

Democratic National Committee Hack

Durgesh Gaurav and Erik Buschardt

Providing Relevant Context: Election 2016 Results

- A surprise upset on November 8, 2016 from about 7 PM to about 2 AM...
- Donald John Trump: 60,265,858 popular votes, 290 electoral votes
- Hillary Diane Rodham Clinton: 60,839,922 popular votes, 228 electoral votes
- Chased by numerous email scandals, capped off by FBI inquiries by a Republican-turned Independent Director James Comey, working under George W. Bush for most of his career.
- Allegations of Wikileaks revelations regarding Trump alliance with Vladimir Putin throughout the primary season.
- *“Oh, it's... complicated.” ~ Count Mondego (The Count of Monte Cristo, 2002)*

Details of the Successful Cyber Espionage Attack

- Hackers apparently had access to data for more than a year (Reconnaissance)
- “High Confidence” that Russian state sponsorship was behind the attacks.
- Leaks contained information about DNC’s interactions with the media (incl. CNN, WSJ, WaPo, Politico); Hillary Clinton’s and Bernie Sanders’ campaigns, and financial contributions including donor information such as CC and SSNs.
- DNC tried to push HRC over Bernie after polls showed a clear lead over Trump.
- Guccifer 2.0: A fictitious persona created by Russian intel services.
- Essentially, worst case scenario... DNC’s secret plan backfired completely.

The Kill Chain

- Reconnaissance: Researching preliminary information about a target.
- Weaponization: Coupling a remote access trojan with an exploit into a deliverable payload. Amassing 19,252 emails and 8,034 attachments.
- Delivery: Transmission of the weapon to the target environment, usually by email attachment. Russian servers via Wikileaks. Possible communications to Trump, still under investigation to this day. **Further leaks re: 2018 and 2020.**
- Exploitation: Triggering the intruder's code, "OK" or "Cancel" button.
- Installation / Command & Control (C2): Installation on the victim's system.
- Actions on Objectives: Intruders can now take action on the intended target.

Any Questions?

Thank you for your time and attention.

Hack of Democrats' Accounts Was Wider Than Believed, Officials Say

<http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html>

Russian government hackers broke into DNC servers, stole Trump oppo

<http://www.politico.com/story/2016/06/russian-government-hackers-broke-into-dnc-servers-stole-trump-oppo-224315>

Russian government hackers penetrated DNC, stole opposition research on Trump

https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cfo06cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

DNC Breach Rallies Hackers To Clinton's Side in Vegas

<https://www.wired.com/2016/08/dnc-breach-rallies-hackers-clintons-side-vegas/>

Sources: US officials warned DNC of hack months before the party acted

<http://www.cnn.com/2016/07/25/politics/democratic-convention-dnc-emails-russia/>

