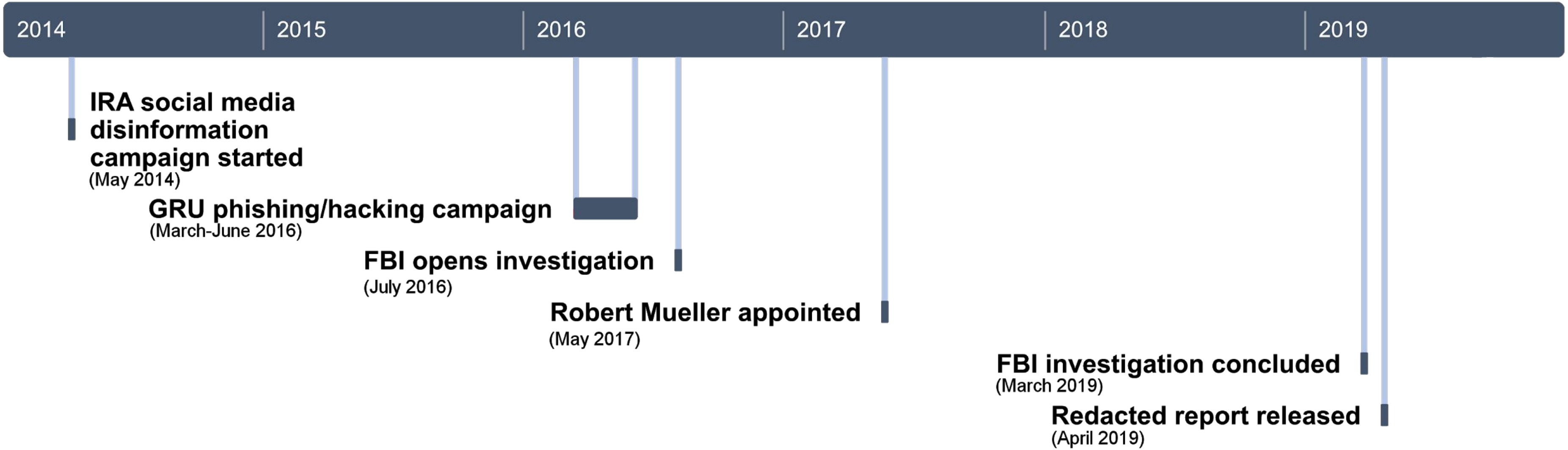
Non-Political Security Learnings from the Mueller Report

Arkadiy Tetelman (@arkadiyt)

Agenda

- Background
- Blue Team Learnings
    - timeline of attacks; recommendations
    - tools installed by GRU
    - data stolen from DNC/DCCC
    - structure of GRU
    - data exfiltration
- Questions

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)

Background

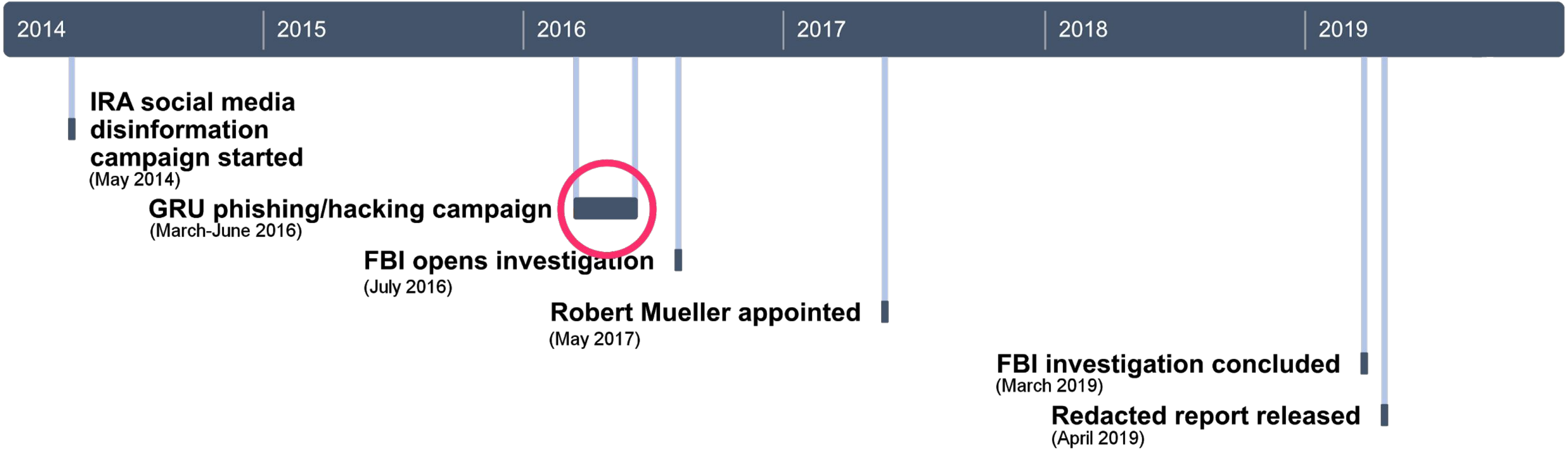
- 2 years 8 months
- Employed:
  - ~22 attorneys & paralegals
  - ~9 support staff
- Worked alongside:
  - ~40 FBI staff (agents, analysts, etc)
- Estimated cost: $25M
- Estimated gain: $48M

Background

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

Blue Team Learnings

Timeline



IRA social media disinformation campaign started
(May 2014)

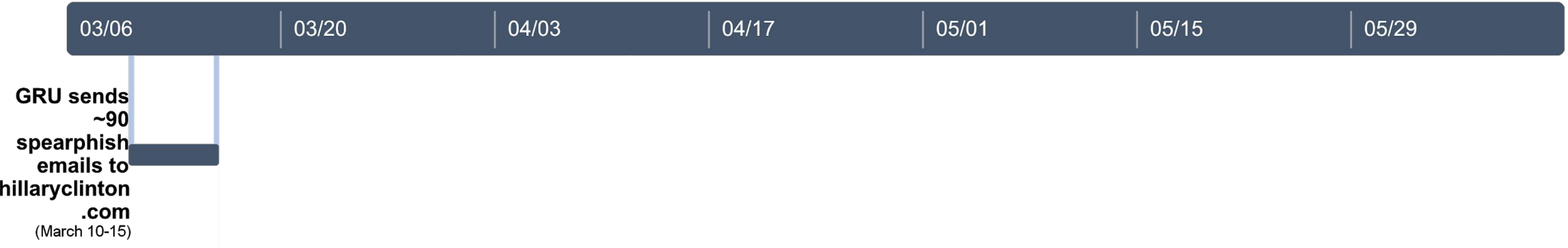
GRU phishing/hacking campaign
(March-June 2016)

FBI opens investigation
(July 2016)

Robert Mueller appointed
(May 2017)

FBI investigation concluded
(March 2019)

