Non-Political Security Learnings from the Mueller Report

Arkadiy Tetelman (@arkadiyt)

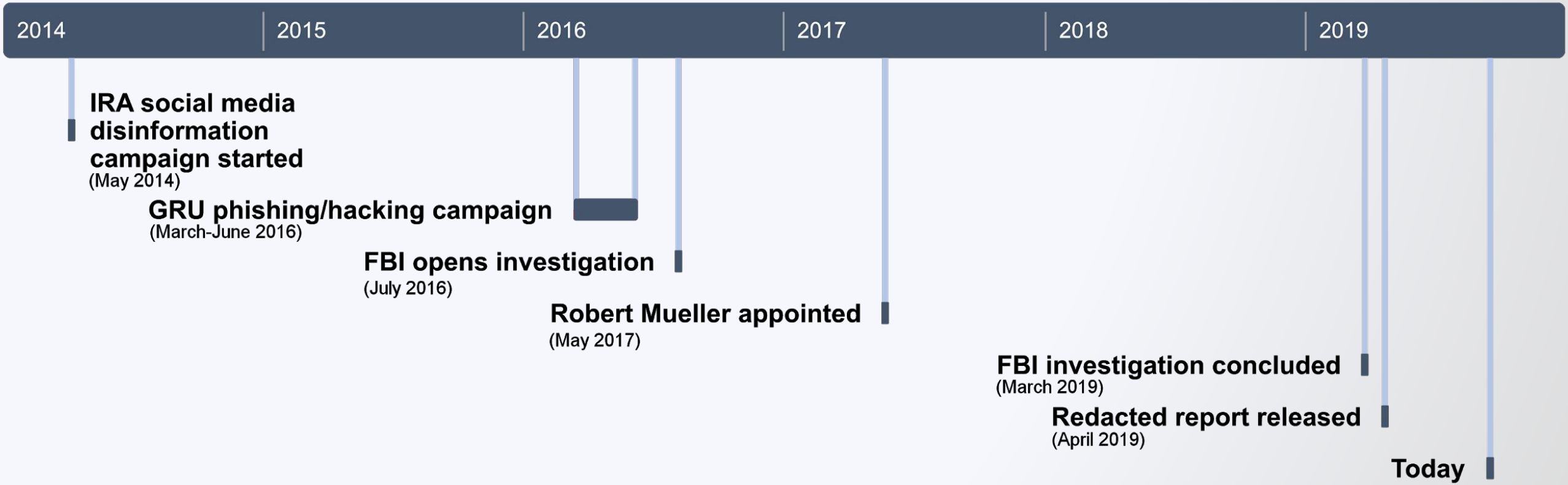
Agenda

- Background
- Blue Team Learnings
- Personal Security Learnings
- Questions

About me

- Arkadiy Tetelman (@arkadiyt)
- Head of Security at Lob
- Previously appsec at Airbnb, Twitter
- Fun fact

Background


2014
2015
2016
2017
2018
2019
IRA social media disinformation campaign started
(May 2014)
GRU phishing/hacking campaign
(March-June 2016)
FBI opens investigation
(July 2016)
Robert Mueller appointed
(May 2017)
FBI investigation concluded
(March 2019)
Redacted report released
(April 2019)
Today

Background

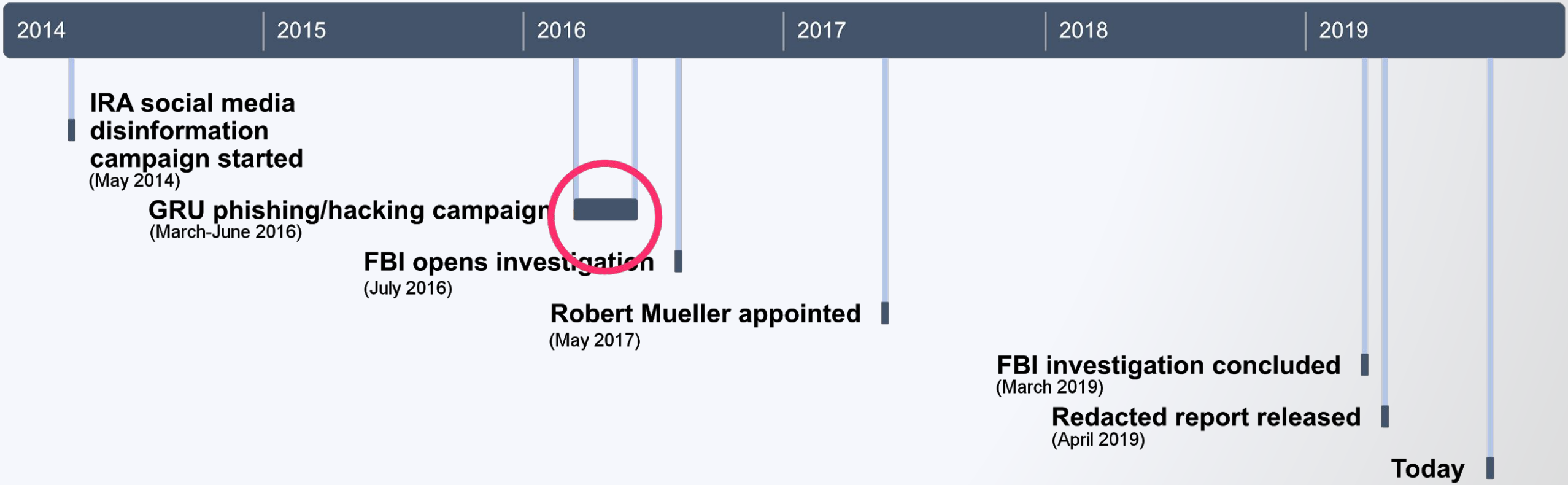
- 2 years 8 months
- Employed:
  - ~22 attorneys & paralegals
  - ~9 support staff
- Worked alongside:
  - ~40 FBI staff (agents, analysts, accountants, etc)

