Center for American Progress

Why Americans Should Care About Russian Hacking

By Michael H. Fuchs, Carolyn Kenney, Anna Perina, and Francesca VanDoorn
February 14, 2017

Russia's interference in the 2016 presidential election was an attack on the American people, threatening the integrity and legitimacy of the democratic process, as well as the outcome of the election. And yet, the Intelligence Community Assessment on Russian activity in the election found that this was but the most recent and aggressive expression to date of a longstanding Russian desire to sow chaos and instability in the United States. Russia's meddling in the 2016 election should be a wake-up call to every American about the diverse ways in which Russian malicious cyberactivity could affect every aspect of their lives.[1]

The so-called information warfare campaign ordered by Russian President Vladimir Putin during the election is part-and-parcel of a longstanding and multi-faceted Russian intelligence strategy that "blends covert intelligence operations—such as cyberactivity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls'" in order to cripple its adversaries.[2] The election is not the first time Russian cyberactors have been successful. Over the past decade, Russian hacking groups—many of which are backed by the government—have successfully deployed a technology-based strategy to infiltrate, tamper with, and steal sensitive information across government, military, banking, and communications systems in the United States and Europe.

The United States remains seriously vulnerable to a range of cybersecurity threats from Russia.[3] If left unchecked, Russian cyberoperations will likely continue to target American institutions, infrastructure, leaders, and citizens. According to former National Security Agency Director Michael S. Rogers, hacking attacks, including those from Russia, are costing the United States "hundreds of billions of dollars" and will lead to "truly significant, almost catastrophic failures if we don't take action."[4]

Every American should be deeply concerned about Russia's attempts to interfere in the 2016 U.S. presidential election, and the potential for Russian actors to interfere with our everyday lives. Below is a sampling of the ways in which Russian groups and individuals are reported to have already attempted to target a variety of U.S. and European institutions, from banking to personal data to government entities.[5]

Banking and finance

Americans rely on banks and financial institutions to protect college savings, retirement accounts, and livelihoods. But U.S. banks and financial institutions have been subjected to numerous attacks by Russian-based hacking groups over the past decade, highlighting key vulnerabilities in the financial security of everyday Americans.

- In May 2015, Russian hackers[6] used malware to target a number of American and international banks, including Bank of America and TD Bank, stealing up to $900 million in one year alone.[7] The full extent to which these malicious Russian programs infiltrated other financial institutions remains unknown.

- The same Russian hackers also reportedly built the largest botnet ever discovered, allowing them to steal login information and password credentials to tens of millions of online accounts, including banking accounts, and costing victims hundreds of millions of dollars.[8]

Personal data

Several hacking schemes have emerged that target personal devices, including phones and computers, in an attempt to obtain sensitive user data and security materials. The examples below illustrate the ways in which Russian hackers exploited programs most Americans use every day in an attempt to gain access to their personal files.

- In February 2015, researchers discovered that Russian hackers[9] had developed iOS malware designed to access users' personal data on devices with iOS7 software, which at the time still operated on a quarter of iOS devices. Apple sold 130 million iOS devices in 2014 alone, meaning it is possible that millions of these devices could still be affected. In addition to being able to start audio recordings in the background without a user's knowledge, the malware can collect a user's text messages, contact lists, pictures, geo-location data, installed app list, process list, and WiFi status. [10]

- In October 2015 and 2016, the same Russian hackers also exploited several zero-day vulnerabilities, or previously unknown software flaws, in Adobe Systems and Microsoft Windows in an attempt to gain access to users' personal data, which it then used to target other individuals.[11] These attacks occurred with the intent of gaining access to and taking control of individual computers remotely.[12]

Government and military

Russian hacking groups have successfully gained access to a variety of government agency and employee servers. In addition to the threats to national security posed by these attacks, the billions of dollars that are spent by the government to recover from attacks and protect information, particularly classified information, comes out of the pockets of U.S. taxpayers.

The examples below illustrate the dangers posed by the Russian hacking campaign:

- In 2015, a ring of Russian hackers[13] targeted computer servers at the U.S. Department of State,[14] the White House,[15] and the joint chiefs of staff.[16] As part of the attacks on the State Department and White House, the hackers gained access to highly sensitive information, including details about President Barack Obama's schedule. Additionally, in the attacks on the email system used by the joint chiefs of staff, the hackers were able to seize control of the system within an hour, allowing them to access the computer credentials of then-Chairman of the Joint Chiefs Martin Dempsey, as well as hundreds of other senior officers.[17] The Pentagon was only able to stop the attack by taking the entire network down. The purpose of the attack was not to spy but to "cause damage and force the Pentagon to replace both hardware and software, which took about two weeks to accomplish."[18]

Political influence

The Russian government has used different forms of cybercampaigning in an attempt to influence not only American elections, but also to provoke instability by creating feelings of fear and mistrust towards American governance institutions. Russian hackers and trolls have successfully used hacking schemes, propaganda, and well-timed information leaks to achieve their agenda, as evidenced below.

