# Advanced persistent threat

An **advanced persistent threat** (**APT**) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.[1][2] In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals.[3]

Such threat actors' motivations are typically political or economic.[4] Every major business sector has recorded instances of cyberattacks by advanced actors with specific goals, whether to steal, spy, or disrupt. These targeted sectors include government, defense, financial services, legal services, industrial, telecoms, consumer goods and many more.[5][6][7] Some groups utilize traditional espionage vectors, including social engineering, human intelligence and infiltration to gain access to a physical location to enable network attacks. The purpose of these attacks is to install custom malware (malicious software).[8]

The median "dwell-time", the time an APT attack goes undetected, differs widely between regions. FireEye reported the mean dwell-time for 2018 in the Americas as 71 days, EMEA as 177 days, and APAC as 204 days.[5] Such a long dwell-time allows attackers a significant amount of time to go through the attack cycle, propagate, and achieve their objective.

## Contents



## Definition

Definitions of precisely what an APT is can vary, but can be summarized by their named requirements below:

- *Advanced* – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include commercial and open source computer intrusion technologies and techniques, but may also extend to include the intelligence apparatus of a state. While individual components of the attack may not be considered particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.[3][9][10]
- *Persistent* – Operators have specific objectives, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. If the operator loses access to their target they usually will reattempt access, and most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats who only need access to execute a specific task.[9][11]
- *Threat* – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well funded. Actors are not limited to state sponsored groups.[3][9]

# History and targets

Warnings against targeted, socially-engineered emails dropping trojans to exfiltrate sensitive information were published by UK and US CERT organisations in 2005. This method was used throughout the early 1990s and does not in itself constitute an APT. The term "advanced persistent threat" has been cited as originating from the United States Air Force in 2006[12] with Colonel Greg Rattray cited as the individual who coined the term.[13]

The Stuxnet computer worm, which targeted the computer hardware of Iran's nuclear program, is one example of an APT attack. In this case, the Iranian government might consider the Stuxnet creators to be an advanced persistent threat.[14]

Within the computer security community, and increasingly within the media, the term is almost always used in reference to a long-term pattern of sophisticated computer network exploitation aimed at governments, companies, and political activists, and by extension, also to ascribe the A, P and T attributes to the groups behind these attacks.[15] Advanced persistent threat (APT) as a term may be shifting focus to computer-based hacking due to the rising number of occurrences. PC World reported an 81 percent increase from 2010 to 2011 of particularly advanced targeted computer attacks.[16]

Actors in many countries have used cyberspace as a means to gather intelligence on individuals and groups of individuals of interest.[17][18][19] The United States Cyber Command is tasked with coordinating the US military's offensive and defensive cyber operations.[20]

