A High-Profile Attack on The US Election 2016

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**A High-Profile Attack on The US Election 2016**

In the 2016 US Election, there are two cyber attacks on the US government. First, The Democratic National Committee (DNC) experienced a traumatic data breach as per private emails. The subjects of the emails appear that the DNC is biased against presidential candidate Bernie Sanders and in favor of Hillary Clinton.

The second attack was an Advanced Persistent Attack (APT) including the distributed denial of service (DDoS) attack on Hilary’s website; PSYOPS used bots to spread fake news about Hilary Clinton’s health condition, her political involvement, her emails probe, and foreign political involvement.

Several US Government agencies believe Rusian Intelligence involves in these attacks.

# Cyber Kill Changes in the 2016 Election

I may conclude the first cyberattack can combine with the second one and the target is presidential candidate Hillary Clinton. The attack progressed through each phase of the Cyber Kill Chain.

* Reconnaissance: President Putin (or Russia) acknowledges Hillary Clinton as a threat to his power. Therefore, she is the target of the cyber attack.
* Weaponize: The weapon in this scenario is the information that the hacker obtains from the DNC; the DDoS attack on Clinton’s website, the bot to spread the fake news, and the PSYOPS toward Clinton’s email scandal
* Delivery: The method used in DNC’s data breach is spear-phishing. It was believed they gain access to some high-level staff to gain access to the DNC’s server. Also, PSYOPS was delivered through Twitter and other social media platforms through bots. All attack was conducted on large scale by expert.
* Exploit: According to the Office of Public Affairs (2018), hundreds of phishing emails were sent to "hillaryclinton.com" emails, DNC emails, and Gmail accounts used by the Clinton campaign. This allows hackers to gain access to John Podesta's (a Clinton campaign chairman) email accounts. On April 12 of 2016, hackers gained access to the Democratic Congressional Campaign Committee (DDDC) server. On April 18 of 2016, hackers gained access to the (DNC) server. This is how hackers gained temporary Control of the’s DNC system.
* Install: According to (3), GRU compromises more than 30 computers on the DNC network, infecting them with malware. That is how they get access to mass data and transfer thousands of emails out of the server.
* Command and Control:  Control was maintained until they get what they want
* Act on Objective: Hackers created a domain to release stolen documents. When DNC announces the breach and theft of documents, DCLeaks and Guccifer 2.0 (both aliases of the Russian cyber military group) begin to communicate with WikiLeaks about releasing the data online. This creates serious damage to the 2016 election and the reputation of the president candidates (especially Hillary Clinton)

References

Chapple, M., & Seidl, D. (2023). Chapter 5: The Evolving Threat: From Script Kiddies to Advanced Attackers. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)

Office of Public Affairs (Jul 2018) *The DOJ indicted 12 Russian nationals alleged to be members of GRU for hacking the Democratic National Convention.* Retrieved from: <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election> (2)

Block, E., and Fischer., J., (2019) *Russians Hack the DNC's Server: A Timeline.* Retrieved from [Russians Hack the DNC's Server: A Timeline | wusa9.com](https://www.wusa9.com/article/news/russians-hack-the-dnc-a-timeline/65-bd1326a7-7ed5-4cd7-92a3-63eed75f1bd9#:~:text=Below%20find%20a%20timeline%20of%20hacking%20activities%20by,the%20Democratic%20National%20Committee%20%28DNC%29%20server.%20More%20items) (3)