Redacted report released
(April 2019)



03/06

03/20

04/03

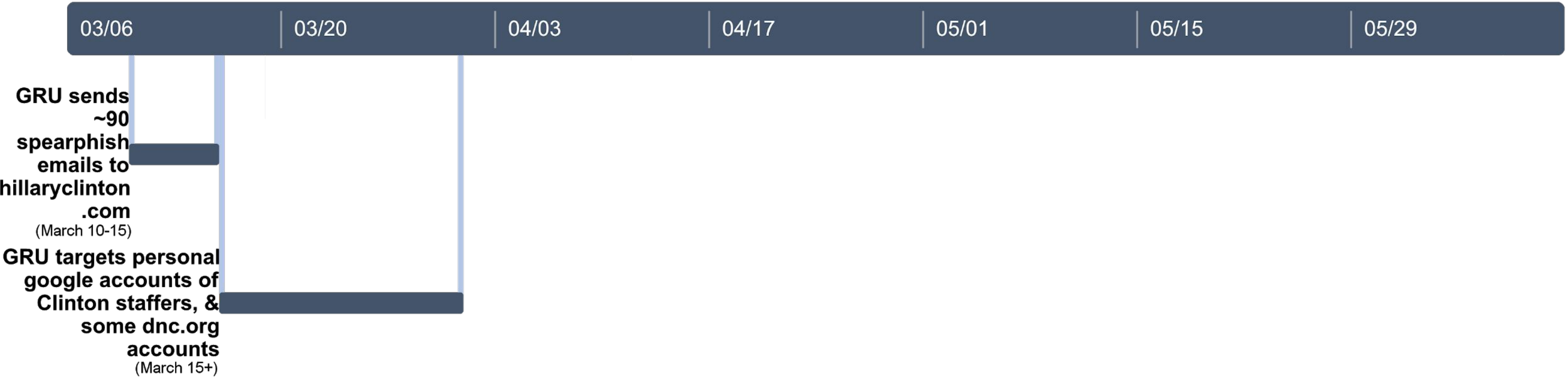
04/17

05/01

05/15

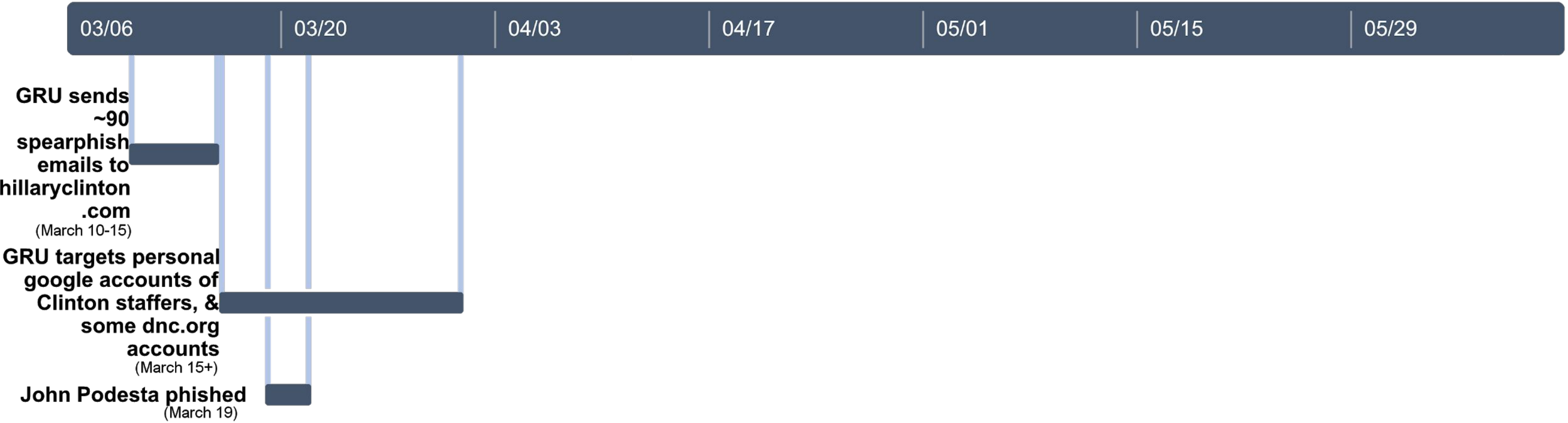
05/29

GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)



GRU sends ~90 spearphish emails to hillaryclinton.com
(March 10-15)

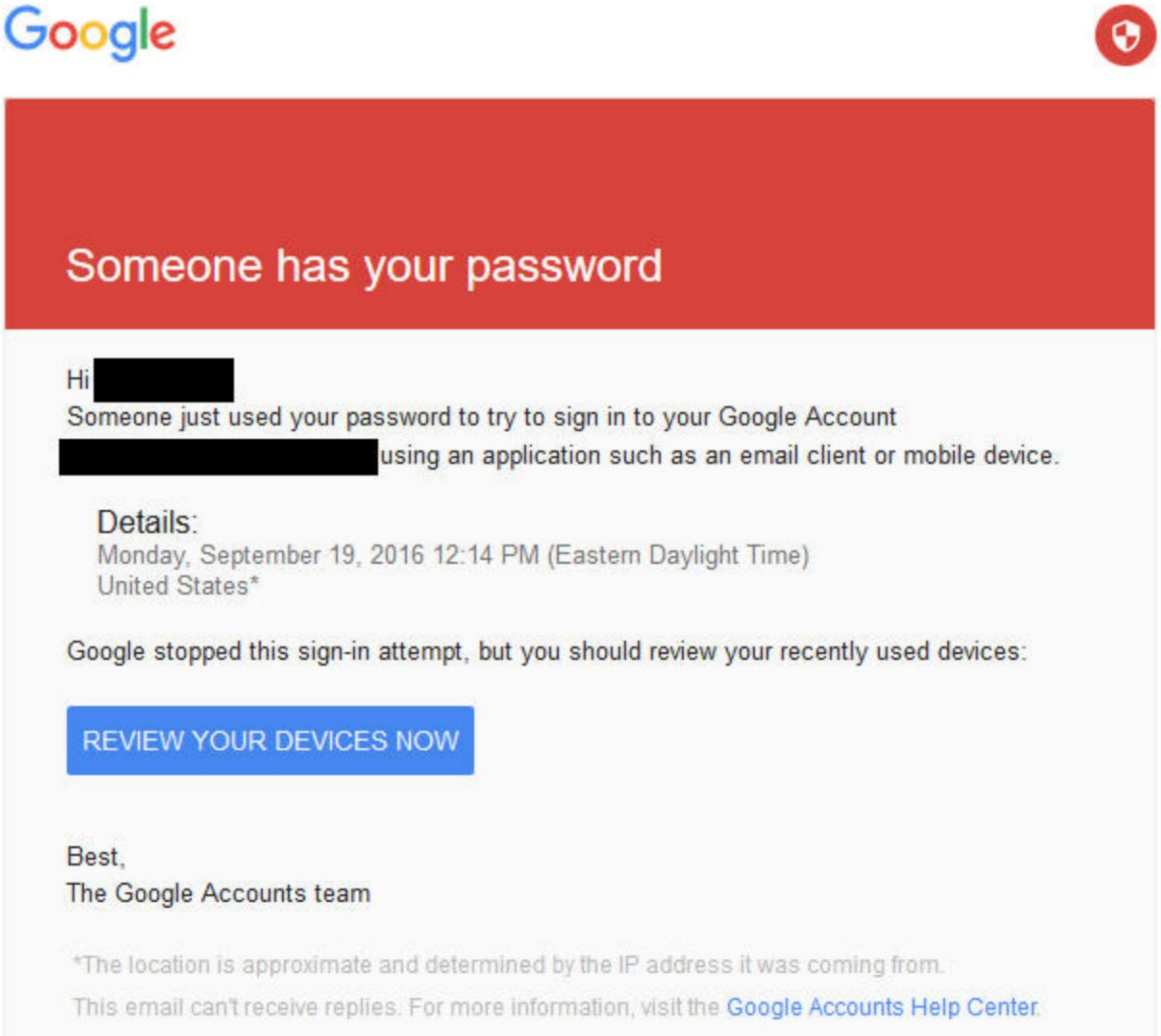
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)



