CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 99 April 2017

The Curious Case of the DNC Hack

Col. **Debashish Bose**

Background

During the last US Presidential elections hackers had broken into the servers of the Democratic National Committee (DNC). DNC is the formal governing body of the Democratic party of the United States. The hackers stole a large amount of information, including personal emails, research about opposition leaders, and general campaign correspondence. They then leaked out this information selectively through various agencies. As the election campaign progressed further it slowly became evident that this cyber hacking was not an independent incident; it was part of a larger Russian information warfare campaign.

The Russian information warfare campaign was devised to disrupt the 2016 presidential election. The campaign blended covert intelligence operations like cyber activity, with overt efforts by Russian

Keynotes

- The article is about the famous case of the hacking of the Democratic National Committee(DNC), during the US Presidential elections of 2016. The investigations into the hacking effort are still continuing and the full impact of the campaign is still to be understood. The hackers stole a large amount of information, including personal emails, research about opposition leaders, and general campaign correspondence. They then leaked out this information selectively through various agencies. As the election campaign progressed further it slowly became evident that this cyber hacking was not an independent incident it was part of a larger Russian information warfare campaign.
- The article covers in detail the Modus Operandi, the Russian motivations in conceiving the operation, the forensic evidence that links the entire operation to Russian hackers and finally some details of the aftermath, as they are becoming public.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an autonomous think tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic and outlook and policy-oriented in approach.

Website: www.claws.in Contact us: landwarfare@gmail.com

government agencies, state-funded media, third party intermediaries, and paid social media users as trolls. This can truly be said to be the first successful information warfare campaign done by one nation state against another. Though there would have been many campaigns before, but this was unique because of the following reasons:

- Impacted the highest and most powerful American office.
- The operation happened in full public glare.
- Open source community participated actively in deciphering the whole campaign. In the words of Thomas Reid, 'The result was an unprecedented open-source counterintelligence operation. Never in history was intelligence analysis done so fast, so publicly, and by so many.
- The understanding of the campaign was not restricted to secretive national intelligence agencies.
- Damaged the foundations of American democracy.
- The operation and its details are still unfolding. The post incident damage and its assessment are not yet complete.
- Has left behind a universal template which can be replicated in all national elections across the globe.
- The first such attempt by a foreign power in American history.
- Has brought to the forefront the enigma of 'fake news', like never before.
- What started as an information-gathering operation, ultimately morphed into an effort to harm one candidate, Hillary Clinton, and tip the election in favour of her opponent, Donald J Trump.

To put things in perspective, this hack should not be seen as an isolated case of hacking by the Russians. In fact 2016 was almost two decades of Russian cyber attacks on the US and vice versa. The first major detected hacking attempt by Russians, which led to large scale exfiltration of official files was code named as the Moonlight Maze. Since then the hacking effort of both sides has never really stopped, it has continued in different ways and forms. Throughout these two decades the GRU (Russia) and the Federal Security Service (FSB, Russia) has attacked many political and military targets, while the NSA (USA) and the GCHQ (UK) have done the same. In fact it is reported that during the Cold War period, both the USSR and the US have covertly interfered in multiple elections.

What is new this time is that the Russians have combined two different approaches, covert hacking with an overt influence operation, to effectively meddle into the US Presidential elections. Another important incident that needs to be seen in conjunction with this incident is the leakage of the Panama papers. The biggest damage of the leakage of the Panama papers was to Putin and his trusted core group. The leaked documents directly pointed to the Russian premiers' vast hidden wealth. Putin felt that the US was directly responsible for the entire issue. He felt that the US wanted to weaken Russia from within and spread distrust for the ruling establishment from within. From this perspective the DNC hack seems to be a very close tit-for-tat.

Modus Operandi

News of the hacking of the DNC servers first broke out in mid-June 2016. That is the time when CrowdStrike, a firm that analyzes threats to network security, was brought in by the DNC to check anomalous behaviours in its networks. Their analysis revealed that two separate Russian intelligence-affiliated adversaries were present in the DNC network. CrowdStrike released a comprehensive report of its findings on 14 June 2016, which accompanied a *Washington Post* article detailing the attacks on the same day. One of the hacking groups had access to the DNC servers for almost a year. This assumption was made on the analysis that the malwares and the methods used were identical to those used in other attacks attributed to the same Russian hacking groups. The first group identified as APT 29, i.e. The Dukes), suspected to be the FSB, had been on the DNC's network since at least summer 2015. The second group APT 28, i.e. Fancy Bear, identified as Russia's military intelligence agency GRU, had breached the democrats in April 2016, and this probably led to the investigation. The following week, two reputed cyber security firms, Fidelis Cybersecurity and Mandiant (Chinese APT fame), independently corroborated CrowdStrike's assessment that Russian hackers infiltrated DNC networks.