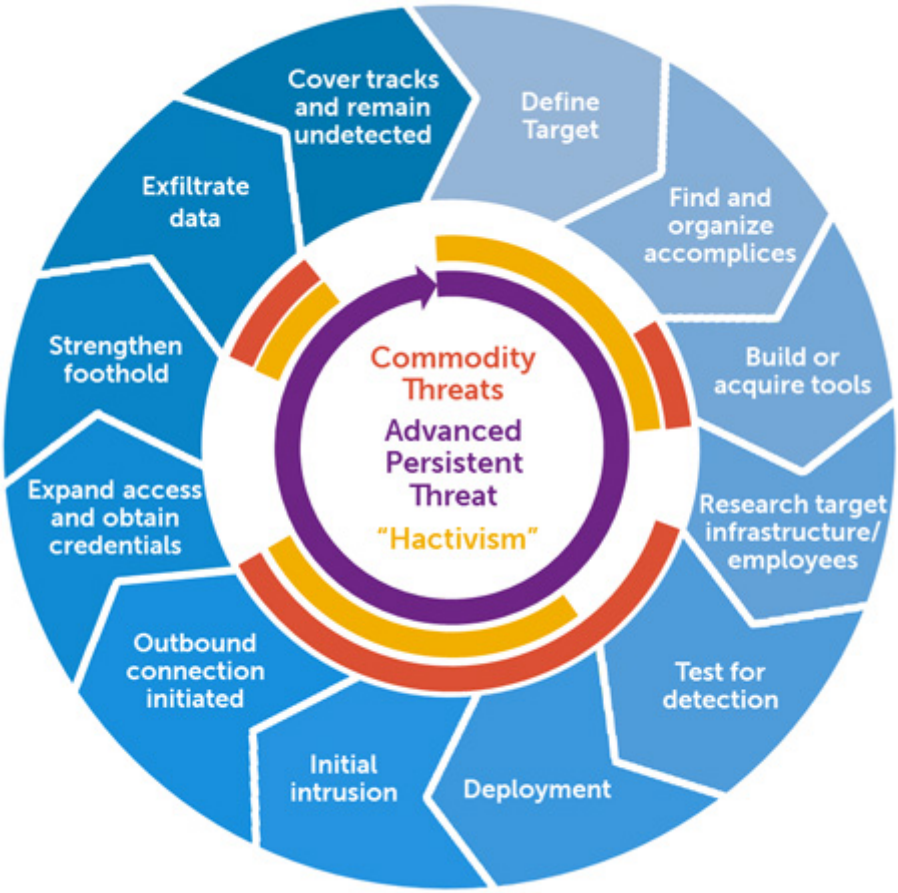
Numerous sources have alleged that some APT groups are affiliated with, or are agents of, governments of sovereign states.[21][22][23] Businesses holding a large quantity of personally identifiable information are at high risk of being targeted by advanced persistent threats, including:[24]

- Higher education[25]
- Financial institutions
- Energy
- Transportation
- Technology
- Health care
- Telecommunications
- Manufacturing
- Agriculture[26]

A Bell Canada study provided deep research into the anatomy of APTs and uncovered widespread presence in Canadian government and critical infrastructure. Attribution was established to Chinese and Russian actors.[27]

## Life cycle

Actors behind advanced persistent threats create a growing and changing risk to organizations' financial assets, intellectual property, and reputation[28] by following a continuous process or kill chain:




1. Target specific organizations for a singular objective
2. Attempt to gain a foothold in the environment (common tactics include spear phishing emails)
3. Use the compromised systems as access into the target network
4. Deploy additional tools that help fulfill the attack objective
5. Cover tracks to maintain access for future initiatives

The global landscape of APT's from all sources is sometimes referred to in the singular as "the" APT, as are references to the actor behind a specific incident or series of incidents, but the definition of APT includes both actor and method.[29]

In 2013, Mandiant presented results of their research on alleged Chinese attacks using APT method between 2004 and 2013[30] that followed similar lifecycle:

- **Initial compromise** – performed by use of social engineering and spear phishing, over email, using zero-day viruses. Another popular infection method was planting malware on a website that the victim's employees will be likely to visit.
- **Establish foothold** – plant remote administration software in victim's network, create net backdoors and tunnels allowing stealth access to its infrastructure.
- **Escalate privileges** – use exploits and password cracking to acquire administrator privileges over victim's computer and possibly expand it to Windows domain administrator accounts.
- **Internal reconnaissance** – collect information on surrounding infrastructure, trust relationships, Windows domain structure.
- **Move laterally** – expand control to other workstations, servers and infrastructure elements and perform data harvesting on them.
- **Maintain presence** – ensure continued control over access channels and credentials acquired in previous steps.
- **Complete mission** – exfiltrate stolen data from victim's network.