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)



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.

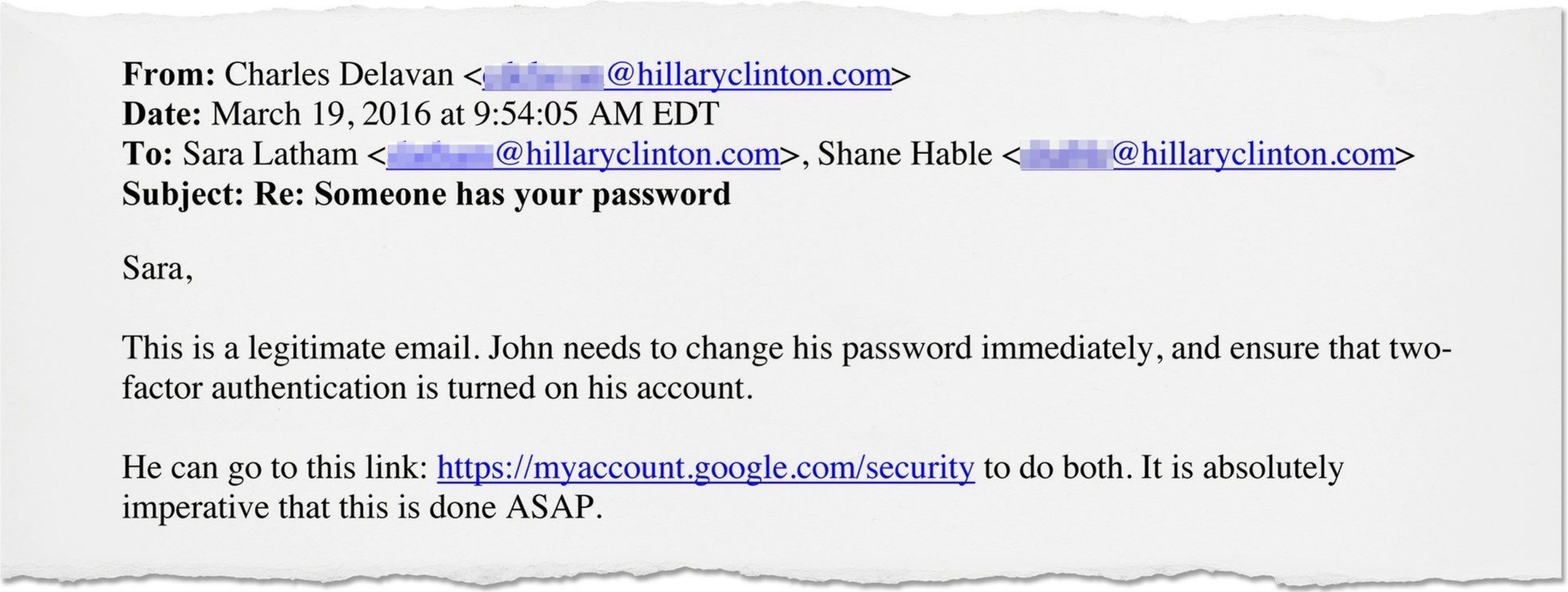
Details:
Monday, September 19, 2016 12:14 PM (Eastern Daylight Time)
United States*

Google stopped this sign-in attempt, but you should review your recently used devices:

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.**

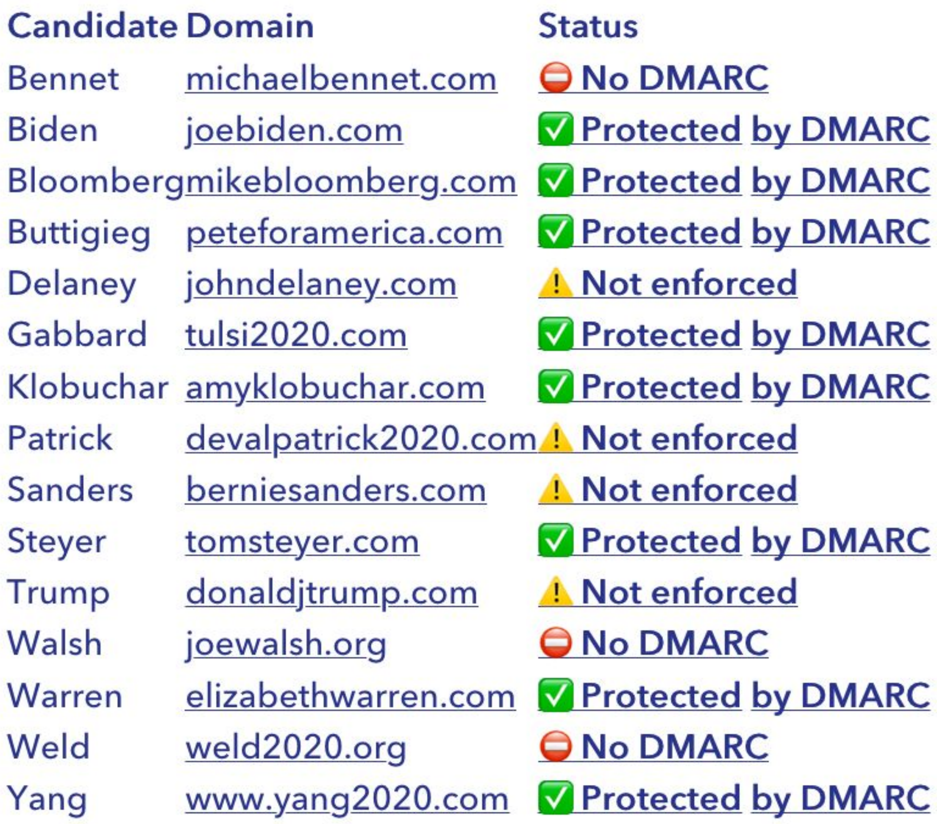
* https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

