth.[2]

How do we know APT's exist?

Many sophisticated and targeted attacks have come to light over the past decade, including, Operation Aurora and Stuxnet.[4] Hacking groups use the same Tactics, Techniques and Procedures (often referred to as TTP's) time and again on multiple targets. Multiple investigations by cyber security researchers from all around the world lead back to the same source despite many of these investigations happening without knowledge of the other parties.[5]

Once these targets start to share information about an attack, the TTP's overlap and the evidence often produces a clear narrative of the attack and description of the attackers.[10] The group will then be given a name, such as; "'Fancy Bear' APT28", so that cyber analysts can do their job more effectively and align individual attacks to likely responsible parties.[7]

Who are the most active state sponsors?

China, Russia, Iran and North Korea (CRINK) have been the most prominent countries, however, there is evidence that western countries have also setup APTs.[1] This includes the United States (DoD & CIA), the United Kingdom (GCHQ & MI6) and Israel. The victims of the attacks made by the western groups

European Union
European Regional Development Fund
Manchester Metropolitan University
MANCHESTER 1824 The University of Manchester
University of Salford MANCHESTER
Lancaster University

have been mostly at a government level, these include; Iran, ISIS and Belgium.[1] Whereas the attacks made by CRINK are known to target governments, charities, companies and organisations.[5] The most famous of these would be the attack on the NHS, WannaCry; produced by North Korea.[9]

Is it impossible to protect against a state sponsored attack?

Although it is true that many state sponsored hacking groups use zero-day vulnerabilities, it is not impossible to protect yourself from these attacks.[10] Many attacks exploit vulnerabilities that penetrate the outer layer of a company's security. If your security is setup correctly to detect and/or prevent privilege escalation, it is possible to become aware very quickly that an APT is inside your system and lock them out. Many experts use an onion to explain the layers of security. At each layer there should be a clear wall or barrier that prevents and detects movement, this allows you to track and remove attackers inside of your system even if there was no way to prevent them from the initial penetration.[3]

What motivates state sponsored hacking groups?

The vast majority of attacks are financially motivated. Some countries are under very heavy scrutiny and/or sanctions regarding their international trade. This makes producing wealth in that country a difficult task for the government in charge.

We all know that certain nation states sponsor activities such as human trafficking and even kidnapping, cyber espionage can almost be seen as a victimless crime by comparison.[11] Those involved do not feel the same sort of responsibility or guilt associated with their criminal activities, as the internet creates a barrier between the digital and our real world.
However, other nations are motivated by the theft of intellectual property and/or personal data. For example; source code, military schematics, healthcare data and personal information on targeted individuals. Many of the intellectual property theft attacks aim to stay on the victim's system for as long as possible and concentrate on exfiltration of documents over a prolonged period.

What motivates the individuals involved in these hacking groups?

Unlike most countries in the west where cyber security jobs can offer a very competitive salary, many nations struggle to have the same sort of infrastructure regarding the variety of positions and fair wages offered for such work.

Definitions

Zero-day vulnerabilities

A Zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software).

Privilege escalation

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

Exfiltration

Data exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various techniques, typically by cyber criminals over the Internet.

Finding Support

In many instances, running a cyber security firm in a country like China or Russia will mean that only Chinese or Russian companies would ever consider your services. Whereas a similar company in America will have worldwide clients and be able to ask a lot more for their services.

Talented hackers can wear many hats, they do not necessarily need to be criminals. However, if your country offers you a job with a far higher salary than what would or could be achieved by a private company[8], it is often very easy to go down the path of becoming an international criminal.

The other side to this is that many countries do not consider your actions criminal if you are working against foreign 'enemy' states. Although you may be considered an international criminal, if you never leave your home country you will never face charges for your activity. It is very rare for a country to extradite a hacker to an 'enemy' foreign nation.

Do we know who these criminal hackers are?