Now this is where it gets interesting, so far the hacking effort was going on silently, with the hackers collecting and keeping the material. After all 'The Dukes' had been stealing information since the summer of 2015. On realizing that their operations have been detected and made public, the whole operation now changed gears. A day after that report, someone calling themselves Guccifer 2.0 (an implied reference to notorious hacker Guccifer) claimed responsibility for the hack in a blog post. Through the blog and an accompanying Twitter account, Guccifer 2.0 refuted CrowdStrike's claims that this was a Russian operation, instead calling himself a 'lone hacker'. He also claimed to have handed much of the DNC bounty to *Wikileaks* (Julian Assange).

Like a typical warfare campaign, Russian tactics evolved over a period of time, i.e. it evolved in a manner synchronized with the election campaign. The manner of evolution depended on the electoral prospects of the two candidates. When it appeared to Russia that Clinton would win the election, the focus of the campaign changed over to undermining her presidency.

Russian Motivations

There were many reasons which motivated Russia to carry out such an activity. These are listed next:

(a) Undermine public faith in the US Democratic system.

(b) Harm Hillary Clinton's electability and potential presidency.

(c) Putin felt that the leaks of the Panama papers and the Olympic doping scandal were efforts to defame Russia by the US. Thus, he was eagerly looking for disclosures to discredit the US.

(d) Putin wanted to discredit Secretary Clinton, because he had publicly accused her for inciting mass protests against his regime in late 2011 and the early 2012.

(e) Russia saw the election of Trump as a way to achieve an international counter terrorism coalition against the Islamic State in Iraq and the Levant (ISIL).

(f) Donald Trump has been a long time admirer of Putin, and has publicly stated that he would not necessarily support NATO allies against a Russian invasion.

(g) Paul Manafort, Trump's campaign manager, formerly worked as an advisor to Viktor Yanukovich, the Russian backed Ukranian President, who was ousted in 2014. Thus, sympathetic benefits could be achieved in case Trump came to power. Manafort was forced out of the campaign in August 2016. Till date, he remains a major player in K street.

(h) Julian Assange has also been a frequent outspoken critic of Hillary Clinton's time at the State Department. Thus, it can be said that publication of the leaked e-mails a week before Clinton's nomination aligned well with both interests of Russia and Julian Assange (*Wikileaks*).

Proof of Russian Involvement

The possibility of the US allegations being true finds weight from the following interesting facts:

(a) The most compelling evidence linking the DNC breach to Russia was found at the beginning of July 2016 by Thomas Rid, a professor at King's College in London, who discovered an identical command-and-control address hardcoded into the DNC malware that was also found on malware used to hack the German Parliament in 2015. According to German security officials, the malware originated from Russian military intelligence. An identical SSL certificate was also found in both breaches.

(b) The evidence mounts from there. Traces of metadata in the document dump reveal various indications that they were translated into Cyrillic. Furthermore, while Guccifer 2.0 claimed to be from Romania, he was unable to chat with Motherboard journalists in coherent Romanian. Besides which, this sort of hacking wouldn't exactly be outside of Russian norms.

(c) One of the first leaked files had been modified on a computer using Russian-language settings by a user named 'Feliks Dzerzhinsky'. Dzerzhinsky was the founder of the Cheka, the Soviet secret police—a figure whose mythic renown was signaled by a 15 tonne bronze statue that once stood in front of KGB headquarters.

(d) Another error had to do with the computer that had been used to control the hacking operation. Investigators found that the malicious software, used to break into the DNC was controlled by a machine involved in a 2015 attack of the German parliament. German intelligence later traced the Bundestag breach to the Russian GRU, i.e. Fancy Bear.