In incidents analysed by Mandiant, the average period over which the attackers controlled the victim's network was one year, with longest – almost five years.[30] The infiltrations were allegedly performed by Shanghai-based Unit 61398 of People's Liberation Army. Chinese officials have denied any involvement in these attacks.[31]

Previous reports from Secdev had previously discovered and implicated Chinese actors.[32]

# Mitigation strategies

There are tens of millions of malware variations,[33] which makes it extremely challenging to protect organizations from APT. While APT activities are stealthy and hard to detect, the command and control network traffic associated with APT can be detected at the network layer level with sophisticated methods. Deep log analyses and log correlation from various sources is of limited usefulness in detecting APT activities. It is challenging to separate noises from legitimate traffic. Traditional security technology and methods have been ineffective in detecting or mitigating APTs.[34] Active cyber defense has yielded greater efficacy in detecting and prosecuting APTs (find, fix, finish) when applying cyber threat intelligence to hunt and adversary pursuit activities.[35][36] Human-Introduced Cyber Vulnerabilities (HICV) are a weak cyber link that are neither well understood nor mitigated, constituting a significant attack vector.[37]

# APT groups

## China

Since Xi Jinping became General Secretary of the Chinese Communist Party in 2012, the Ministry of State Security gained more responsibility over cyberespionage vis-à-vis the People's Liberation Army, and currently oversees various APT groups.[38] According to security researcher Timo Steffens "The APT

landscape in China is run in a 'whole country' approach, leveraging skills from universities, individual, and private and public sectors."[39]

- PLA Unit 61398 (also known as APT1)
- PLA Unit 61486 (also known as APT2)
- Buckeye (also known as APT3)[40]
- Red Apollo (also known as APT10)
- Numbered Panda (also known as APT12)
- DeputyDog (also known as APT17)[41]
- Codoso Team (also known as APT19)
- Wocao (also known as APT20)[42][43]
- APT 27[44]
- PLA Unit 78020 (also known as APT30 and Naikon)
- Zirconium[45] (also known as APT31)[46]
- Periscope Group (also known as APT40)
- Double Dragon[47] (also known as APT41, Winnti Group, Barium, or Axiom)[48][49][50]
- Tropic Trooper[51][52]
- Hafnium[53][54]

## Iran

- Elfin Team (also known as APT33)
- Helix Kitten (also known as APT34)
- Charming Kitten (also known as APT35)
- APT39
- Pioneer Kitten[55]

## Israel

- Unit 8200

## North Korea

- Kimsuky
- Lazarus Group (also known as APT38)
- Ricochet Chollima (also known as APT37)

## Russia

- Fancy Bear (also known as APT28)
- Cozy Bear (also known as APT29)
- Sandworm
- Berserk Bear
- FIN7
- Venomous Bear

### United States

- Equation Group[56]

### Uzbekistan

- SandCat (associated with the National Security Service (Uzbekistan))[57]

### Vietnam

- OceanLotus (also known as APT32)[58][59]

## See also

- Bureau 121
- Chinese intelligence activity abroad
- Cyber spying
- Darkhotel
- Fileless malware
- Ghostnet
- Kill chain
- NetSpectre
- Operation Aurora
- Operation Shady RAT
- Proactive cyber defence
- Spear-phishing
- Spyware
- Stuxnet
- Tailored Access Operations
- Unit 180
- Unit 8200

## References


1. "What Is an Advanced Persistent Threat (APT)?" (https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats). *www.kaspersky.com*. Retrieved 11 August 2019.
2. "What Is an Advanced Persistent Threat (APT)?" (https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html). *Cisco*. Retrieved 11 August 2019.
3. Maloney, Sarah. "What is an Advanced Persistent Threat (APT)?" (https://www.cybereason.com/blog/advanced-persistent-threat-apt). Retrieved 9 November 2018.
4. Cole., Eric (2013). *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization* (http://worldcat.org/oclc/939843912). Syngress. OCLC 939843912 (https://www.worldcat.org/oclc/939843912).
5. "M-Trends Cyber Security Trends" (https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html). *FireEye*. Retrieved 11 August 2019.
6. "Cyber Threats to the Financial Services and Insurance Industries" (https://web.archive.org/web/20190811091624/https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/ib-finance.pdf) (PDF). *FireEye*. Archived from the original (https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/ib-finance.pdf) (PDF) on 11 August 2019.
7. "Cyber Threats to the Retail and Consumer Goods Industry" (https://web.archive.org/web/20190811091947/https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/ib-retail-consumer.pdf) (PDF). *FireEye*. Archived from the original (https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/ib-retail-consumer.pdf) (PDF) on 11 August 2019.