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

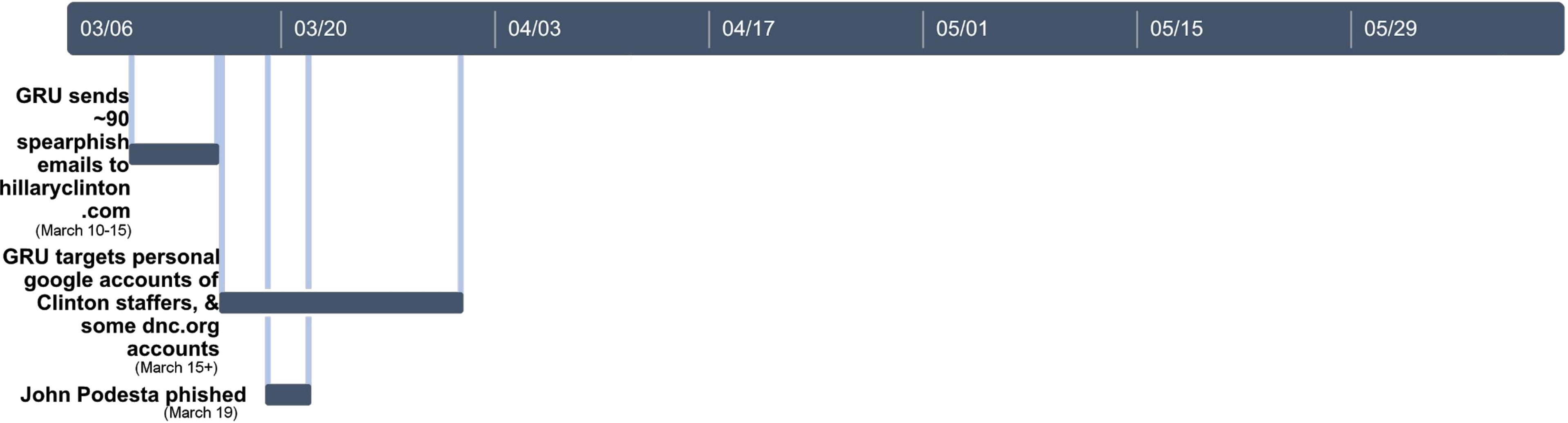
Recommendations

- Password manager / hardware (U2F, WebAuthn) 2fa tokens
  - https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing
- Ingest & alert on DNS
- Scan incoming emails
- Ingest mail audit log events
- Phishing exercises?
- SPF/DKIM/DMARC, MTA-STS, TLS-RPT



Candidate	Domain	Status
Bennet	michaelbennet.com	⛔ No DMARC
Biden	joebiden.com	✅ Protected by DMARC
Bloomberg	mikebloomberg.com	✅ Protected by DMARC
Buttigieg	peteforamerica.com	✅ Protected by DMARC
Delaney	johndelaney.com	⚠ Not enforced
Gabbard	tulsi2020.com	✅ Protected by DMARC
Klobuchar	amyklobuchar.com	✅ Protected by DMARC
Patrick	devalpatrick2020.com	⚠ Not enforced
Sanders	berniesanders.com	⚠ Not enforced
Steyer	tomsteyer.com	✅ Protected by DMARC
Trump	donaldjtrump.com	⚠ Not enforced
Walsh	joewalsh.org	⛔ No DMARC
Warren	elizabethwarren.com	✅ Protected by DMARC
Weld	weld2020.org	⛔ No DMARC
Yang	www.yang2020.com	✅ Protected by DMARC

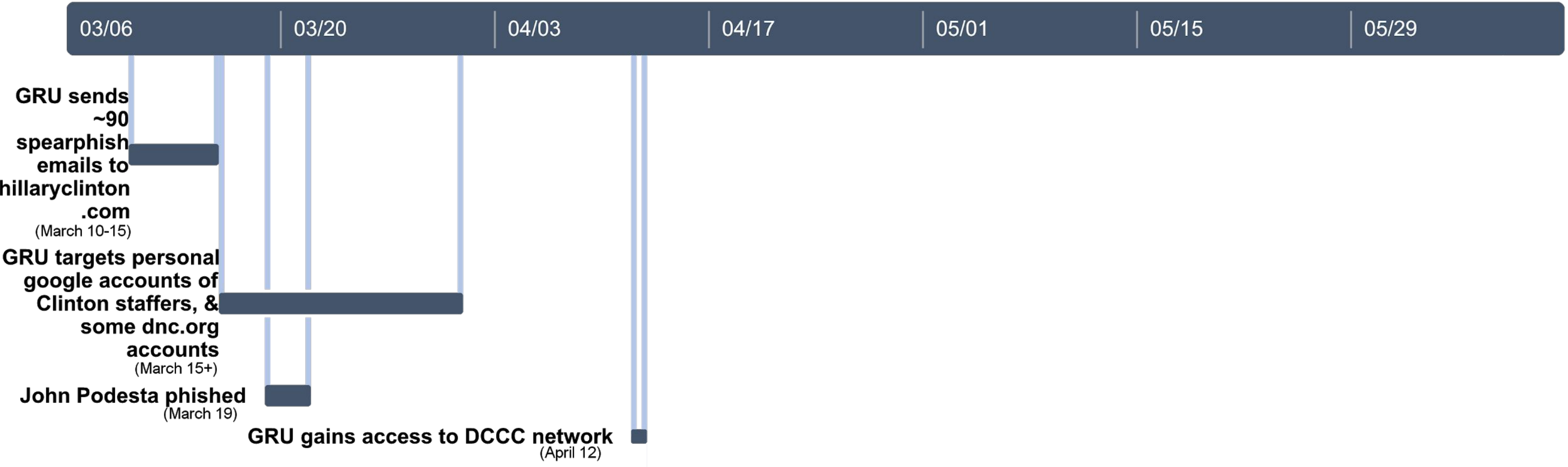
https://www.valimail.com/blog/campaign-security-milestone/
https://fireoakstrategies.com/email-and-website-security-for-the-2020-presidential-candidates/



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 sends ~90 spearphish emails to hillaryclinton.com
(March 10-15)

