Avoiding Infection: A Cyber Threat Assessment of COVID-19

Sam Heavenrich, JD ‘22

Though COVID-19’s full impact has yet to be seen, it’s clear that the crisis has revealed and exacerbated major vulnerabilities in the United States’ digital infrastructure.

This paper explores four digital security threats that the pandemic crisis has substantially amplified. First, hackers have stepped up attacks on businesses by taking advantage of the sudden and drastic shift to remote work. Second, cyber threats to the public have increased as hackers opportunistically employ coronavirus-related topics to lure in vulnerable targets. Third, nation-states have exploited the crisis through disinformation campaigns, coronavirus-related spyware, and espionage operations that seek to obtain advance information about vaccine development. And finally, measures taken to slow the virus’s spread—such as large-scale location tracking through smartphone data—have prompted pushback from digital privacy advocates and civil libertarians, who warn that the new practices have not been sufficiently scrutinized and risk becoming entrenched.

These threats—a combination of magnified forms of existing dangers and entirely new ones—call for a holistic approach to cybersecurity that includes robust digital security practices and continued vigilance against the variety of bad actors that seek to take advantage of the crisis.

Cyber Threats to Businesses

Although some (but not all) cybercrime organizations have suspended attacks on medical and healthcare targets, hackers continue to target businesses by capitalizing on the explosive growth in remote work. Remote employees often use their personal devices, which may lack proper security protections against endpoint attacks. And accessing company information over unsecured Wi-Fi networks or through remote desktop software creates additional opportunities for hackers to gain access to internal networks.

To combat these threats, the Cybersecurity and Infrastructure Security Agency (CISA) recently announced that VPNs are now required for remote work. VPNs (virtual private networks) securely connect endpoints (the remote employee’s laptop or phone) to the company’s internal network. However, they are not a panacea—challenges include limited network capacity (especially in light of their recent surge in use), device compatibility issues, application security vulnerabilities, and the ever-present risk of credential stealing.

CISA has also encouraged the adoption of multifactor authentication (MFA) in an effort to cut down on phishing and credential-stealing attacks. One promising but currently overlooked possibility would be for companies to adopt Universal 2nd Factor (U2F) authentication policies for their remote workers. The U2F protocol is a stronger version of MFA that relies on a physical key (akin to a USB drive) rather than randomly-generated codes sent to your phone each time you log on. This would cut down on
phishing success rates and be especially convenient for employees, who often need to access company servers many times each day.

The transition to telework and remote learning has led to a massive increase in users of Zoom’s video conferencing application. However, its sudden growth has surfaced a host of security problems, including zero-day privacy vulnerabilities, substandard encryption practices, and data routed through Chinese servers (not to mention the now-notorious practice of zoom-bombing). Industry observers have also discovered sales of compromised Zoom accounts on the dark web, Zoom website spoofing, and the use of malicious email attachments masquerading as Zoom downloaders. As a result, many organizations (the U.S. Senate among them) are curtailing their use of Zoom while the company seeks to address these vulnerabilities. It remains to be seen whether Zoom will be able to fix its issues or whether a more secure alternative will take its place.

Cyber Threats to the Public

The past two months have seen the emergence of phishing and malware attacks that seek to employ coronavirus-related topics such as fake cures, tests, and government alerts in an effort to boost engagement. Hackers have sent phishing emails posing as the WHO and the CDC, loaded malware onto sites that host coronavirus tracking maps, and sent phishing text messages purporting to offer recipients emergency relief payments from the government. Though hackers often use current events to trick their victims, the current pandemic represents an opportunity for hackers on a different order of magnitude.

The impact has not been limited to a greater-than-usual number of annoying spam emails. According to the FTC, U.S. consumers have lost nearly $12 million from coronavirus-related scams as of mid-April. The figure is likely far higher, as the vast majority (likely over ninety percent) of consumer fraud goes unreported. In response, Attorney General Barr has announced that the Department of Justice will prioritize investigating and prosecuting hackers and fraudsters that take advantage of the COVID-19 crisis. And many government bodies—the FTC, FCC, FEMA, and DHS among them—have published resources to combat the spread of misinformation and educate the public on how to avoid falling victim to coronavirus scams.

Nation-State Cyber Threats

Countries have not let the pandemic halt their cyber operations. China-linked social media bots have sought to push back against negative publicity surrounding the virus’s origin, while a Russia-linked disinformation campaign is credited with helping spark coronavirus-related panic in Ukraine.

On the espionage front, a number of state-linked cyberactors have infected victims with malware via coronavirus-themed emails. South Korea, for instance, recently experienced a North Korea-linked phishing attack that used emails titled “Coronavirus Correspondence” as a lure. In addition, the prospect of obtaining other countries’ cutting-edge vaccine or treatment research presents a substantial temptation to any
nation struggling with the outbreak. Though no breaches have been reported yet, the FBI has warned medical research organizations that nation-state hackers have been observed attempting to obtain U.S. medical labs’ vaccine data, and the WHO has reported more than double the usual number of attacks on its own systems, many of which have been traced to Iranian government-backed groups. We can expect more attempted cyberattacks in this area as researchers get closer to discovering effective vaccines, treatments, and cures.

Finally, as the United Kingdom continues its lockdown, the British Army has adopted WhatsApp as an official means to issue orders to soldiers. It’s unknown whether other countries will follow suit, but it’s not hard to see the drastic consequences that credential theft could wreak in this scenario.

Digital Privacy Threats

To combat the virus’s spread, many countries have ramped up surveillance against their citizens. China and Taiwan have installed software on citizens’ smartphones to track their movements and monitor their proximity to the infected. Singapore and South Korea have gone further by publishing details of where infected patients live, work, and have traveled. Both federal and state authorities in the United States have been working with Facebook and other major tech companies to harness user location data to map the virus’s spread. And Apple and Google have announced plans to launch a voluntary app that tracks users through Bluetooth. When a user informs the app that s/he has contracted coronavirus, the app notifies everyone who recently came into proximity of the infected person.

Though these practices have, at least so far, appeared to correlate with results (Taiwan, for instance, has reported only six coronavirus deaths as of May 10), they come with serious privacy concerns. Civil liberties advocates have warned that the rapidity with which these measures have commenced has meant less scrutiny of their invasiveness and potential long-term impact. As the crisis drags on, these emergency surveillance tools may become the new normal, and governments may become unwilling to give them up. Though mitigating the virus’s spread calls for immediate action, it’s essential that these new measures maintain basic privacy safeguards, even if only for pragmatic reasons. For instance, South Korea’s aggressive publication of private data has enabled online harassers to identify and target patients. The United States should take heed and recognize that Americans will be far less likely to download and use a tracking app if they believe their data to be at risk of being used for malicious purposes.

Summing Up

Like all major crises, the coronavirus outbreak has both magnified existing threats (phishing, malware, online disinformation campaigns) and created new ones (virus tracking apps, vaccine espionage, “Zoom-bombing”). A strong response to these new dangers is a small part of the fight against COVID-19, but an important one. Like our approach to the virus itself, we must remain proactive and vigilant in the transformed cyber landscape.
Suggested Background Readings:

- CISA Alert: COVID-19 Exploited by Malicious Cyber Actors
- Protocol: Experts Warn: Pandemic Is ‘Perfect Time’ for Foreign Hackers to Strike
- Wall Street Journal: How Coronavirus Is Eroding Privacy