8. "Advanced Persistent Threats: A Symantec Perspective" (https://web.archive.org/web/20180508161501/https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf) (PDF). *Symantec*. Archived from the original (https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf) (PDF) on 8 May 2018.
9. "Advanced Persistent Threats (APTs)" (https://www.itgovernance.co.uk/advanced-persistent-threats-apt). *IT Governance*.
10. "Advanced persistent Threat Awareness" (https://www.trendmicro.co.uk/media/misc/apt-survey-report-en.pdf) (PDF). *TrendMicro Inc*.
11. "Explained: Advanced Persistent Threat (APT)" (https://blog.malwarebytes.com/101/2016/07/explained-advanced-persistent-threat-apt/). *Malwarebytes Labs*. 26 July 2016. Retrieved 11 August 2019.
12. "Assessing Outbound Traffic to Uncover Advanced Persistent Threat" (https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf) (PDF). SANS Technology Institute. Retrieved 14 April 2013.
13. "Introducing Forrester's Cyber Threat Intelligence Research" (https://web.archive.org/web/20140415054512/http://blogs.forrester.com/rick_holland/13-02-14-introducing_forresters_cyber_threat_intelligence_research). Forrester Research. Archived from the original (http://blogs.forrester.com/rick_holland/13-02-14-introducing_forresters_cyber_threat_intelligence_research) on 15 April 2014. Retrieved 14 April 2014.
14. Beim, Jared (2018). "Enforcing a Prohibition on International Espionage" (https://search.proquest.com/docview/2012381493). *Chicago Journal of International Law*. **18**: 647–672. ProQuest 2012381493 (https://search.proquest.com/docview/2012381493).
15. "Advanced Persistent Threats: Learn the ABCs of APTs - Part A" (https://www.secureworks.com/blog/advanced-persistent-threats-apt-a). *SecureWorks*. SecureWorks. Retrieved 23 January 2017.
16. Olavsrud, Thor (30 April 2012). "Targeted Attacks Increased, Became More Diverse in 2011" (https://www.cio.com/article/2396583/targeted-attacks-increased--became-more-diverse-in-2011.html). *CIO Magazine*.
17. "An Evolving Crisis" (https://web.archive.org/web/20100110120647/http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm). BusinessWeek. 10 April 2008. Archived from the original (http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm) on 10 January 2010. Retrieved 20 January 2010.
18. "The New E-spionage Threat" (https://web.archive.org/web/20110418080952/http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm). BusinessWeek. 10 April 2008. Archived from the original (http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm) on 18 April 2011. Retrieved 19 March 2011.
19. Rosenbach, Marcel; Schulz, Thomas; Wagner, Wieland (19 January 2010). "Google Under Attack: The High Cost of Doing Business in China" (https://www.spiegel.de/international/world/google-under-attack-the-high-cost-of-doing-business-in-china-a-672742.html). *Der Spiegel*. Archived (https://web.archive.org/web/20100121005238/http://www.spiegel.de/international/world/0%2C1518%2C672742%2C00.html) from the original on 21 January 2010. Retrieved 20 January 2010.
20. "Commander Discusses a Decade of DOD Cyber Power" (https://www.defense.gov/Explore/News/Article/Article/2193130/commander-discusses-a-decade-of-dod-cyber-power/). *U.S. DEPARTMENT OF DEFENSE*. Retrieved 28 August 2020.