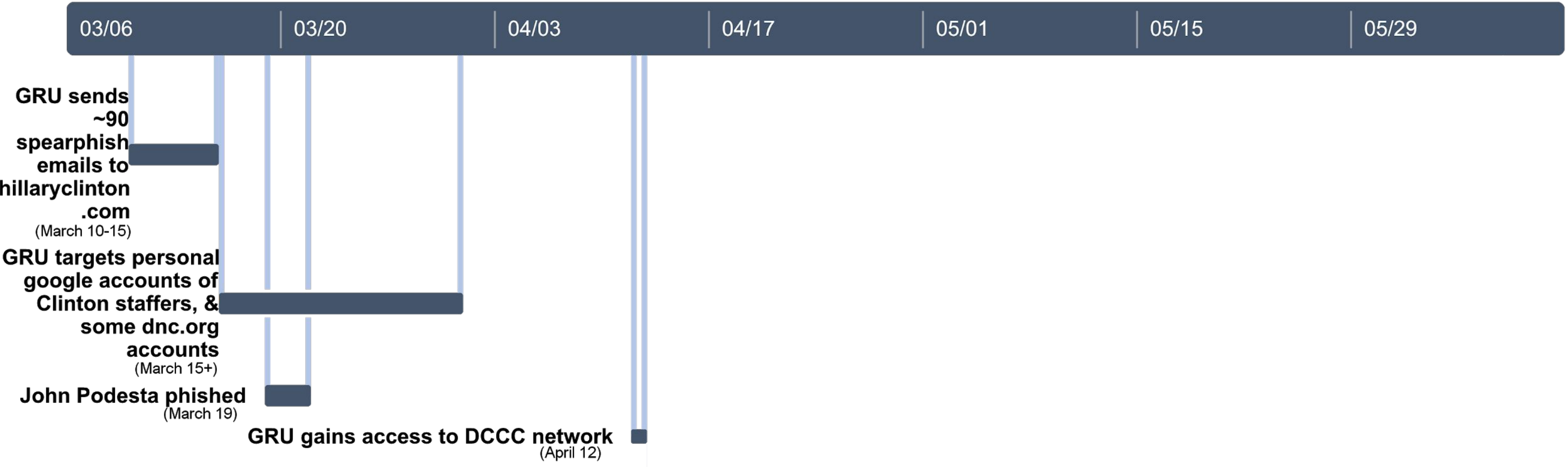
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)

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

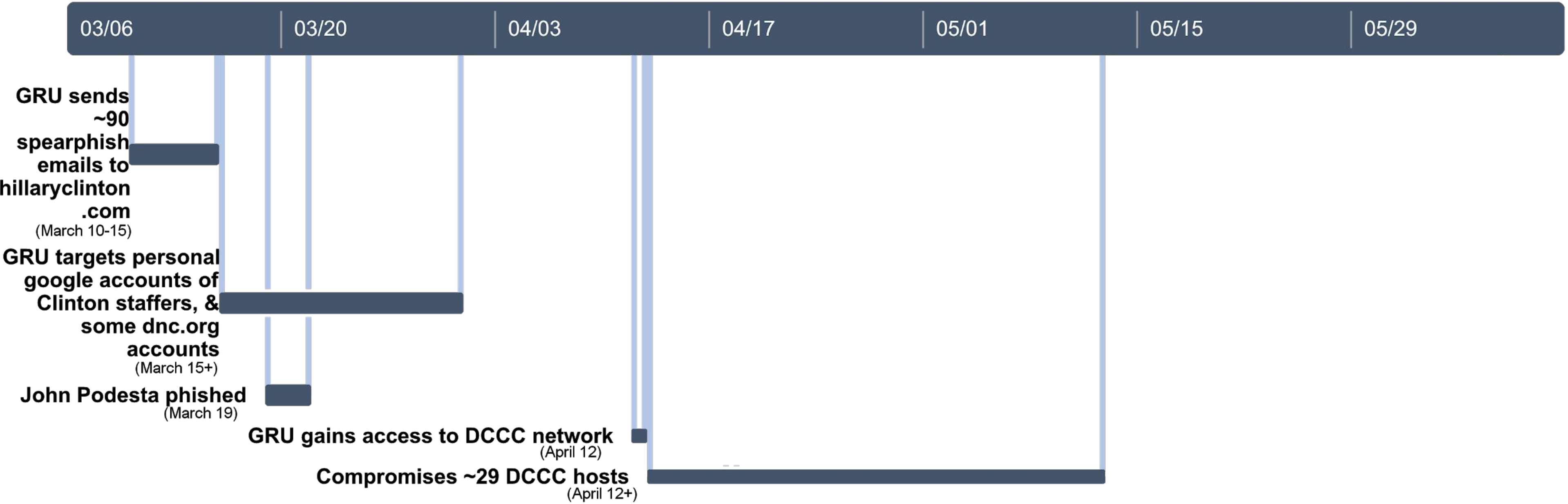


GRU sends ~90 spearphish emails to hillaryclinton .com
(March 10-15)

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)



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)

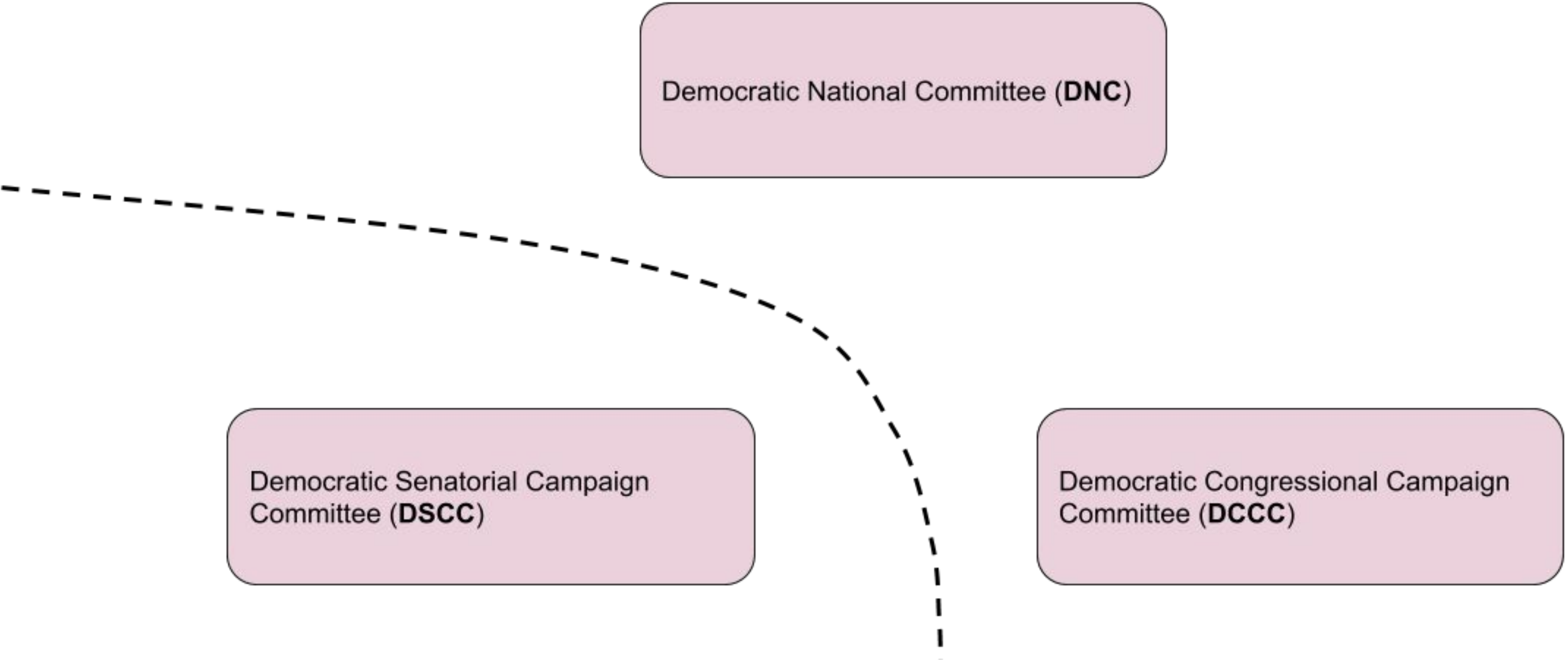
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)

