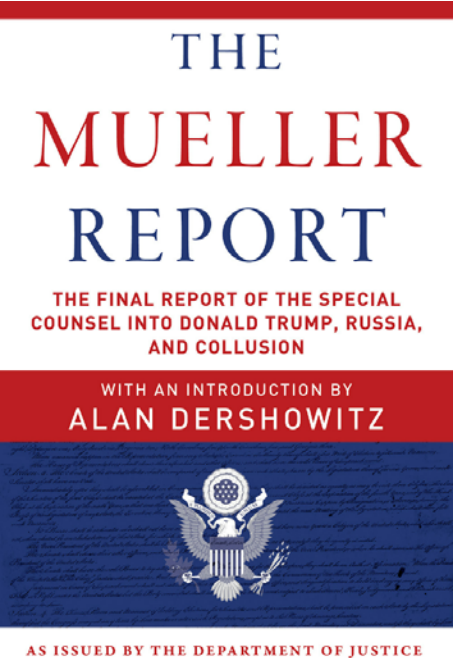


2016 US ELECTION UPDATE
MUELLER REPORT

We cover the computer security aspects of the Mueller Report



© Robert F. Kelly, 2019 ISE331 – Information Security 2

Sources

- Mueller Report
<https://www.justice.gov/storage/report.pdf>
- References cited in the Mueller Report

Unless attributed elsewhere, quotes in the slides are taken from the Mueller Report
Other non-quoted material was taken from Mueller Report, but with some slight modifications

Reading

- Lawfare Blog

https://www.lawfareblog.com/notes-mueller-report-reading-diary?utm_campaign=Brookings%20Brief&utm_source=hs_email&utm_medium=email&utm_content=72134894

Scope of Special Counsel

- “authorized to conduct the investigation confirmed by then-FBI Director James B. Comey in testimony before the House Permanent Select Committee on Intelligence on March 20, 2017, including:
 - Any links and/or **coordination** between the Russian government and individuals associated with the campaign of President Donald Trump; and
 - Any matters that arose or may arise directly for the investigation; and
 - Any other matters within the scope of 28 C.F.R. 600.4(a).



Image: time.com

Major Conclusions of Report

- Russia interaction
 - “numerous links between individuals with ties to the Russian government and individuals associated with the Trump campaign”
 - “evidence not sufficient to support criminal charges”

This session does not address the obstruction of justice aspect of the report

Report Structure

- Volume I – describes the factual results of the investigation
 - Scope
 - Ways Russia interfered with the 2016 presidential election
 - Link between Russian government and Trump campaign
- Volume II – addresses President Trump’s actions towards
 - The FBI investigation in to Russia’s interference in the election and
 - The Special Counsel’s investigation

This session covers material from Volume I

© Robert F. Kelly, 2019 ISE331 – Information Security 7

Report Redactions

- Redaction categories
 - Harm to ongoing matter
 - Investigative technique
 - Personal privacy
 - Grand jury
- Report categories not intelligible due to heavy redactions
 - IRA funding
 - IRA controlled social media
 - IRA botnet activities
 - Targeting and recruitment of US persons
 - WikiLeaks dissemination

Within the Trump Campaign, aides reacted with enthusiasm to reports of the hacks.²³ [1 line redacted for harm to ongoing matter] discussed with Campaign officials that WikiLeaks would release the hacked material.²⁴ Some witnesses said that Trump himself discussed the possibility of upcoming releases [1 line redacted for harm to ongoing matter]. Michael Cohen, then-executive vice president of the Trump Organization and special counsel to Trump, recalled hearing [3 lines redacted for harm to ongoing matter].²⁵ Cohen recalled that Trump responded, “oh good, alright,” and [1 line redacted for harm to ongoing matter].²⁶ Manafort said that shortly after WikiLeaks’s July 22, 2016 release of hacked documents, he spoke to Trump [2 lines redacted for harm to ongoing matter]. Manafort recalled that Trump responded that Manafort should [1 line redacted for harm to ongoing matter] keep Trump updated.²⁷ Deputy campaign manager Rick Gates said that Manafort was getting pressure about [1 line redacted for harm to ongoing matter] information and that Manafort instructed Gates

© Robert F. Kelly, 2019 ISE331 – Information Security 8

Scope of Investigation

- “Office
 - issued more than 2,800 subpoenas under the auspices of a grand jury sitting in the District of Columbia;
 - executed nearly 500 search-and-seizure warrants;
 - obtained more than 230 orders for communications records under 18 U.S.C. § 2703(d);
 - obtained almost 50 orders authorizing use of pen registers;
 - made 13 requests to foreign governments pursuant to Mutual Legal Assistance Treaties; and
 - interviewed approximately 500 witnesses, including almost 80 before a grand jury.”

