COVID-19 and Computer Security

Viruses, and not the Computer Kind

- The “Lectures” page says

> The lectures and readings listed here are subject to change, including in response to current events (i.e., major news items).

- I did not expect a real, biological virus to count, but. . .

Computer Effects of Covid-19

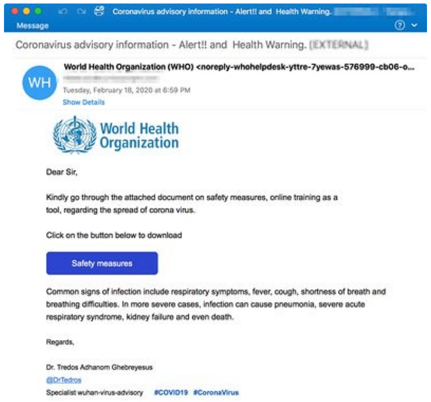
- Scams
- Phishing
- Malware
- VPNs and firewalls
- Internet conferencing (and classes)

Scams

- A Google query for “scams coronavirus” Wednesday night got 75,000,000 hits. . .
- Thousands of new domains mentioning “Coronoavirus” have been registered since January
- Most, of course, are bad news

Covid-19 and Phishing

- Scammers are of course doing phishing, too



Coronavirus advisory information - Alert!! and Health Warning. [redacted]

Coronavirus advisory information - Alert!! and Health Warning. [redacted]

World Health Organization (WHO) <noreply-whohelpdesk-yttre-7yewas-576999-cb06-o...

[redacted]

Tuesday, February 18, 2020 at 6:59 PM

Dear Sir,

Kindly go through the attached document on safety measures, online training as a tool, regarding the spread of corona virus.

Click on the button below to download

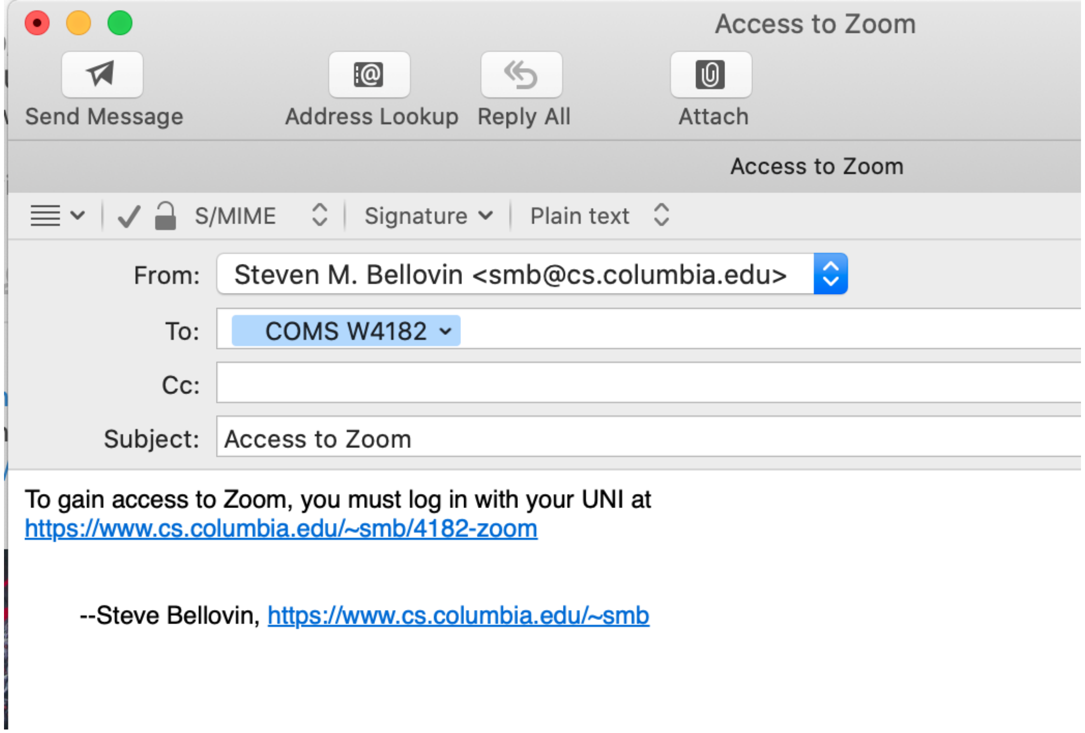
Common signs of infection include respiratory symptoms, fever, cough, shortness of breath and breathing difficulties. In more severe cases, infection can cause pneumonia, severe acute respiratory syndrome, kidney failure and even death.

Regards,

Dr. Tredos Adhanom Ghebreyesus
@DrTedros
Specialist wuhan-virus-advisory #COVID19 #CoronaVirus

- Also: fake purchase orders for, e.g., hand sanitizer

Even I Can Do It. . .