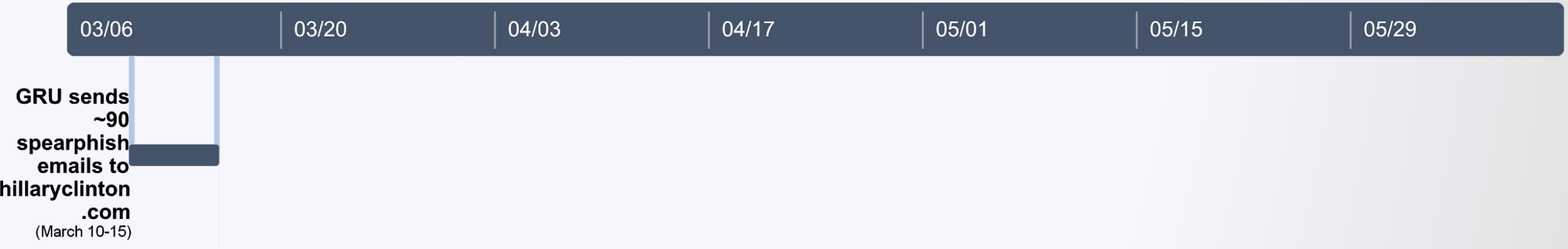
Background

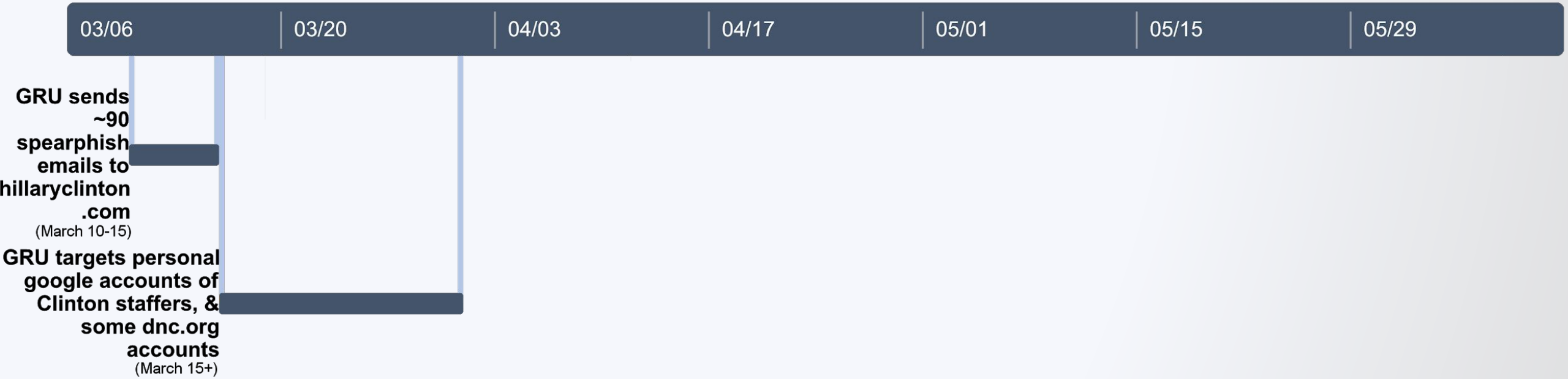
- Volume 1: Russian interference in 2016 election
  - II. “Active Measures” social media campaign
  - III. Hacking/dumping campaign
- Volume 2: Administration obstruction of justice