John Podesta phished
(March 19)

GRU gains access to DCCC network
(April 12)

Compromises ~29 DCCC hosts
(April 12+)

Democratic Party

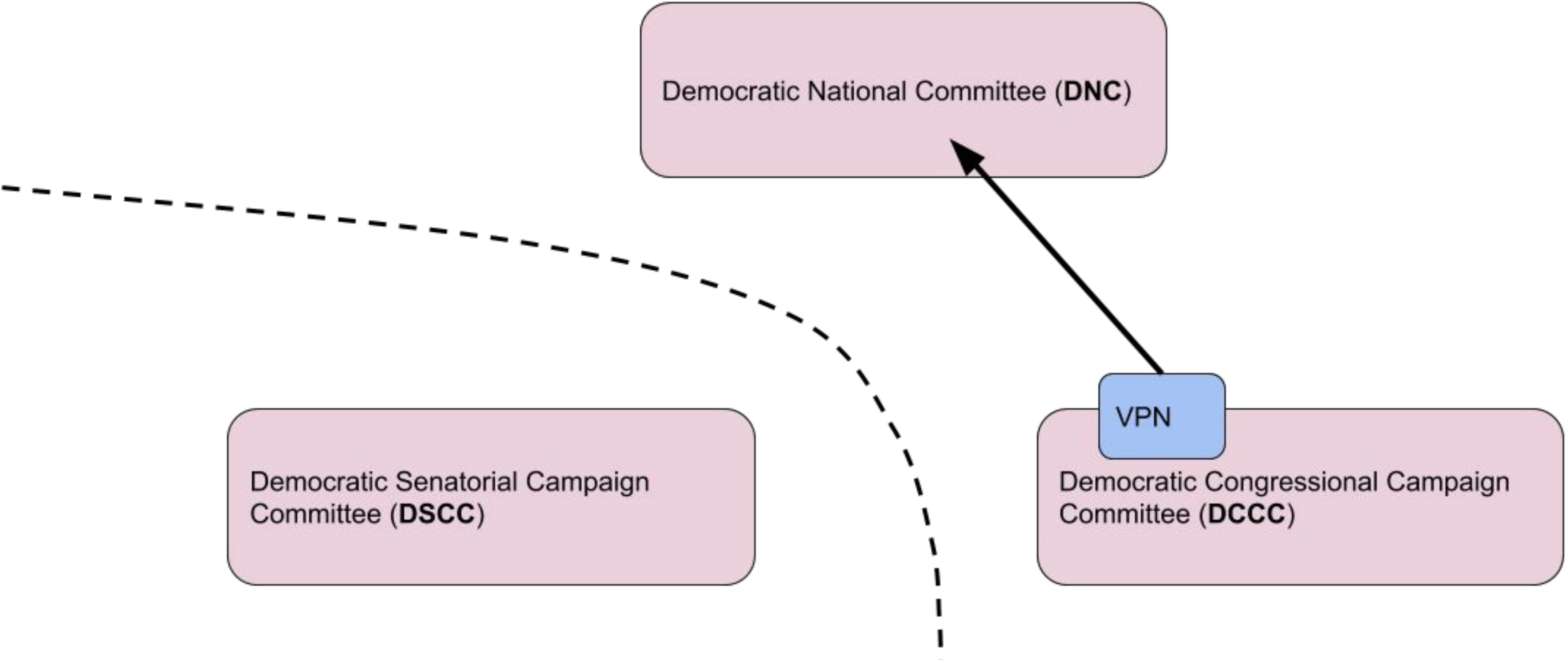


Democratic National Committee (**DNC**)

Democratic Senatorial Campaign Committee (**DSCC**)

Democratic Congressional Campaign Committee (**DCCC**)

Democratic Party

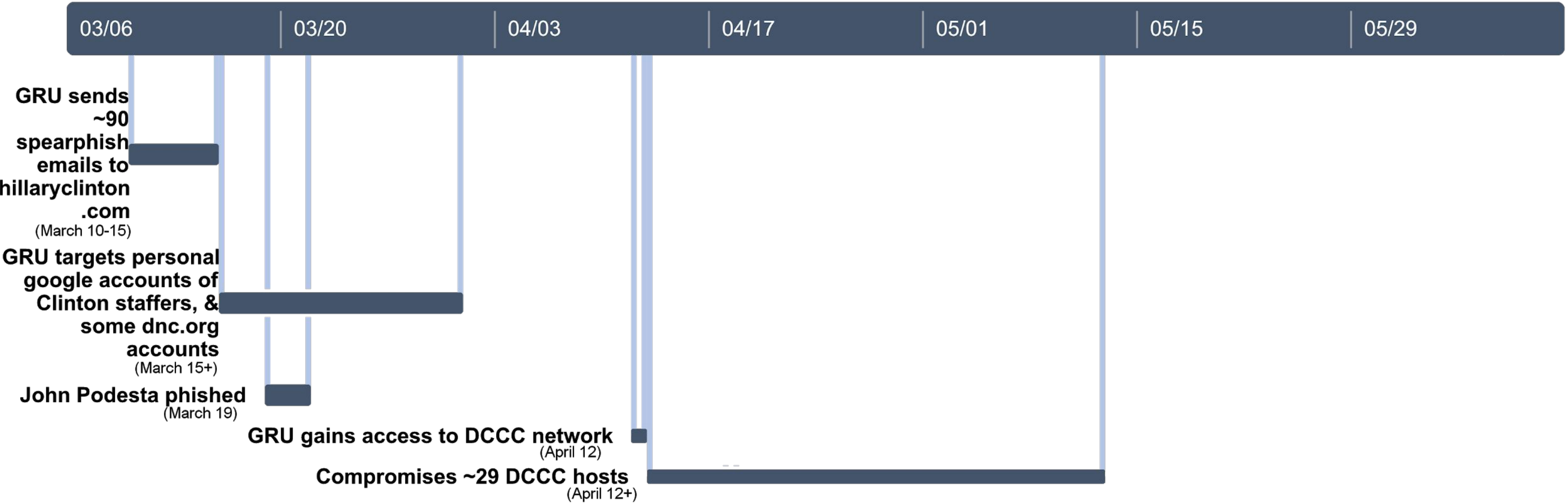


Democratic National Committee (**DNC**)