21. "Under Cyberthreat: Defense Contractors" (https://www.bloomberg.com/news/articles/2009-07-06/under-cyberthreat-defense-contractorsbusinessweek-business-news-stock-market-and-financial-advice). *Bloomberg.com*. BusinessWeek. 6 July 2009. Archived (https://web.archive.org/web/20100111174243/http://www.businessweek.com/technology/content/jul2009/tc2009076_873512.htm) from the original on 11 January 2010. Retrieved 20 January 2010.
22. "Understanding the Advanced Persistent Threat" (http://tominfosec.blogspot.com/2010/02/understanding-apt.html). Tom Parker. 4 February 2010. Retrieved 4 February 2010.
23. "Advanced Persistent Threat (or Informationized Force Operations)" (https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf) (PDF). Usenix, Michael K. Daly. 4 November 2009. Retrieved 4 November 2009.
24. "Anatomy of an Advanced Persistent Threat (APT)" (https://www.secureworks.com/resources/sb-advanced-threat-protection-with-dell-secureworks). Dell SecureWorks. Retrieved 21 May 2012.
25. Ingerman, Bret; Yang, Catherine (31 May 2011). "Top-Ten IT Issues, 2011" (https://er.educause.edu/articles/2011/5/topten-it-issues-2011). Educause Review.
26. Gonzalez, Joaquin Jay, III; Kemp, Roger L. (16 January 2019). *Cybersecurity: Current Writings on Threats and Protection* (https://books.google.com/books?id=FyuFDwAAQBAJ&pg=PA69). McFarland. p. 69. ISBN 9781476674407.
27. McMahon, Dave; Rohozinski, Rafal. "The Dark Space Project: Defence R&D Canada – Centre for Security Science Contractor Report DRDC CSS CR 2013-007" (http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf) (PDF). *publications.gc.ca*. Archived (https://web.archive.org/web/20161105035412/http://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-3-007-2013-eng.pdf) (PDF) from the original on 5 November 2016. Retrieved 1 April 2021.
28. "Outmaneuvering Advanced and Evasive Malware Threats" (https://www.secureworks.com/resources/wp-outmaneuvering-advanced-and-evasive-malware-threats). *Secureworks*. Secureworks Insights. Retrieved 24 February 2016.
29. EMAGCOMSECURITY (9 April 2015). "APT (Advanced Persistent Threat) Group" (https://emagcomsecurity.wordpress.com/2015/04/09/apt-advanced-persistent-threat-group//). Retrieved 15 January 2019.
30. "APT1: Exposing One of China's Cyber Espionage Units" (http://intelreport.mandiant.com/). Mandiant. 2013.
31. Blanchard, Ben (19 February 2013). "China says U.S. hacking accusations lack technical proof" (https://www.reuters.com/article/us-china-hacking-idUSBRE91I06120130220). Reuters.
32. "GhostNet" was a large-scale cyber spying operation" (http://www.nartv.org/mirror/ghostnet.pdf) (PDF).
33. RicMessier (30 October 2013). *GSEC GIAC Security Essentials Certification All* (https://books.google.com/books?id=zUdZAQAAQBAJ&pg=PR25). McGraw Hill Professional, 2013. p. xxv. ISBN 9780071820912.
34. "Anatomy of an APT (Advanced Persistent Threat) Attack" (https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html). *FireEye*. Retrieved 14 November 2020.
35. "Threat Intelligence in an Active Cyber Defense (Part 1)" (https://www.recordedfuture.com/active-cyber-defense-part-1/). *Recorded Future*. 18 February 2015. Retrieved 10 March 2021.
36. "Threat Intelligence in an Active Cyber Defense (Part 2)" (https://www.recordedfuture.com/active-cyber-defense-part-2/). *Recorded Future*. 24 February 2015. Retrieved 10 March 2021.
37. "A Context-Centred Research Approach to Phishing and Operational Technology in Industrial Control Systems | Journal of Information Warfare" (https://www.jinfowar.com/journal/volume-18-issue-4/context-centred-research-approach-phishing-operational-technology-industrial-control-systems). *www.jinfowar.com*. Retrieved 31 July 2021.

