Advanced Persistent Threats

Advanced persistent threats (APTs) are a class of threats that are far more deliberate and potentially devastating than other types of cyberattacks. As its name implies, an APT has three defining characteristics. An APT is:

Advanced. Attackers use advanced malware and exploits and typically also have the skills and resources necessary to develop additional cyberattack tools and techniques, and may have access to sophisticated electronic surveillance equipment, satellite imagery, and even human intelligence assets.

Persistent. An APT may take place over a period of several years. The attackers pursue specific objectives and use a "low-and-slow" approach to avoid detection. The attackers are well organized and typically have access to substantial financial backing, such as a nation-state or organized criminal organization, to fund their activities.

Threat. An APT is deliberate and focused, rather than opportunistic. APTs are designed to cause real damage. including significant financial loss, destruction of systems and infrastructure, and physical harm and loss of life.

Some recent APT threat actors include:

Lazarus (also known as APT38, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team, and Hidden Cobra).[1] The Lazarus APT group is a threat actor linked to North Korea and believed to be behind attacks against more than 16 organizations in at least 11 countries, including the Bangladesh cyber heist (US$81 million was surreptitiously transferred from the New York Federal Reserve Bank account of Bangladesh in February 2016),[2] the Troy Operation (attacks against South Korean infrastructure in 2013),[3] the DarkSeoul Operation (malware-based attacks that wiped tens of thousands of hard drives belonging to South Korean television networks and banks in March 2013),[4] and the Sony Picture hack (employees' emails and personal information including salaries, addresses, and Social Security numbers revealed, unreleased movies posted on file sharing sites, and internal computer systems shut down in 2014).[5]

[1] "Top 25 Threat Actors – 2019 Edition." SBS CyberSecurity. December 12, 2019. https://sbscyber.com/resources/top-25-threat-actors-2019-edition.

[2] Paganini, Pierluigi. "US blames North Korea for the $81 million Bangladesh cyber heist." Security Affairs. March 24, 2017. http://securityaffairs.co/wordpress/57396/cyber-crime/bangladesh-cyber-heist.html.

[3] Paganini, Pierluigi. "Hackers hit South Korea also spread spyware to steal military secrets." Security Affairs. July 9, 2013. http://securityaffairs.co/wordpress/16014/hacking/hackers-hit-south-korea-spyware-steal-military-secrets.html.

[4] Ibid.

[5] Weisman, Aly. "A Timeline of the Crazy Events in the Sony Hacking Scandal." Business Insider. December 9, 2014. http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12.

Fancy Bear (also known as APT28, Sofacy, Sednit, and Tsar Team).[6,7] Fancy Bear is a Russia-based APT threat actor that has been operating since 2010. Recent targets and attacks have included the German Think Tank Attacks (2019), German elections (2017), World Anti-Doping Agency attack (2016), U.S. Democratic National Committee breach (2016), and Operation "Pawn Storm" (2014).[8]

MONSOON (also known as Patchwork, APT -C-09, Chinastrats, Dropping Elephant, and Quilted Tiger).[9] MONSOON is an APT threat actor that appears to have begun in 2014. According to Forcepoint Security Labs, "The overarching campaign appears to target both Chinese nationals within different industries and government agencies in Southern Asia."[10] As of July 2016, more than 110 different victim countries and 6,300 victim IP addresses had been identified.[11] "The malware components used in MONSOON are typically distributed through [weaponized] documents sent through e-mail to specifically chosen targets. Themes of these documents are usually political in nature and taken from recent publications on topical current affairs. Several malware components have been used in this operation including Unknown Logger Public, TINYTYPHON, BADNEWS, and an AutoIt [3] backdoor."[12]

[6] "Top 25 Threat Actors – 2019 Edition." SBS CyberSecurity. December 12, 2019. https://sbscyber.com/resources/top-25-threat-actors-2019-edition.

[7] "Advanced Persistent Threat Groups." FireEye. 2020. https://www.fireeye.com/current-threats/apt-groups.html.

[8] "Top 25 Threat Actors – 2019 Edition." SBS CyberSecurity. December 12, 2019. https://sbscyber.com/resources/top-25-threat-actors-2019-edition.

[9] Ibid.

[10] Settle, Andy, Nicholas Griffin, and Abel Toro. "Monsoon – Analysis of an APT Campaign: Espionage and Data Loss Under the Cover of Current Affairs. Forcepoint Security Labs. 2016. https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf.

[11] Ibid.

[12] Ibid.