VPN

Democratic Senatorial Campaign Committee (**DSCC**)

Democratic Congressional Campaign Committee (**DCCC**)



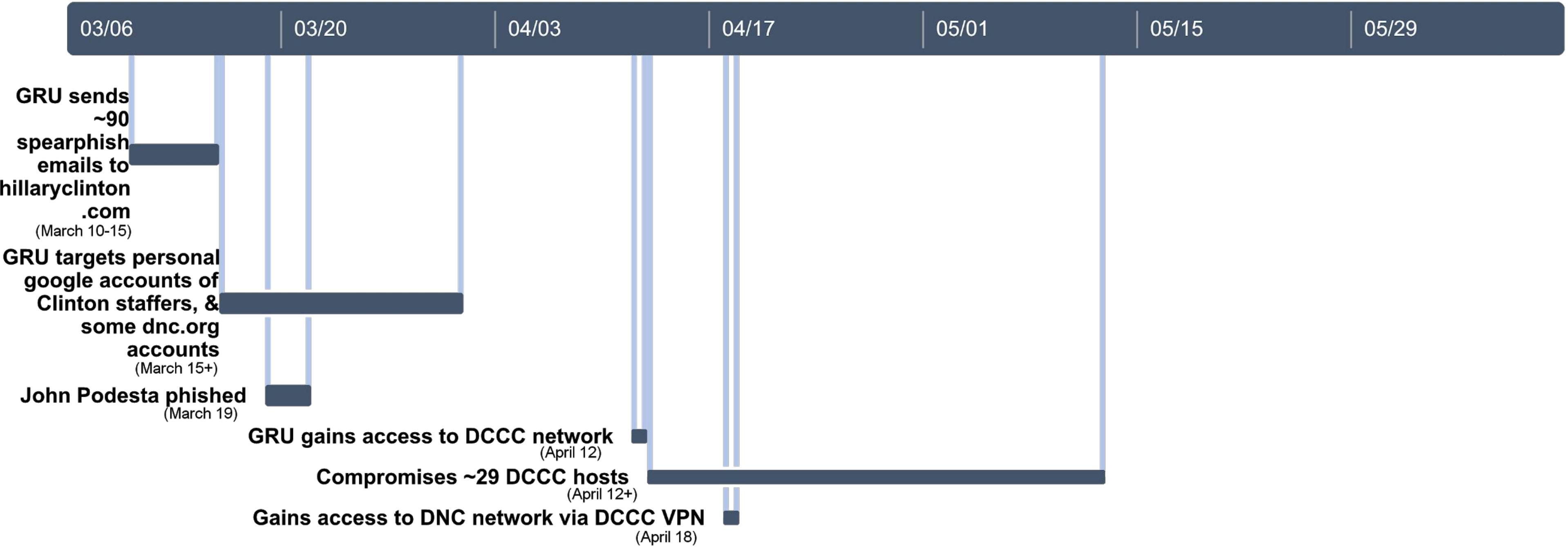
GRU sends ~90 spearphish emails to hillaryclinton.com (March 10-15)

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+)



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

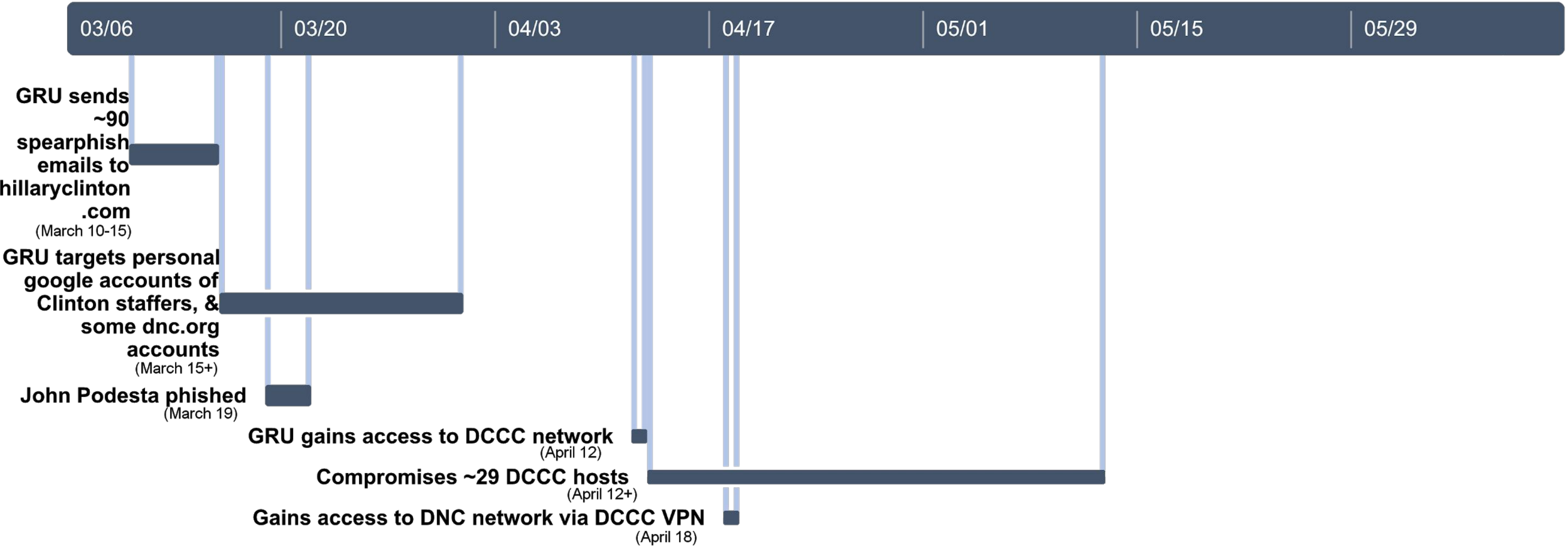
- **“just” don’t allow 3rd party access into your network**

> **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



GRU sends ~90 spearphish emails to hillaryclinton.com
(March 10-15)