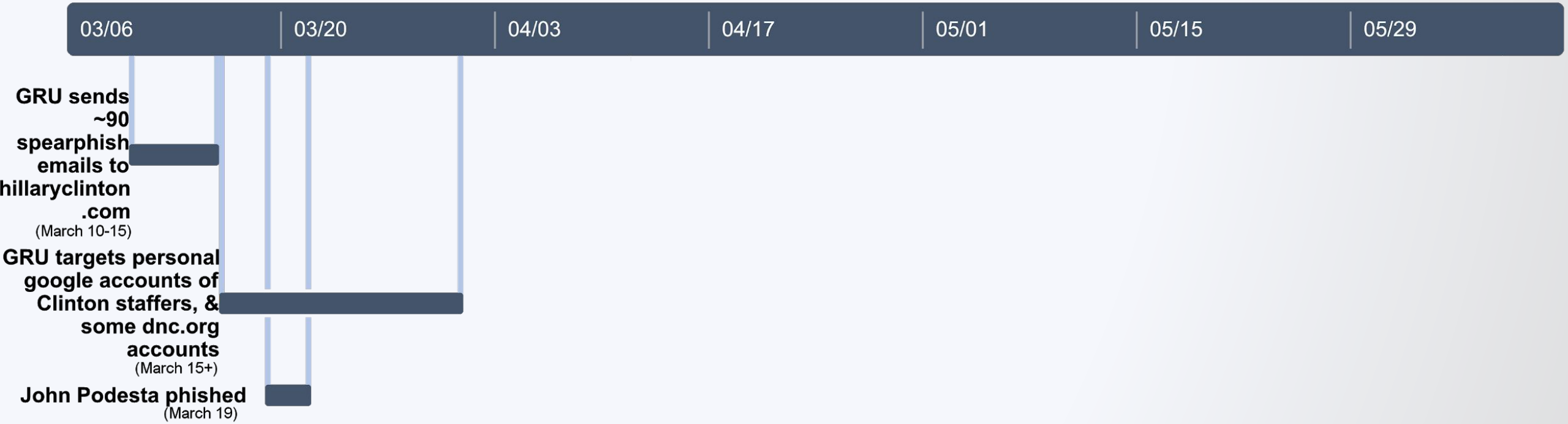
Blue Team Learnings

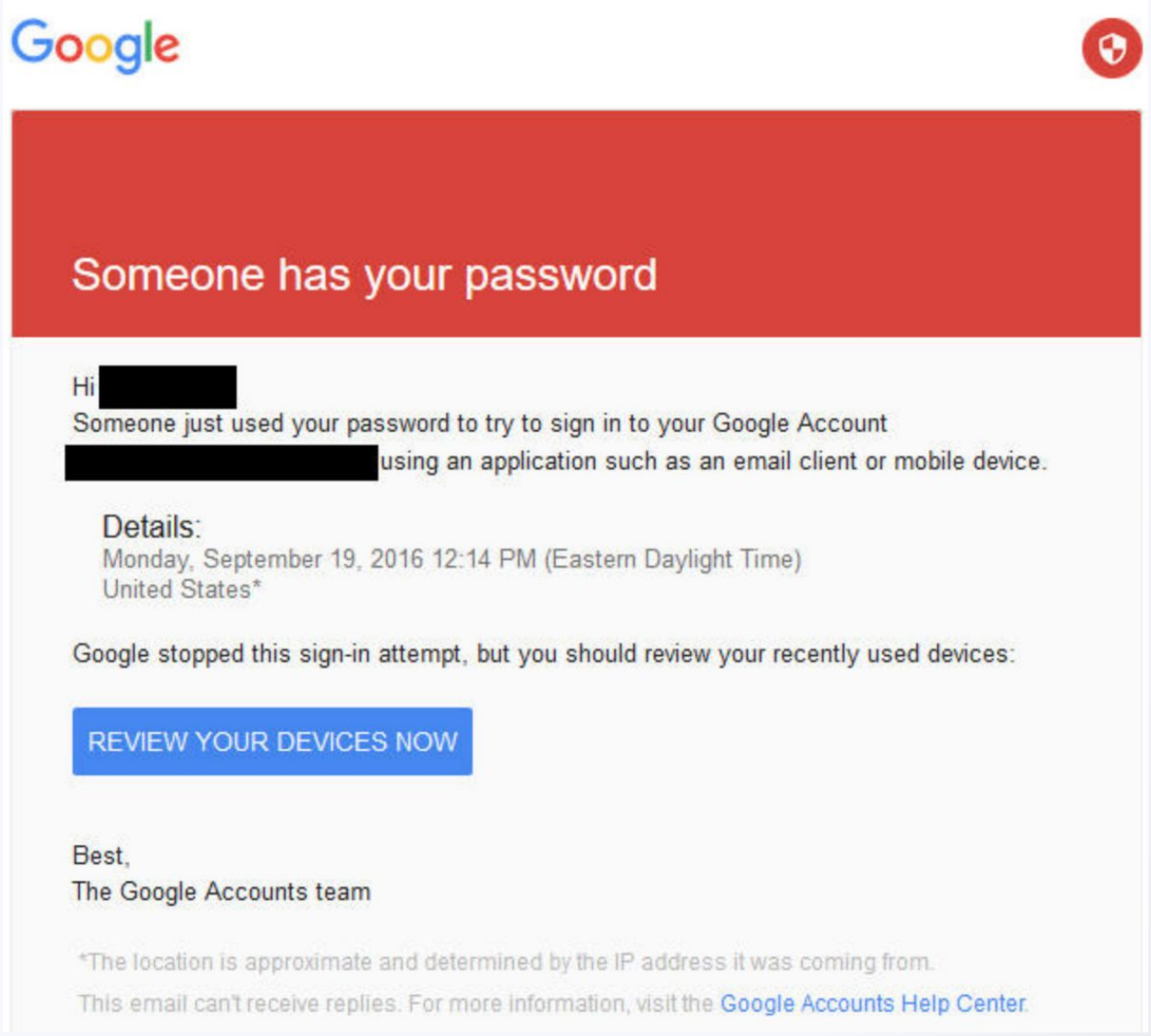
Timeline


2014
2015
2016
2017
2018
2019
IRA social media disinformation campaign started
(May 2014)
GRU phishing/hacking campaign
(March-June 2016)
FBI opens investigation
(July 2016)
Robert Mueller appointed
(May 2017)
FBI investigation concluded
(March 2019)
Redacted report released
(April 2019)
Today


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)


Google
Someone has your password
Hi [redacted]
Someone just used your password to try to sign in to your Google Account [redacted] using an application such as an email client or mobile device.
Details:
Monday, September 19, 2016 12:14 PM (Eastern Daylight Time)
United States*
Google stopped this sign-in attempt, but you should review your recently used devices:
REVIEW YOUR DEVICES NOW
Best,
The Google Accounts team
*The location is approximate and determined by the IP address it was coming from.
This email can't receive replies. For more information, visit the Google Accounts Help Center.

From: Charles Delavan <[redacted]@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara Latham <[redacted]@hillaryclinton.com>, Shane Hable <[redacted]@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

> Mr. Delavan ... said that his bad advice was a result of a typo: He knew this was a phishing attack, as the campaign was getting dozens of them. He said he had meant to type that it was an “illegitimate” email, an error that he said has plagued him ever since.

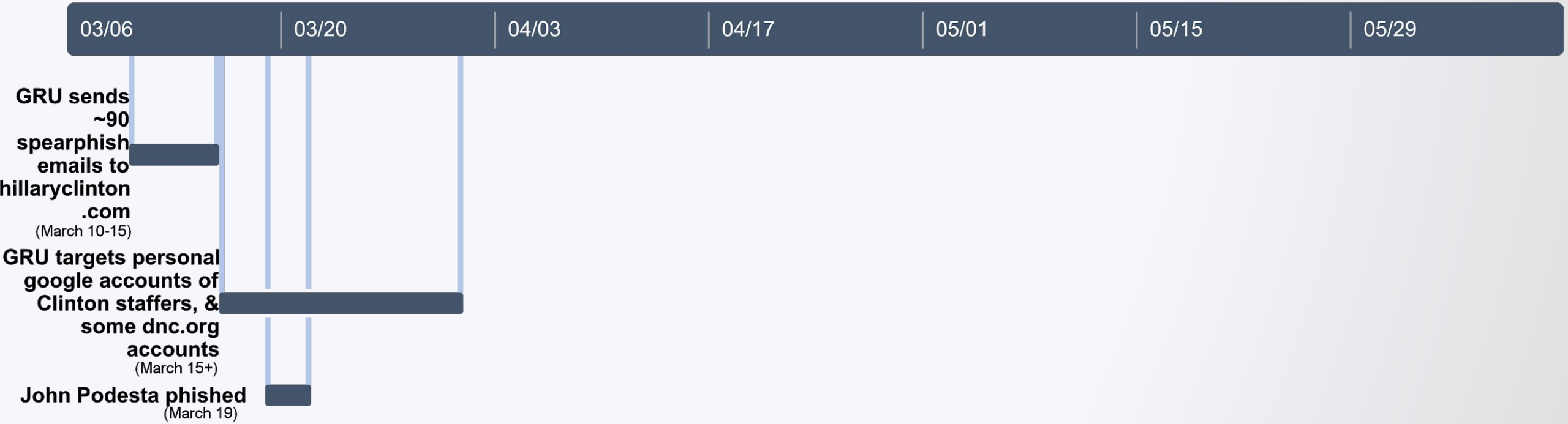
* https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Phished accounts

- numerous email accounts of Clinton Campaign employees and volunteers
- junior volunteers assigned to the Clinton Campaign's advance team
- informal Clinton Campaign advisors
- a DNC employee
- 118 GRU officers stole tens of thousands of emails