From: Steven M. Bellovin <smb@cs.columbia.edu>

To: COMS W4182

Cc:

Subject: Access to Zoom

To gain access to Zoom, you must log in with your UNI at
https://www.cs.columbia.edu/~smb/4182-zoom

--Steve Bellovin, https://www.cs.columbia.edu/~smb

Though it would look more authentic if it seemed to come from the Provost

Malware

- Malware is popular, too
- Example: a fake virus map website installs a back door
- How about airlines, hotels, event organizers?
- A lot of spam filters won't catch these for a while—there's no database of such messages yet

VPNs and Firewalls

- Private Virtual Private Networks (VPNs) are ideal for telecommuters
- They give access to the entire corporate net
- But there are risks

How Secure is Your VPN?

- Cryptographic security (probably pretty good)
- Buggy code—*always* an issue
- Authentication

But. . .

- The buggy code and the bad authentication have always been there
- Why are they risks now?
- Because everyone is thinking about them now

Fate-Sharing

- Everyone exiting a firewall appears to have the same IP address
- This means that the behavior of any user of the VPN will be attributed to all of them
- In other words, VPNs can trigger false positives by intrusion detection systems

Current Awareness

- Employees are using the VPN, perhaps for the first time
- Will they fall for phishing or spearphishing?
- Is it set up properly on employee computers?
- For that matter, is the gateway set up properly?

VPN Authentication

- How do you authenticate to the VPN?
- Passwords?
- Shared secrets stored on employee's computers?
- Shared secrets stored on employee's hacked computers?
- Btw, what is the corporate policy on BYOD? Did it suddenly need to change?
- Or is multi-factor authentication set up?

Working from Home

- Do enough employees have devices?
- Are they secure enough?
- How do you do patch management for such devices?
- What about phones?

Support

- What about tech support? Do employees bring ailing computers into the (deserted) office?
- Is your IT support team up to date on home laptops and VPNs?
- Do you use managed providers? Can they (or you) handle the sudden load?

Who’s Essential?

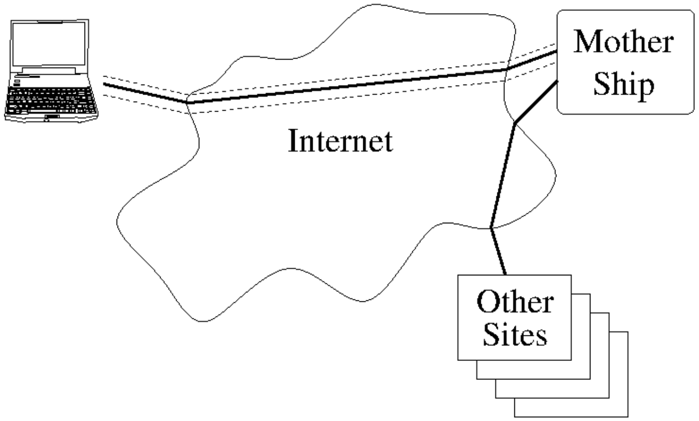
- Maybe it’s too risky to have everyone work from home
- Maybe it should only be essential employees
- That lets you give them equipment, train them, etc.

Firewall Configurations

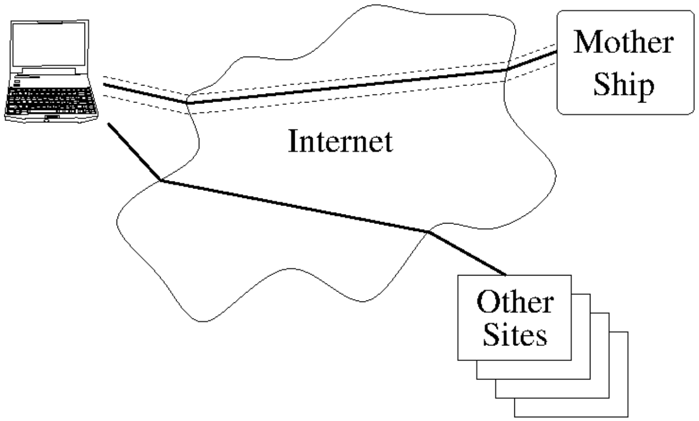
- Does your VPN send all traffic to the gateway, or does non-work traffic go direct to the Internet?
- Triangle routing: provide firewall protection for home laptops
- But—most web traffic is encrypted; does the firewall help?
- But—it's a lot of extra traffic; was your link bandwidth configured correctly for this scenario?

Triangle Routing versus Split Tunneling

Triangle Routing



Split Tunneling



Meetings

- Businesses run on meetings
- So do most other organizations
- And, of course, there are classes
- Move them online: Zoom, Skype, WebEx, GotoMeeting, more
- Are they secure?
- Maybe. . .

Which Meeting Software?