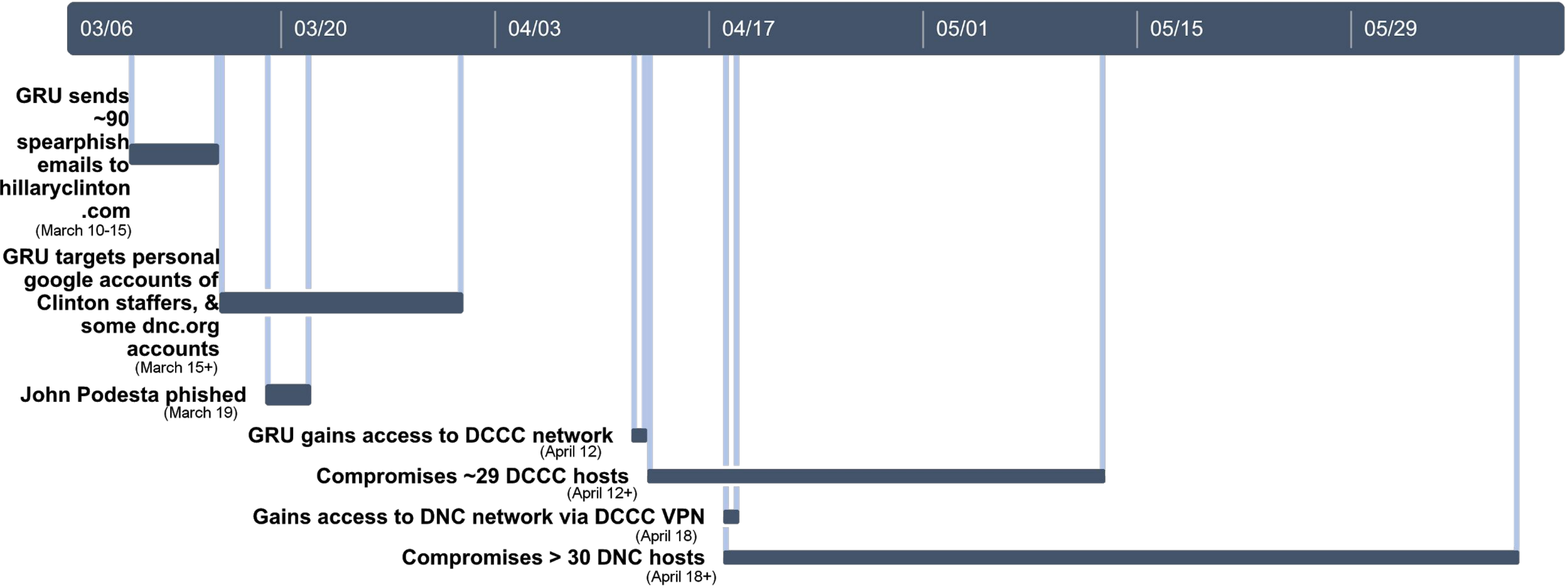
GRU targets personal google accounts of Clinton staffers, & some dnc.org accounts
(March 15+)

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)



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+)

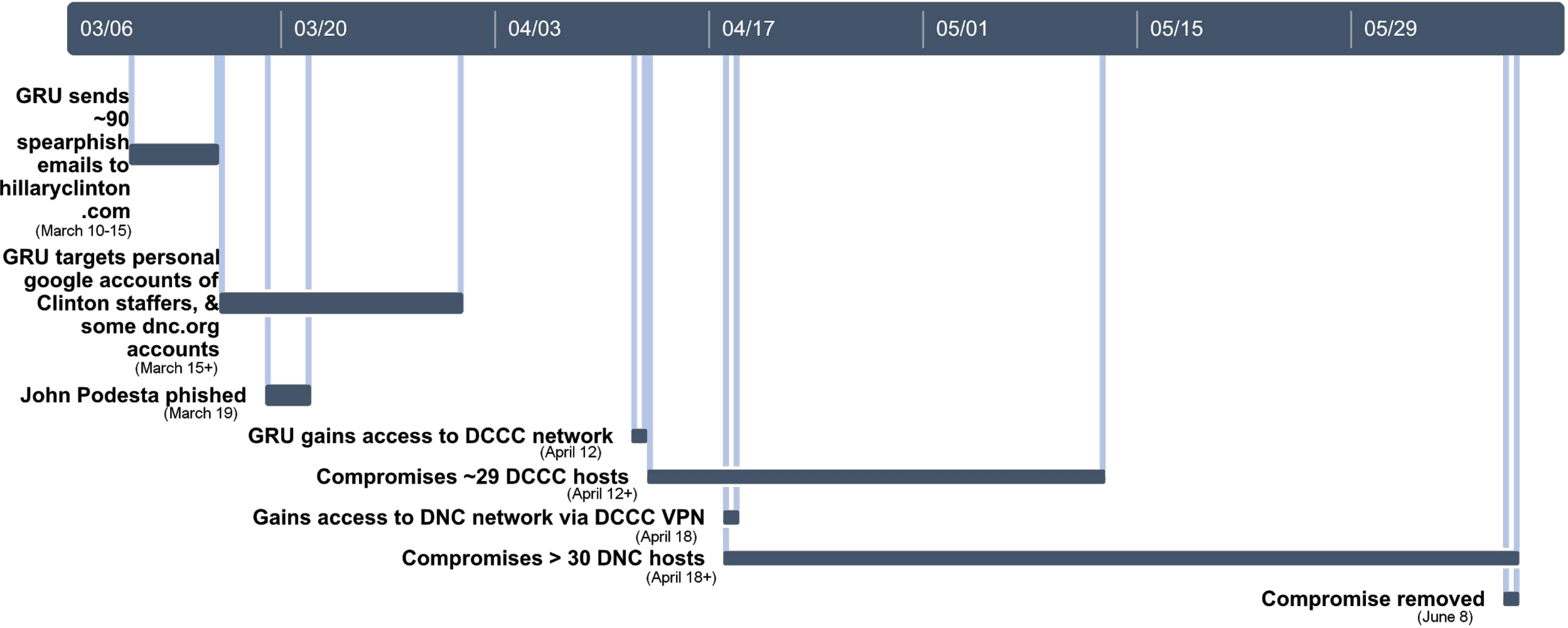
John Podesta phished
(March 19)

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+)



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**

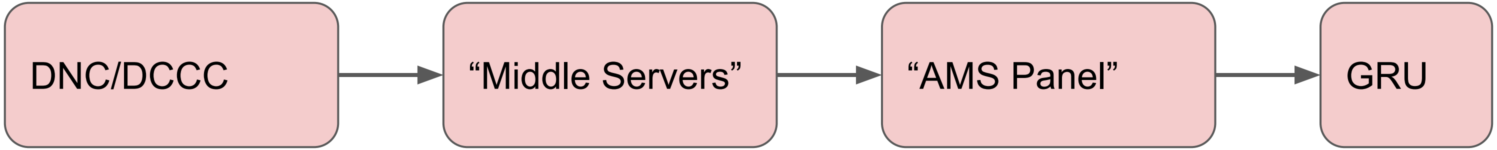
Stolen Data

- 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

- Unit 26165
  - spearphishing
  - building malware
  - mining bitcoin
- Unit 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



DNC/DCCC → “Middle Servers” → “AMS Panel” → GRU

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

Questions

Arkadiy Tetelman (@arkadiyt)