38. Mozur, Paul; Buckley, Chris (26 August 2021). "Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship" (https://www.nytimes.com/2021/08/26/technology/china-hackers.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 27 August 2021.
39. Stone, Jeff (5 October 2020). "Foreign spies use front companies to disguise their hacking, borrowing an old camouflage tactic" (https://www.cyberscoop.com/chinese-iranian-hackers-front-companies/). *cyberscoop.com*. Cyberscoop. Retrieved 11 October 2020.
40. "Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak" (https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit). Symantec. 7 May 2019. Archived (https://archive.today/20190507054409/https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit) from the original on 7 May 2019. Retrieved 23 July 2019.
41. "APT17: Hiding in Plain Sight - FireEye and Microsoft Expose Obfuscation Tactic" (https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf) (PDF). *FireEye*. May 2015.
42. van Dantzig, Maarten; Schamper, Erik (19 December 2019). "Wocao APT20" (https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wocao.pdf) (PDF). *fox-it.com*. NCC Group.
43. Vijayan, Jai (19 December 2019). "China-Based Cyber Espionage Group Targeting Orgs in 10 Countries" (https://www.darkreading.com/attacks-breaches/china-based-cyber-espionage-group-targeting-orgs-in-10-countries/d/d-id/1336676). *www.darkreading.com*. Dark Reading. Retrieved 12 January 2020.
44. Lyngaas, Sean (10 August 2021). "Chinese hackers posed as Iranians to breach Israeli targets, FireEye says" (https://www.cyberscoop.com/china-israel-iran-fireeye-hacking/). *www.cyberscoop.com*. Retrieved 15 August 2021.
45. Lyngaas, Sean (12 February 2019). "Right country, wrong group? Researchers say it wasn't APT10 that hacked Norwegian software firm" (https://www.cyberscoop.com/apt10-apt31-recorded-future-rapid7-china/). *www.cyberscoop.com*. Cyberscoop. Retrieved 16 October 2020.
46. Lyngaas, Sean (16 October 2020). "Google offers details on Chinese hacking group that targeted Biden campaign" (https://www.cyberscoop.com/biden-chinese-hacking-google-security-russia/). *Cyberscoop*. Retrieved 16 October 2020.
47. "Double Dragon APT41, a dual espionage and cyber crime operation" (https://content.fireeye.com/apt-41/rpt-apt41/). *FireEye*. 16 October 2019. Retrieved 14 April 2020.
48. "Bureau names ransomware culprits" (https://www.taipeitimes.com/News/taiwan/archives/2020/05/17/2003736564). *www.taipeitimes.com*. Taipei Times. 17 May 2020. Retrieved 22 May 2020.
49. Tartare, Mathieu; Smolár, Martin (21 May 2020). "No "Game over" for the Winnti Group" (https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/). *www.welivesecurity.com*. We Live Security. Retrieved 22 May 2020.
50. Greenberg, Andy (6 August 2020). "Chinese Hackers Have Pillaged Taiwan's Semiconductor Industry" (https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/). *Wired*. Retrieved 7 August 2020.
51. Chen, Joey (12 May 2020). "Tropic Trooper's Back: USBferry Attack Targets Air-gapped Environments" (https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments/). *blog.trendmicro.com*. Trend Micro. Retrieved 16 May 2020.
52. Cimpanu, Catalin. "Hackers target the air-gapped networks of the Taiwanese and Philippine military" (https://www.zdnet.com/article/hackers-target-the-air-gapped-networks-of-the-taiwanese-and-philippine-military/). *ZDnet*. Retrieved 16 May 2020.