Recommendations

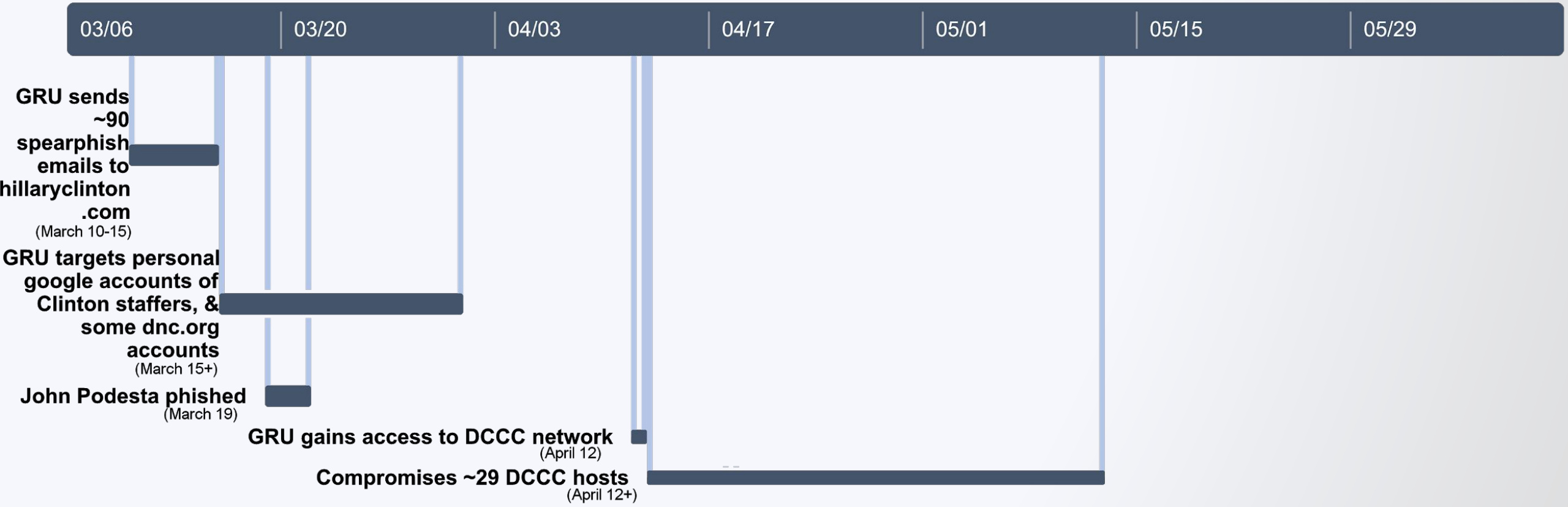
- Password manager / hardware (U2F, WebAuthn) 2fa tokens
- Ingest & alert on DNS
- Scan incoming emails
- Ingest mail audit log events
- Phishing exercises?


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)

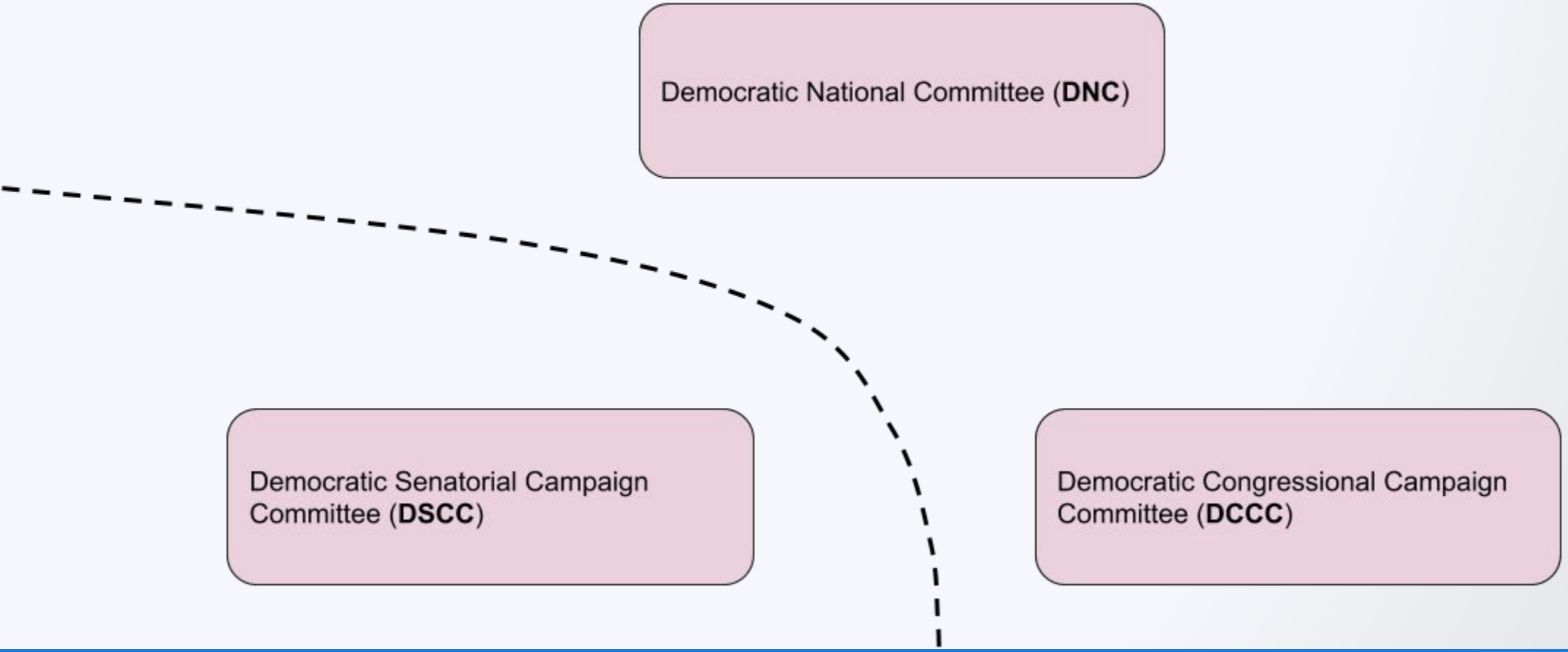

03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)
GRU gains access to DCCC network
(April 12)

> Over the ensuing weeks, the GRU traversed the network, identifying different computers connected to the DCCC network. By stealing network access credentials along the way (including those of IT administrators with unrestricted access to the system), the GRU compromised approximately 29 different computers on the DCCC network.