“If a vendor uses Zoom and they schedule the meeting we use Zoom (on Windows). If I schedule the meeting it’s WebEx, which is one click in Outlook to add to the calendar appointment. Also Cisco is our phone vendor and our video conference room vendor so stuff integrates to a frightening extent.”

Remote Meeting Security Issues

- Crypto (probably good enough)
- Buggy code
- Usability

Buggy Code

- All code is buggy
- Zoom had a serious security issue last year: their Mac software let anyone hijack your camera
- Why? “User-friendliness”. . .

Usability

- How easy is it to accidentally invite others to a meeting?
- (What would happen if I published the URL for this class?)
- What if autocomplete on email sends a message to the wrong person?

Case Study: The U.S. Congress

- Suppose that Congress feels that it’s too risky to meet in person
- Can they meet electronically?
- What about every else they need to do?
- Remember: this is a high-threat scenario; many intelligence agencies would love to mess with this

Requirements: Meetings

- The entire House and the entire Senate
- Many committees—some have fixed membership; others are ad hoc
- Mechanism to give the committee chairs control
- Internal meetings: Members with staffers, groups of staffers, etc.
- Some meetings are public and should be webcast and recorded
- Some meetings involve classified material—but may still need to be recorded

Requirements: Voting

- Either house and any regular committee can hold votes
- Member votes are often—but not always—recorded (Constitution: “the yeas and nays of the members of either House on any question shall, at the desire of one-fifth of those present, be entered on the journal.”)
- Voting process is *heavily* constrained by process and tradition

Requirements: Other

- Strong authentication is required
- (Some years ago, executive branch employees had ID cards with chips—but Senate staffers had ID cards with *pictures* of a chip. . .)
- Email: internal to a Member’s office, between offices, to/from constituents, etc. (exists today)

Voting Design

- Probably no existing software—while there is online voting software, it probably doesn't meet Congress' requirements
- Today: Members have "voting cards" that they use to authorize their vote, and to supply their name for the written record
- Likely solution: some form of MFA, probably an ID card with a chip

Meetings

- Commerical meeting software may meet the base functionality issue—but is it secure enough?
- Remember the enemies: the intelligence services of the world
- "Probably secure" cruypto is not good enough
- Is the meeting server secure? Are their employees trustworthy?
- Or would the attackers go after the Member's (and their staffers') computers?
- (Would they tamper with a close vote? Probably not—it would be too easily detected, when some Member realized that their vote was listed incorrectly. But would anyone hand-count the recorded votes?)

Email

- In principle, it's the same as today
- (Some Members don't use email—email didn't exist in the latter part of the 19th century—but *all* of their staffers do)
- Is it secure enough?

Member and Staffer Computers

- Arguably, the weakest point
- Perhaps have a permanent VPN, which will reject all non-Congressional packets
- It doesn't work...

Always-On VPN

- People travel and need to get at hotel, etc., sign-in screens
- There’s still a need for external email and external web access
- If nothing else—and there are many other needs—there’s an absolute requirement to communicate with other parts of the government

Multiple Devices?

- Perhaps everyone should have two devices, one a general-purpose computer for email, Web, etc., and one for meetings and voting; the latter would have a VPN
- That might work, with the proper configuration and restrictions

Physical Security

- How should these devices be protected from physical intrusions?
- Might an intelligence agency stage a “black bag job”?
- Should local police provide 24/7 physical security?

Classified Material

- The U.S. government has strict rules on handling classifed material
- The most sensitive information can only be handled in a “SCIF” (Sensitive Compartmented Information Facility)
- (The Wikipedia page on SCIFs has a lot of good references.)
- (“Compartmented” refers to the code words you see in the movies—during World War II, for example, “ULTRA” meant “derived from cryptanalysis”)
- SCIFs have requirements for alarms, guards, and more
- There are many SCIFs in the Capitol—but I doubt that any Members have home SCIFs
- At best, they could try to borrow a local FBI SCIF
- Conclusion: handling classified information in a distributed Congress probably doesn’t work

It’s Complicated!

- Even if all of the necessary software exists, it will take a lot of work to set all this up
- There’s also the issue of training and support
- Each Member runs their own office—the Senate or House IT staff has very limited ability to tell Members what to do
- Columbia took a couple of weeks to commit to Zoom classes—and they’d been experimenting with Zoom for about two years
- Even so: two days for training and preparation, profs had to learn how to use Zoom, SEAS (at least) bought a lot of tablets and cameras for folks who don’t have them, etc.
- And some of this training could be security-sensitive

Conclusions

- Setting this up properly will take a couple of weeks at a minimum
- I *hope* they're already working on it
- There's no feasible way to handle classified material; Members and staffers for, e.g., the Intelligence Committees will have to stick around D.C. and go to work as usual
- At a guess, they'll go with commercial solutions for now and hope things settle down before an upgrade is in place
- Voting? They could always fall back to old-fashioned roll calls. . .

Corvid ’18