Pen register - A device which records or decodes electronic or other impulses which identify the numbers called or otherwise transmitted on the telephone line to which such device is dedicated

Clarification of Prosecution Threshold

- Criminal prosecution standard – proof beyond a reasonable doubt
- Counterintelligence/impeachment standard – more likely than not
- Mueller standard - “whether admissible evidence would probably be sufficient to obtain and sustain a conviction.”
- Mueller definition - “ ‘coordination’ does not have a settled definition in federal criminal law. We understood coordination to require an agreement — tacit or express.”

Explains the differing explanations of the conclusions of the Mueller Report

Avoiding Surveillance

- “some of the individuals we interviewed or whose conduct we investigated – including some associated with the Trump Campaign – deleted relevant communications or communicated during the relevant period using applications that feature encryption or that do not provide for long-term retention of data or communications records.”

Conclusion that some public secure communications were not able to be decrypted

Volume I Report Categories

- Russian social media campaign
- Russian hacking operation
- Russian contacts with campaign

Russian Social Media Campaign

- Conducted by the Internet Research Agency (IRA)
- Funded by Yevgeniy Prigozhin
- Mid 2014 – sent IRA employees to the US for intelligence gathering
- Used social media accounts and interest groups to sow discord in the US through what it termed “**information warfare**”
- By early 2016 it favored Trump and targeted Clinton
- No evidence that any US persons conspired or coordinated with the IRA

Evidence standard sometimes lost in all the coverage of the Mueller Report

IRA Campaign

- IRA targeted US as early as 2014 – traveled to US to gather information and photos used in social media posts
- Used fictitious US personas initially, later added groups (e.g., @TEN_GOP)
- Operated social media accounts designed to attract US audiences – falsely claiming to be controlled by US activists



Image: Twitter

IRA Rally Organization Technique

- Posed as US grassroots activists
- Used social media to announce the event
- Sent messages to followers of its social media accounts, asking for attendance
- Sought a US event coordinator
- Contacted US media, asking them to speak with coordinator
- Post-event posted photos and videos



Earliest rally was a “confederate” rally in November 2015

Image: NY Times

IRA Rally Example

- Poster created by IRA and included in the Mueller Report
- Image of an coal miner who had died of complications of black lung disease
- Photo taken without permission from either the family or the photographer

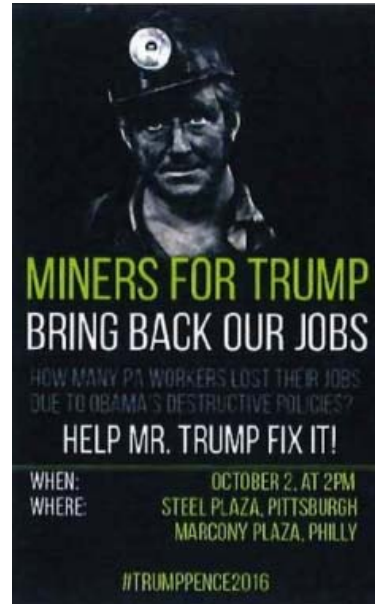


Image: NPR

Scope

- By the end of the 2016 election, IRA had the ability to reach millions of US persons through their social media accounts
- IRA controlled social media accounts had hundreds of thousands of US participants; similar Twitter accounts had tens of thousands of followers



Image: Twitter

© Robert F. Kelly, 2019 ISE331 – Information Security 17

Power of Social Media Campaign

- US political figures retweeted IRA-created content
 - Former Ambassador Michael McFaul
 - Roger Stone
 - Sean Hannity
 - Michael Flynn Jr.

Sean Hannity has over 4 million Twitter followers



Image: Politico

© Robert F. Kelly, 2019 ISE331 – Information Security 18

Social Media Companies

- Facebook identified
 - 470 IRA controlled Facebook accounts
 - 80,000 posts between 1/15 and 8/17
 - Over 3,500 purchased ads (\$100,000)
 - Reached 126 million persons (29 million through direct contact)
- Twitter
 - identified 3,814 IRA controlled accounts
 - Notified 1.4M people that they may have been in contact with an IRA-controlled account
 - IRA posted 175,993 tweets from 3,814 accounts in the 10 weeks before the election

"To those people, who hate the Confederate flag. Did you know that the flag and the war wasn't about slavery, it was all about money." The tweet received over 40,000 responses. @Jenn_Abrams 4/24/17 (2:37 p.m.) Tweet

Donald Trump Jr. claimed the investigation "has had a much harsher impact on our democracy than a couple Facebook ads."