53. Naraine, Ryan (2 March 2021). "Microsoft: Multiple Exchange Server Zero-Days Under Attack by Chinese Hacking Group" (https://www.securityweek.com/microsoft-4-exchange-server-zero-days-under-attack-chinese-apt-group). *securityweek.com*. Wired Business Media. Retrieved 3 March 2021.
54. Burt, Tom (2 March 2021). "New nation-state cyberattacks" (https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/). *blogs.microsoft.com*. Microsoft. Retrieved 3 March 2021.
55. "Pioneer Kitten APT Sells Corporate Network Access" (https://threatpost.com/pioneer-kitten-apt-sells-corporate-network-access/158833/). *threatpost.com*.
56. "Equation: The Death Star of Malware Galaxy" (https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/). Kaspersky Lab. 16 February 2015. Archived (https://web.archive.org/web/20190711082936/https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/) from the original on 11 July 2019. Retrieved 23 July 2019.
57. Gallagher, Sean (3 October 2019). "Kaspersky finds Uzbekistan hacking op… because group used Kaspersky AV" (https://arstechnica.com/information-technology/2019/10/kaspersky-finds-uzbekistan-hacking-opbecause-they-used-kaspersky-av/). *arstechnica.com*. Ars Technica. Retrieved 5 October 2019.
58. Panda, Ankit. "Offensive Cyber Capabilities and Public Health Intelligence: Vietnam, APT32, and COVID-19" (https://thediplomat.com/2020/04/offensive-cyber-capabilities-and-public-health-intelligence-vietnam-apt32-and-covid-19/). *thediplomat.com*. The Diplomat. Retrieved 29 April 2020.
59. Tanriverdi, Hakan; Zierer, Max; Wetter, Ann-Kathrin; Biermann, Kai; Nguyen, Thi Do (8 October 2020). Nierle, Verena; Schöffel, Robert; Wreschniok, Lisa (eds.). "Lined up in the sights of Vietnamese hackers" (https://web.br.de/interaktiv/ocean-lotus/en/). Bayerischer Rundfunk. "In Bui's case the traces lead to a group presumably acting on behalf of the Vietnamese state. Experts have many names for this group: APT 32 and Ocean Lotus are best known. In conversations with a dozen of information security specialists, they all agreed that this is a Vietnamese group spying, in particular, on its own compatriots."

# Further reading

- Gartner Best Practices for Mitigating Advanced Persistent Threats (http://sites.miis.edu/cysec/files/2014/01/Best-Practices-for-Mitigating-Advanced-Persistent-Threats.pdf)
- Bell Canada, Combating Robot Networks and Their Controllers: PSTP08-0107eSec 06 May 2010 (PSTP) (https://www.scribd.com/document/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0)
- Prepare for 'post-crypto world', warns godfather of encryption (https://www.theregister.co.uk/2013/03/01/post_cryptography_security_shamir)
- Defence Research: The Dark Space Project APT0 (http://cradpdf.drdc-rddc.gc.ca/PDFS/unc159/p537638_A1b.pdf) Archived (https://web.archive.org/web/20200726160607/https://cradpdf.drdc-rddc.gc.ca/PDFS/unc159/p537638_A1b.pdf) 2020-07-26 at the Wayback Machine
- Gartner: Strategies for Dealing With Advanced Targeted Attacks (https://www.gartner.com/doc/2508415)
- XM Cyber: Remote file infection by an APT attack example (https://xmcyber.com/did-you-just-create-a-paradise-for-hackers/)
- Secdev, "GhostNet" was a large-scale cyber spying operation discovered in March 2009 (http://www.nartv.org/mirror/ghostnet.pdf)
- Secdev, "Shadows in the Cloud". A complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the Offices of the Dalai

Lama, the United Nations, and several other countries. (http://www.nartv.org/mirror/shadows-in-the-cloud.pdf)

### List of Advanced Persistent Threat Groups

- FireEye: Advanced Persistent Threat Groups (https://www.fireeye.com/current-threats/apt-groups.html)
- MITRE ATT&CK security community tracked Advanced Persistent Group Pages (https://attack.mitre.org/groups/)

---