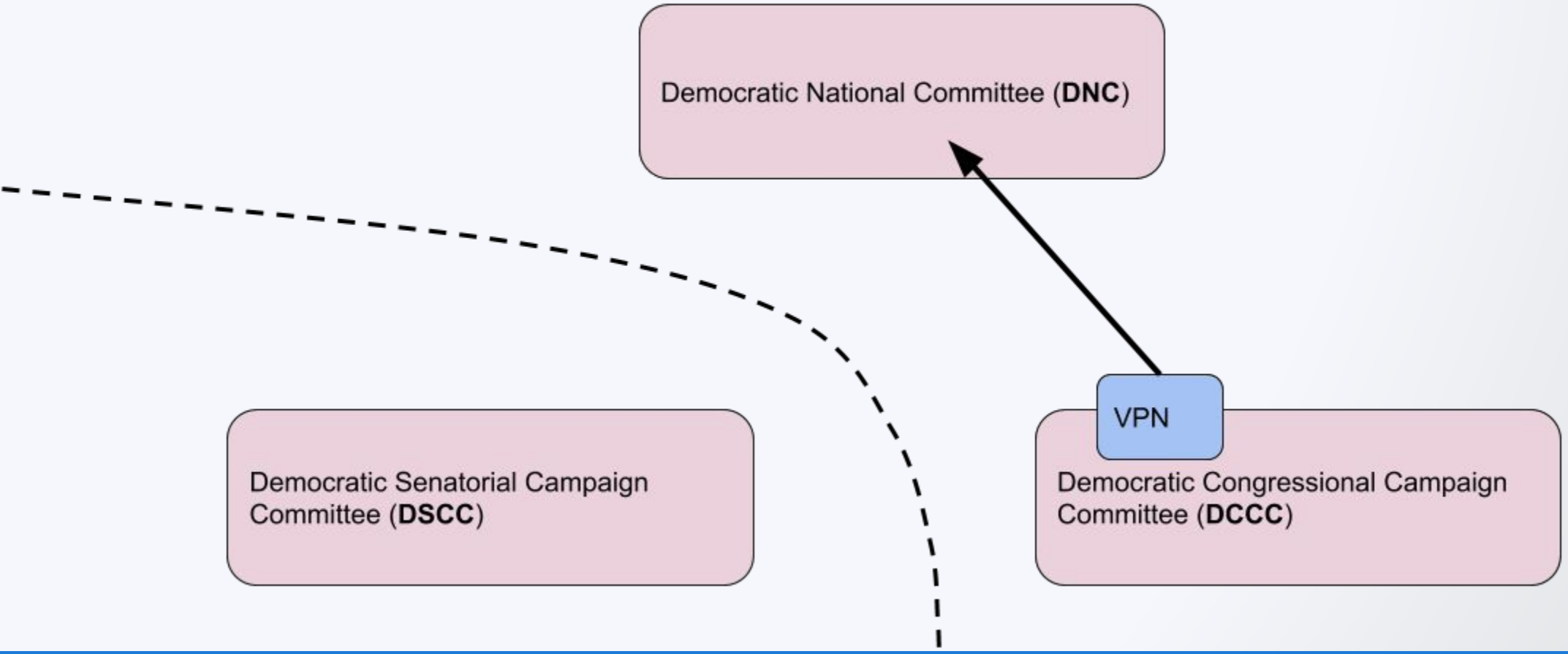
* Report Volume 1, p38

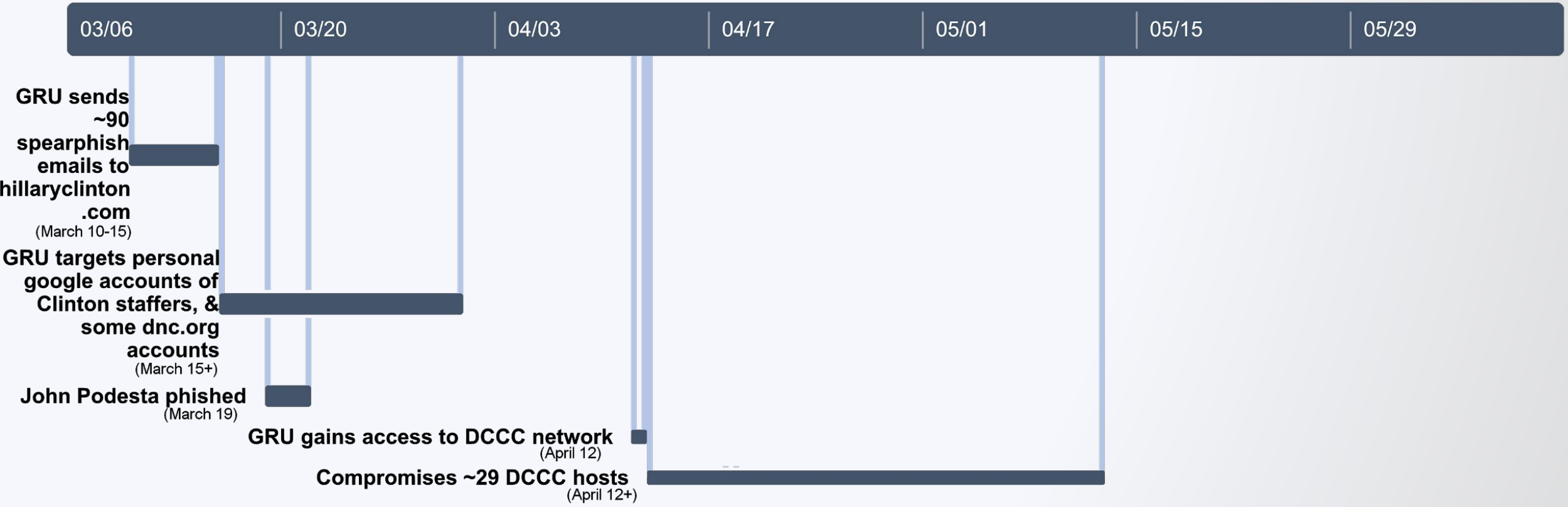

03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)
GRU gains access to DCCC network
(April 12)
Compromises ~29 DCCC hosts
(April 12+)