Sharing of Polling Data

- “Manafort had caused internal polling data to be shared with Kilimnik and the sharing continued for some period of time after their August meeting”
- Polling data – detailed data concerning specific characteristics, opinions, issue-strength, etc. of individual voters
- Micro-targeting – use of polling data to target individual voters with targeted messages

Not a great deal of detail in the report concerning the nature of the polling data that was shared

Lies

- “investigation established that several individuals affiliated with the Trump Campaign lied to the Office and to Congress about their interactions with Russian-affiliated individuals and related matters. These lies materially impaired the investigation of Russian election interference.”

Russian Hacking

- Mueller Report refers to the Russian hacking units as Military Units (not referred to by Bear designation)
- Unit 26165 – GRU cyber unit dedicated to targeting organizations outside of Russia
 - Develops malware, Spearphishing and bitcoin mining
- 74455
 - Release of documents stolen by 26165
 - Promotion of document releases
 - Publication of anti-Clinton content on social media accounts
 - Hacking in to state computers and US companies

Bitcoins used to purchase computer infrastructure and in hacking operations

Spearphishing Campaign

- Gained access to numerous e-mail accounts
 - Clinton campaign
 - John Podesta
 - Junior volunteers
 - Informal campaign advisors
 - DNC employee
- Stole tens of thousands of emails from spearphishing victims

Intrusion into DCCC and DNC Networks

- Access to DCCC used credentials stolen from an employee
 - Compromised 29 computers on the DCCC network
 - Gained access to a DNC network via a VPN from DCCC
 - More than 30 computers on DNC network were compromised
 - Installed malware on DNC and DCCC networks
 - Credential harvesting tool
 - Tool to compile and compress in info for exfiltration
 - Logged keystrokes, took screenshots, and gathered other info
 - Activity of malware controlled by at least 2 sets of GRU-controlled computers
- The Arizona based “AMS Panel” served as the nerve center through which GRU officers monitored and directed the malware

AMS Panel

- One of the GRU external control centers
- Located in Arizona
- Stored thousands of files containing key logging sessions
- GRU officers monitored DCCC and DNC employees work on infected computers
- Captured data included passwords, internal employee communications, banking info, and sensitive personal info
- Captured DNC opposition research on Donald Trump

Dissemination of Hacked Materials

- Released initially through DCLeaks and Guccifer 2.0
- Later released through WikiLeaks
- DCLeaks (dcleaks.com)
 - Registered in April 2016 through a service that anonymized the registrant
 - Paid for using a pool of bitcoins mined by the GRU
 - Landing page enabled easy access to the material
 - Some pages password protected to control timing of released info
 - GRU used Facebook, Twitter, and a Gmail account to communicate privately with reporters to give them early access to archives of leaked material

Guccifer 2.0

Some Twitter posts show abbreviations and typos not found in more polished material

- In June 2016, DNC announced the hacking of DNC computers and suspected theft of documents
- In an apparent response to that announcement, GRU officers logged into a Moscow-based server (used and managed by 74455), searched for words in English
- Hours later, Guccifer 2.0 published its first post attributing the DNC hack to a lone Romanian hacker, using words and phrases from earlier GRU searches
- Many documents released through August 2016
- Some documents related to Congressional races
- Twitter briefly suspends Guccifer 2.0 account in August 2016

WikiLeaks

- DCLeaks persona used to contact WikiLeaks about possible coordinate of stolen emails
- WikiLeaks contacted Guccifer 2.0 to suggest coordination of document releases
- “GRU and WikiLeaks sought to hide their communications” indications of encryption between organizations
- Stolen documents transferred from GRU to WikiLeaks using a method redacted in report due to “Investigative Technique”
- Subsequently, GRU transmitted documents to WikiLeaks
- PGP used to encrypt some files

Coordination, Not Conspiracy

- “Russia, if you’re listening, I hope you’re able to find the 30,000 emails that are missing”
- Within 5 hours,
 - GRU officers targeted for the first time Clinton’s personal office
 - Unit 26165 created and sent malicious links targeting 15 email accounts
 - No evidence found of earlier penetration attempts
 - Not clear how GRU able to identify these non-public accounts



Image: Yahoo! News

© Robert F. Kelly, 2019 ISE331 – Information Security 29

Hacking Administration of US Elections

- “GRU officers also targeted individuals and entities involved in the administration of the elections”
- “GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations”
- **Office did not investigate further**
- “GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents).”
- Spearphishing campaign against election administration using a Trojan Horse Word document

Office did not investigate much beyond its charter, passing many leads and material to other investigative and prosecutive organizations

© Robert F. Kelly, 2019 ISE331 – Information Security 30

Class Discussion

- What controls (if any) should be placed on media organizations to limit the release of stolen campaign documents?

Class Discussion

- What is your response to the Giuliani statement?

"There's nothing wrong with taking information from Russians. It depends on where it came from," – Rudy Giuliani



Image: Charles Krupa, AP

Questions