(e) There were other errors, too, including a Russian smile emoji—')))'

(f) The hackers' gravest mistake involved the emails they'd used to initiate their attack. As part of a so-called spear-phishing campaign, Fancy Bear had sent mails to thousands of targets around the world. The emails were designed to trick their victims into clicking a link that would install the malicious software or send them to a fake but familiar-looking login site to harvest their passwords. The malicious links were hidden behind short URLs of the sort often used on Twitter. To manage so many short URLs, Fancy Bear had created an automated system that used a popular link-shortening service called Bitly. The hackers forgot to set two of their Bitly accounts to 'private'. As a result, a cyber security company called SecureWorks was able to glean information about Fancy Bear's targets. Between October 2015 and May 2016, the hacking group used 9,000 links to attack about 4,000 Gmail accounts, including targets in Ukraine, the Baltics, the United States, China, and Iran. Among the group's recent breaches were the German parliament, the Italian military, the Saudi foreign ministry, the email accounts of Philip Breedlove, Colin Powell, and John Podesta—Hillary Clinton's campaign chairman—and, of course, the DNC.

(g) Emails sent by Guccifer 2.0 to reporters show evidence that the hacker used a Russian-language anonymity protection service— a language he has claimed he could not read or even recognize. In the same interview, when forced to answer questions in Romanian, he used such clunky grammar and terminology that experts believed he was using an online translator.

(h) Russian behaviour changed after the declaration of election results, for example ussian officials stopped publicly criticizing the US electoral process as unfair, almost immediately after the election, because that would be counter productive. Before the elections they tried to cripple Clintons presidency by discrediting the fairness of the election. Pro-Kremlin bloggers had prepared a twitter campaign, #DemocracyRIP, on election night in anticipation of Clintons victory.

(i) Russian Intelligence accessed elements of multiple US electoral boards. These compromised elements were not used for vote tallying.

The first group, APT28 has been active since the mid-2007. Its targets included NATO, several US defense contractors, the German parliament and, after Russia's doping scandal began, the World Anti Doping Agency(WADA), (This is another proof to show that APT28 is Russian.)

(j) The other group, APT29, was first spotted operating in Chechnya in 2008. Stealthier and more cautious than Fancy Bear, the Dukes have nonetheless been detected infiltrating the White House, the State Department, and the Joint Chiefs of Staff. Known for innovation—one attack campaign used Twitter as a command-and-control channel—they have their own fleet of customizable malwares, including a programme called Seaduke, which was found again on the DNC's network.

(k) Whereas Grucifer 2.0 claimed to be an independent Romanian hacker made multiple contradictory statements and false claims about his likely Russian identity. Press reports suggested that more than one person claiming to be Grucifer 2.0 interacted with the press.

One should not think that the Republican party was better at anticipating and protecting itself against such attacks. The FBI had notified the Republican party in June 2016, that some of its email accounts may have been hacked by the same group. However, the perpetrators decided to release documents only related to the democrats. This is a stark but interesting fact.

Based on the capabilities of the Russian hacking communities, it would have been likely that they would have tried to hide the fact that they had done it. They could have easily left a trail pointing to someone else, though initially that had also been tried by Grucifer 2.0. Then where did it go wrong for the Russian agencies. One thing that they would have totally not appreciated is the fact that as soon as the hacked files hit the internet, a horde of investigators of *unimaginable proportions* starting from hackers to former intelligence operatives to security consultants and journalists started going through the information (as a result for the first time we had the best brains of the open source community concentrating in this effort. Much more than what any investigating agency can put together). Over a period of time these self-motivated investigators became very concerted in their efforts, with proper dedicated exchange of information between themselves. The most important piece of information in all this was circulated by Julian Assange, the founder of *Wikileaks*, who actually released the 'hacked' emails to the public, and assured the world that he got the material from a DNC insider and not from Russian hackers.

Deliberate Swing in Favour of Trump

The character Guccifer 2.0, in possession of hacked Democratic party documents had released primary strategies for states regarded as crucial for a Donald Trump victory, indicating an attempt to swing the US presidential election. In September 2016, he released primary documents from Ohio, New Hampshire, North Carolina, and Illinois. Previously he had released similar document dumps on two states, Pennsylvania and Florida. All of these states except Illinois were swing states, with Florida, Ohio, and Pennsylvania being widely regarded as fundamental for Trump to have a chance to win the electoral college.