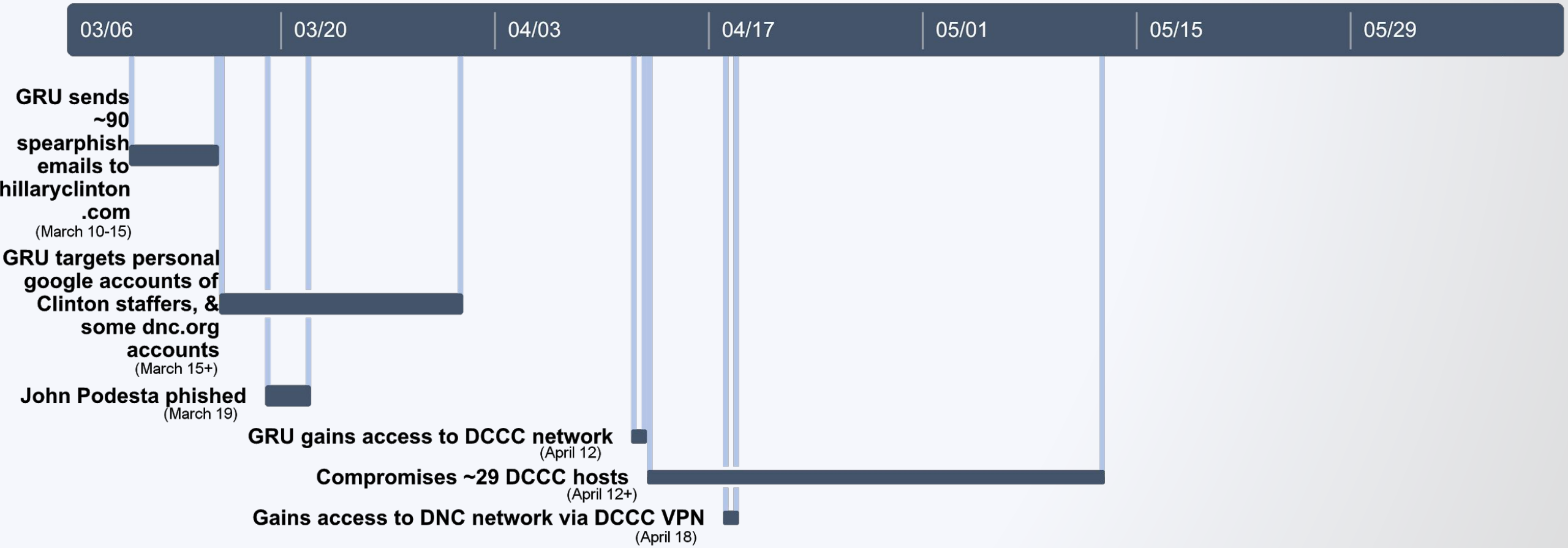
Democratic Party



Democratic Party




03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)
GRU gains access to DCCC network
(April 12)
Compromises ~29 DCCC hosts
(April 12+)


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)
GRU gains access to DCCC network
(April 12)
Compromises ~29 DCCC hosts
(April 12+)
Gains access to DNC network via DCCC VPN
(April 18)

Recommendations

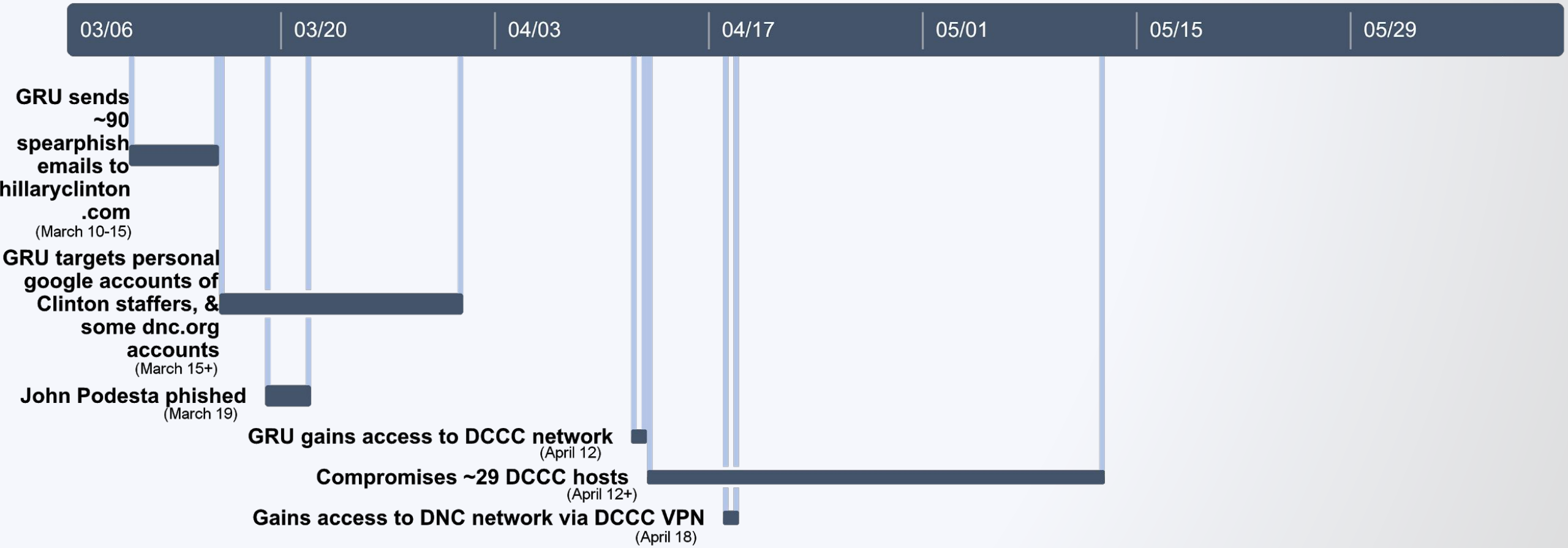
- “just” don’t allow 3rd party access into your network

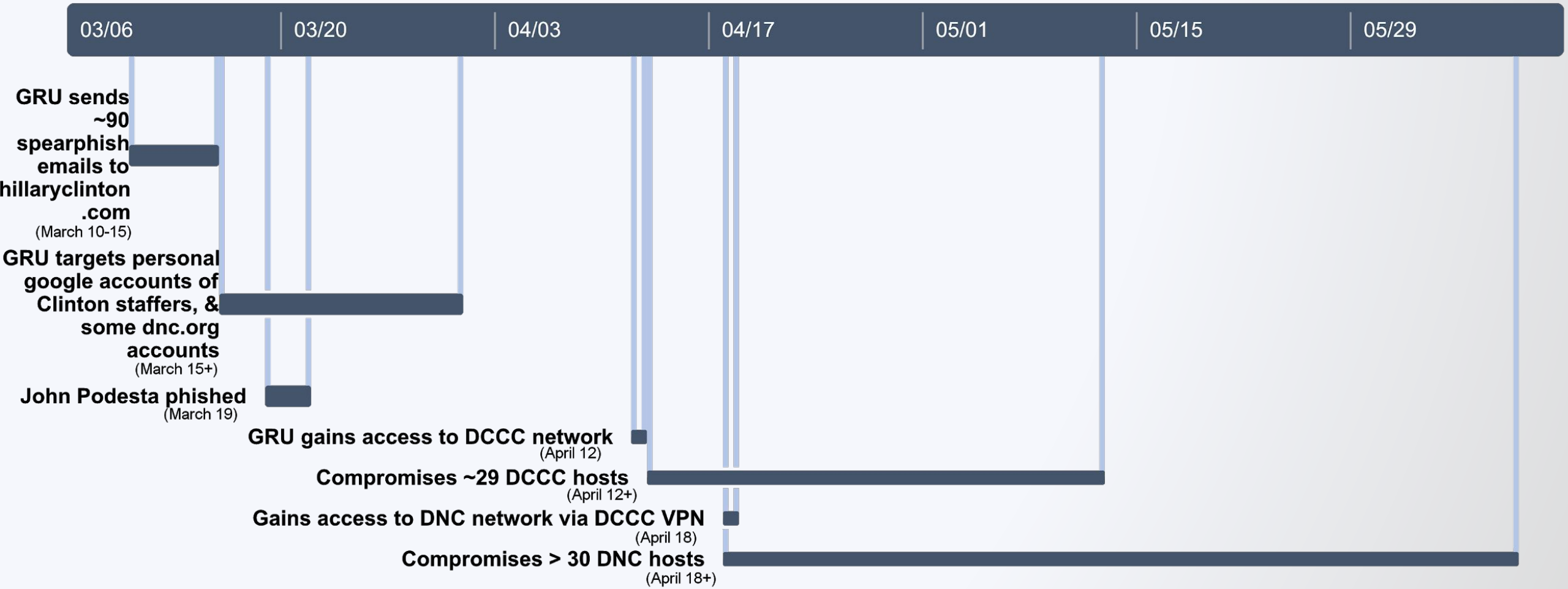
> The VPN in this case had been created to give a small number of DCCC employees access to certain databases housed on the DNC network.

