

[25] McAfee Labs and McAfee Foundstone Professional Services, "Protecting Your Critical Assets – Lessons Learned from 'Operation Aurora'", 2010, https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf,
Access Date: 12 February 2019.

[26] FireEye Labs, "APT28: A Window Into Russia's Cyber Espionage Operations?", 2014, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>,
Access Date: 12 February 2019.

[27] FireEye Labs, "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation", 2015, <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf>,
Access Date: 12 February 2019.

[28] Clearsky - Cyber Security, "Thamar Reservoir - An Iranian cyber-attack campaign against targets in the Middel East", 2015, <https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf>,
Access Date: 12 February 2019.

[29] R. Dela Paz, "The HeartBeat APT Campaign", Trend Micro, 2012, <https://docplayer.net/17881843-The-heart-beat-apt-campaign.html>,
Access Date: 12 February 2019.

[30] Kaspersky Labs - Global Research & Analysis Team, "The Desert Falcons Targeted Attacks", 2015, <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf>,
Access Date: 12 February 2019.

[31] Symantec, "The Waterbug attack group", 2016, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf,
Access Date: 12 February 2019.

[32] N. Villeneuve and J. T. Bennett and N. Moran and T. Haq and M. Scott and Kenneth Geers, "Operation 'Ke3chang': Targeted Attacks Against Ministries of Foreign Affairs", FireEye Labs, 2015, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf>,
Access Date: 12 February 2019.