Yes, the FBI has a website that lists their most wanted cyber criminals at: www.fbi.gov/wanted/cyber - it is well known that appearing on this list has massive consequences and will drastically reduce your ability to freely travel around the world.[2] Many famous individuals have appeared on such lists and then been detained by foreign nations before being extradited to the United States.

The most famous could be considered Pyotr Levashov; while on vacation in Barcelona the Spanish National Police arrested him and then extradition to the United States was approved several months later. There was also a rejected extradition request made by the Russian government.[6]

How Can Your Business Navigate The Cyber Challenges Of 2020?

The Greater Manchester Cyber Foundry runs a Secure Digitalisation Programme designed to support businesses facing cyber challenges in Greater Manchester. The programme consists of two full-day workshops, alongside online open learning elements. In addition, enrolling gives you access to our digital portal full of cyber innovation tools and services to better defend, innovate and grow your business.

Image: Helena Lopes on Unsplash

The course aims to teach the basics of secure digitalisation before going on to explore how you and your business could grow and thrive through cyber innovation. Participation in this has the potential to lead to a bespoke technical assist in cyber innovation from one of our dedicated technical teams from a partner university.

The support is free due to being part funded by the European Regional Development Fund, and is in partnership with Lancaster University, the University of Manchester, Manchester Metropolitan University, and Salford University.

To find out more about how your business can access support and register on one of upcoming cohorts contact us:

gmcyberfoundry@lancaster.ac.uk

Further Reading

About the Author

Robert Marsh is a published Internet of Things Forensics Researcher and an award-winning Artificial Intelligence Software Developer. He is currently working as a Cyber Security Analyst with the Greater Manchester Cyber Foundry technical team at The University of Salford.

READ MORE

1. "APT Index." Kumu, 14 Aug. 2019, embed.kumu.io/0b023bf1a971ba32510e86e8f1a38c38
2. "Cyber's Most Wanted." FBI, FBI, 28 Aug. 2010, www.fbi.gov/wanted/cyber
3. Fowler, Sitima. "Cybersecurity is like an onion." Rochester Democrat and Chronicle, ROC, 4 Oct. 2016, eu.democratandchronicle.com/story/money/business/blogs/innovation/2016/10/04/cybersecurity-is-like-an-onion/91543960/
4. Fruhlinger, Josh. "What Is Stuxnet, Who Created It and How Does It Work?" CSO Online, CSO, 22 Aug. 2017, www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html
5. "A New Approach to China." Official Google Blog, 12 Jan. 2010, googleblog.blogspot.com/2010/01/new-approach-to-china.html
6. "Suspected Spam King Extradited to US." Voice of America, www.voanews.com/silicon-valley-technology/suspected-spam-king-extradited-us
7. Team, Editorial. "Fancy Bear Hackers (APT28): Targets & Methods." CrowdStrike, 13 May 2019, www.crowdstrike.com/blog/who-is-fancy-bear/
8. Weissman, Cale Guthrie. "Some Hackers Make More than $80,000 a Month - Here's How." Business Insider, Business Insider, 14 July 2015, www.businessinsider.com/we-found-out-how-much-money-hackers-actually-make-2015-7?r=US&IR=T#the-business-model-5
9. Kiruri, K. And Kamau, L., 2018. Lessons On Cyber Security: A Case Study Of Wannacry Ransomware. In Jkuat Annual Scientific Conference Proceedings (Pp. 192-198)
10. Barnum, S., 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corporation, 11, pp.1-22
11. Creech, G., 2014. Developing a high-accuracy cross platform Host-Based Intrusion Detection System capable of reliably detecting zero-day attacks (Doctoral dissertation, University of New South Wales, Canberra, Australia)
12. Lutscher, P., 2020. Digital Responses to Sanctions? Denial-of-Service Attacks against Sender Countries. SocArXiv.

European Union
European Regional Development Fund
Manchester Metropolitan University
MANCHESTER 1824 The University of Manchester
University of Salford MANCHESTER
Lancaster University