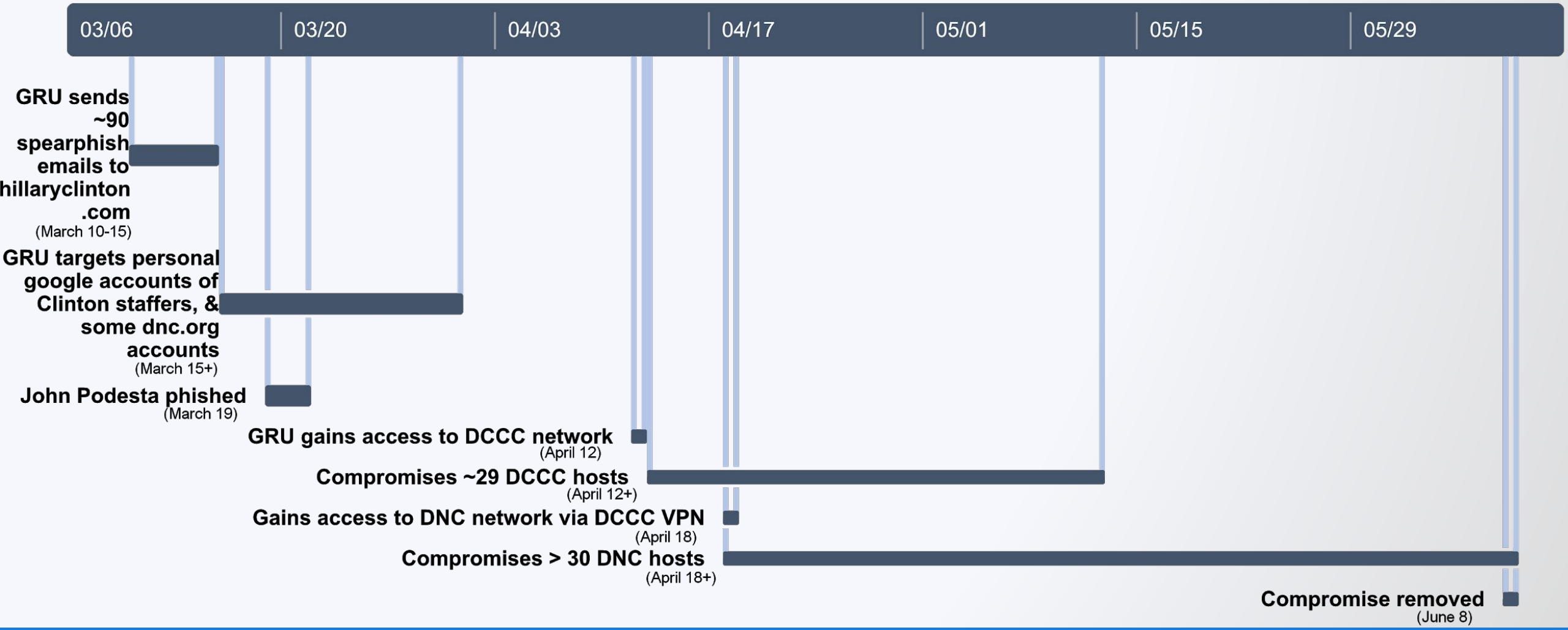
* Report Volume 1, p38

Recommendations

- ~~“just” don’t allow 3rd party access into your network~~
- segregate access, practice least privilege, add monitoring


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)
GRU gains access to DCCC network
(April 12)
Compromises ~29 DCCC hosts
(April 12+)
Gains access to DNC network via DCCC VPN
(April 18)


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)
GRU gains access to DCCC network
(April 12)
Compromises ~29 DCCC hosts
(April 12+)
Gains access to DNC network via DCCC VPN
(April 18)
Compromises > 30 DNC hosts
(April 18+)


03/06
03/20
04/03
04/17
05/01
05/15
05/29
GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)
John Podesta phished
(March 19)
GRU gains access to DCCC network
(April 12)
Compromises ~29 DCCC hosts
(April 12+)
Gains access to DNC network via DCCC VPN
(April 18)
Compromises > 30 DNC hosts
(April 18+)
Compromise removed
(June 8)

Installed tools

- X-Agent:
  - Log keystrokes, take screenshots, gather filesystem/OS info, etc
- X-Tunnel:
  - Create an encrypted tunnel for large-scale data transfers
- Mimikatz
- rar.exe

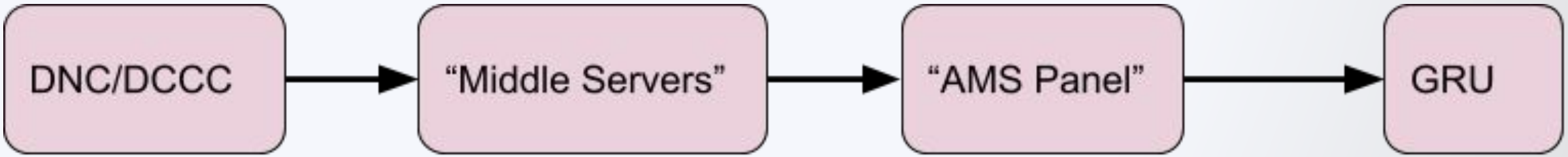
Stolen data

- keylog sessions containing passwords, internal communications, banking information, sensitive PII
- internal strategy documents, fundraising data, opposition research, emails from work inboxes
- exfiltrated > 70GB in election documents

Structure of GRU

- 26165
  - spearphishing
  - building malware
  - mining bitcoin
- 74455
  - assisted with release & promotion of stolen materials
  - “Officers from Unit 74455 separately hacked computers belonging to state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.” (Report Volume 1, p37)

Exfiltration



Recommendations

- alert on mimikatz
- endpoint monitoring
- network segregation
- IDS?