Aftermath

Starting December 2016 a number of very strange activities have started taking place in the cyber intelligence world of Russia. A top Russian cyber intelligence officer who US officials say could have overseen last year's election hacking was arrested. Sergei Mikhailov, a senior member of the FSB, was charged with treason along with him another FSB officer Major Dmitry Dokuchayev was also arrested. Mikhailov served in the FSB's Center for Information Security, the agency's cyber intelligence branch, which has been implicated in the American election hacking. But it is not clear whether the arrest was related to those intrusions. According to an article in *Kommersant*, the arrest stems from Mikhailov's work on criminal hacking investigations. However, *Moscow Times* reports the senior officer was arrested on suspicion of leaking information to US intelligence officials. It is assessed that in addition to forensic evidence, leakage of information through physical sources is what helped US intelligence agencies to point their fingers towards Russia after their investigations.

This news follows reports that Kaspersky Labs security researcher Ruslan Stoyanov was also arrested for treason in December. Details are also scarce on that arrest, but the security firm says the incident isn't related to Stoyanov's work at Kaspersky Labs. We may never know the exact reasons for the arrests, but the events are certainly notable at a time when tensions are high between the US and Russia over hacks of the DNC.

The *New York Times* reports that the Director of the Center for Information Security, Andrei Gerasimov, was fired earlier in January 2017. This news was also released by *Kommersant* which reported that the termination followed an investigation into the agency's work with Kaspersky on criminal hacking cases. Gerasimov was FSB's Deputy Director for counterintelligence.

It may not be clear or known. But given the crisis touched off by the hacking campaign, US accusations about it and sanctions tied to it, it is rather difficult to estimate that these incidents are not connected. But these arrests are a very rare case of disturbances in the country's super secretive intelligence/cyber security apparatus slipping into public view. The arrests were deliberately made public for a country that prides itself on secrecy. What is the reason for the public attention???

Summary

What makes these kinds of cyber espionage and propaganda campaigns so worthwhile is that even if Russia cannot get its favourite candidate elected, Moscow may still consider it a success if it can continuously sow doubt in the minds of Americans about the legitimacy of the US election process and other tenets of democracy.

While there's no way to be certain of the ultimate impact of the hack, this much is clear: A low-cost, high-effect weapon that Russia had first tried out in elections from Ukraine to Europe was tested on the United States, with devastating effectiveness. For Russia, with a relatively weak economy and a nuclear arsenal which it cannot use for conventional war, information operations proved the perfect weapon: cheap, difficult to detect, and extremely difficult to attribute.

In case these allegations are true, then it is major cranking up of information operations by Russia. The current hearings that are on by the House and Senate Intelligence Committees are extremely informative regarding the way that the incidents worked during the election campaign and the role of various players. As far as the Intelligence Committee hearings are concerned, they are still looking into details and responsibilities have not yet been fixed. In the Indian context also this operation has major implications. We are a thriving democracy with elections being held at regular intervals. All the tricks learnt in this campaign can be equally effectively used over here.

Hacking attempts are nothing new, but leaking out hacked documents in a deliberate attempt to sway the elections is absolutely new and innovative. It is a case study in carrying out Information Warfare to achieve the nation-states aim. Russia has always had a longstanding desire to undermine the US led democratic system of government. This current round of activities demonstrated a major escalation in directness, level of activity and quantum of effort compared to previous such activities. What is going to be the final ramifications/impact of the DNC hack is still anybody's guess.

References

1. Background to 'Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution', 6 January 2017.
2. 'Krebs on Security', available at https://krebsonsecurity.com/2017/01/the-download-on-the-dnc-hack/,last accessed on 11 January 2017.
3. Thomas Reid, 'All signs point to Russia being behind the DNC Hack',, 25 July 2016.
4. Available at http://www.thedailybeast.com/articles/2017/01/06/how-the-u-s-enabled-russian-hack-truthers.html, last accessed on 15 January 2017.
5. AM ET, 16 September 2016 at 11:52, available at. http://www.vocativ.com/359466/guccifer-2-swing-states/, last accessed on 15 January 2017.
6. Available at https://www.engadget.com/2017/01/26/russian-cybersecurity-officer-treason-arrest/, last accessed on 2 February 2017.
7. Available at http://warincontext.org/2016/07/25/all-signs-point-to-russia-being-behind-the-dnc-hack/, last accessed on 4 February 2017.
8. Available at http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/, last accessed on 4 February 2017.

The contents of this Issue Brief are based on the analysis of material accessed from open sources and are the personal views of the author. It may not be quoted as representing the views or policy of the Government of India or Integrated Headquarters of MoD (Army).

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com
Website: www.claws.in