Blue Team Conclusions

- attack vectors: spearphishing, lateral movement via overprivileged permissions & mimikatz
- defense in depth: 2fa, endpoint monitoring, least privilege, etc
- few organizations can defend against a nation state

Background

- Volume 1: Russian interference in 2016 election
  - II. “Active Measures” social media campaign
  - III. Hacking/dumping campaign
- Volume 2: Administration obstruction of justice

Personal Security Learnings

Sources

- Twitter DMs, Facebook messages, LinkedIn messages & emails

[90] 8/19/16 Facebook Message, ID 100009922908461 (Matt Skiber) to ID PP [redacted]

[91] 12/8/16 Email, robot@craigslist.org to beingpatriotic@gmail.com (confirming Craigslist advertisement).

[92] 8/18-19/16 Twitter DMs, @march_for_trump & PP [redacted]

Sources

- Text messages

[355] FS00011 (1/21/16 Text Message, Sater to Cohen (7:44 p.m.));

- Call records

[351] Telephone records show a 20-minute call on January 20, 2016 between Cohen and the number Poliakova provided in her email. Call Records of Michael Cohen Grand Jury [redacted] After the call, Cohen saved Poliakova's contact information in his Trump Organization Outlook contact list. 1/20/16 Cohen Microsoft Outlook Entry (6:22 a.m.).

Sources

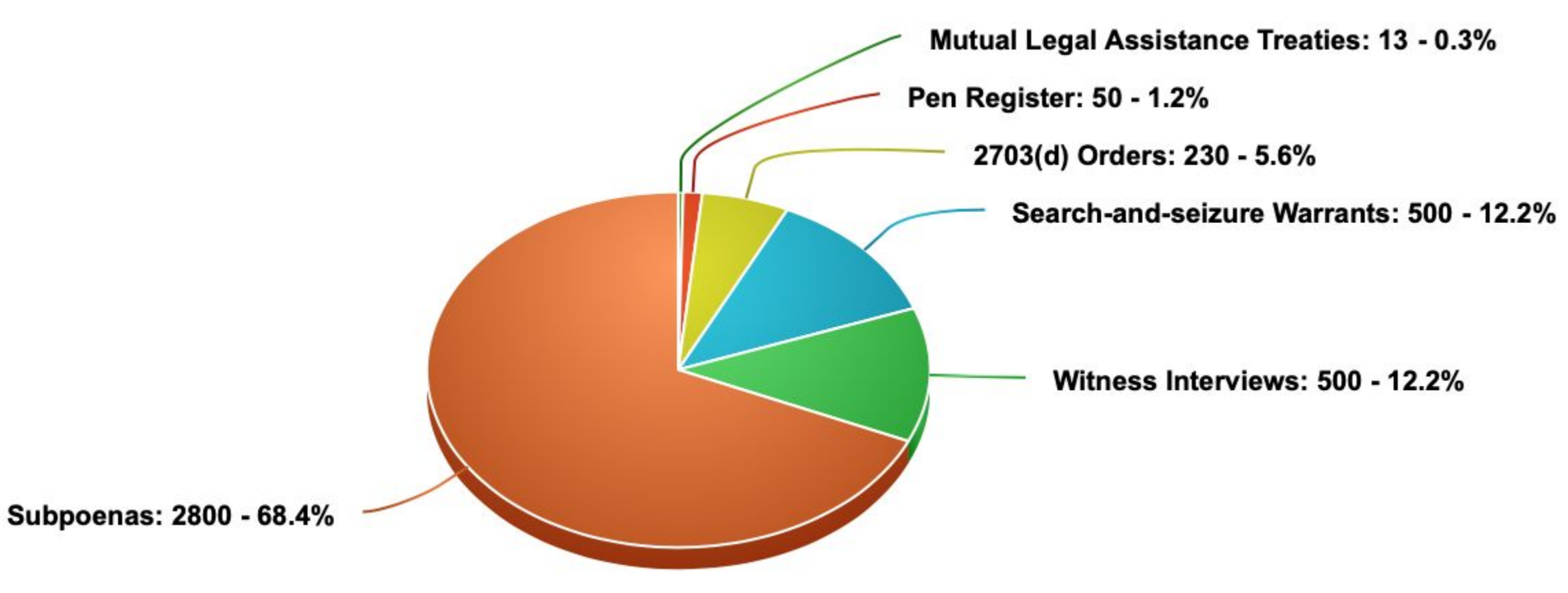
- Internet search histories

[424] Papadopoulos 8/10/17 302, at 3; Papadopoulos 2/10/17 302, at 2-3; Papadopoulos Internet Search History (3/24/16) (revealing late-morning and early-afternoon searches on March 24, 2016 for "putin's niece," "olga putin," and "russian president niece olga," among other terms).

Sources

- Company financial records
- US State Department visa records
- Hotel / flight / CBP records

Sources



* Report Volume 1, p13

Michael Cohen

- Credit: Marcy Wheeler (@emptywheel)
- 7/18/2017: warrant on Michael Cohen's Google activity from 1/1/2016 - 7/18/2017
- 8/8/2017: warrant on Michael Cohen's iCloud account
- 11/13/2017: warrant on business email hosted by 1&1

Michael Cohen

- Credit: Marcy Wheeler (@emptywheel)
- 11/7/2017 & 1/4/2018: pen-registers for real time communications info
- 2/8/2018: Mueller handed off Cohen investigations to SDNY
- 4/8/2018: SDNY got warrant for stingray to figure out what room in hotel

Michael Cohen

- Credit: Marcy Wheeler (@emptywheel)
- 4/9/2018: SDNY got warrant for that hotel room, Cohen's home/office/hotel raided

What Didn't Work

The investigation did not uncover evidence of Manafort's passing along information about Ukrainian peace plans to the candidate or anyone else in the Campaign or the Administration. The Office was not, however, able to gain access to all of Manafort's electronic communications (in some instances, messages were sent using encryption applications).

What Didn't Work

Gates stated that, in accordance with Manafort's instruction, he periodically sent Kilimnik polling data via WhatsApp; Gates then deleted the communications on a daily basis.[892]

What Didn't Work

Further, the Office learned that 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.

Personal Security Conclusions

- be cognizant about what data you share
- e2e encryption works
  - expiring messages protect against physical device access

Rate this Session

SCAN THE QR CODE TO COMPLETE THE SURVEY

Non-Political Security Learnings from the Mueller Report

Arkadiy Tetelman (@arkadiyt)

Thank You!