Election and post-election hacks

- In the summer of 2015, two Russian hacking groups[19] accessed the Democratic National Committee, or DNC, network and exposed private information sent over DNC servers.[20] The Office of the Director of National Intelligence, or ODNI, has confirmed that it believes these attacks were designed to influence the outcome of the 2016 election.[21] The hackers then leaked sensitive and private information, which was often misconstrued by the public, in an attempt to discredit the DNC and Democratic presidential candidate Hillary Clinton and help then-Republican presidential candidate Donald Trump.

- In March or April of 2016, Russian hackers[22] also hacked the Democratic Congressional Campaign Committee, or DCCC.[23] As a result, Democratic House around the country candidates fell prey to a Russian influence operation after hackers first released lawmakers' personal information and later internal party documents, including candidate evaluations.[24]

- Throughout 2016, Russian hackers, who the Federal Bureau of Investigation, or FBI, believes were working for Russian intelligence, infiltrated state voter registration systems in Illinois, Arizona, and Florida. In Illinois, officials claimed that data on fewer than 90,000 people may have been affected. In Arizona, state officials indicated that the hackers were unable to access data in their systems, though U.S. officials indicated that investigators were working on the assumption that hackers were able to access data. And in Florida, federal investigators also indicated that the personal data of Florida voters may have been exposed. [25]

- Following Donald Trump's electoral success, Russian hackers[26] began targeting individuals associated with liberal think tanks and nongovernmental organizations, or NGOs, in the United States.[27] The security firm Volexity, which investigated the attacks, said that it is likely the attackers were looking for long term access that would give them sensitive information on U.S. policymaking. The Office of the Director of National Intelligence report suggests that national security and foreign policy organizations were the main target, and it argues that the hacking campaign could provide intelligence allowing for future electoral manipulation.[28]

Disinformation campaigns

- In addition to these hacks, the Russian government has been using propaganda groups to target mass media outlets in the United States in an attempt to cause panic and create general feelings of mistrust towards the US government.[29] For instance, prior to and during the election campaign, Russian trolls were likely being paid by the Kremlin to pose as pro-Trump U.S. citizens in an attempt to garner support for the candidate in online forums.[30]

- On September 11, 2014, the U.S. Department of Homeland Security received notice that a chemical plant in Centerville, Louisiana, had exploded.[31] Popular media supported the claim as a YouTube video emerged in which the Islamic State, or IS, took credit for the attack and hundreds of Twitter users spread the news.[32] A fake Facebook account,[33] Louisiana News, reported the story and cited the fake YouTube video as evidence. Authorities quickly discovered the entire event was a hoax, likely playing off of public fear on the anniversary of the September 11, 2001, attacks.

- In December 2014, panic ensued following a fake announcement made on a hacked Yahoo News page that an outbreak of the Ebola virus had occurred in Atlanta and that more than 145 people were infected.[34] The story was supported by a large Twitter campaign and a YouTube video posted showing Centers for Disease Control and Prevention, or CDC, personnel trying to secretly move an Ebola patient. The video was later proven to be faked as well.[35]

International attacks

In addition to some of the attacks on U.S. institutions highlighted here, Russia has carried out many more attacks and influence campaigns around the world, often to devastating effect, as highlighted in the examples below.

- In 2007, following Estonia's decision to remove and relocate a Soviet World War II memorial statue, hackers unleashed a three-week long wave of cyberattacks on Estonia, disabling the websites of government ministries, political parties, newspapers, banks, and businesses.[36] Cybersecurity experts and Estonian officials identified that many of the internet addresses for the attacks were Russian, and some were from Russian state institutions.

- In 2008, in the lead up to and during the Russian land, sea, and air invasion of Georgia, Russian hackers believed to be backed by the Kremlin carried out coordinated attacks on Georgia's internet, including attacks on the president's website as well as communication, finance, and government sites.[37] These attacks effectively blocked communications within the country, preventing citizens from accessing websites for information and instructions as the conflict was underway.[38]

- In 2014, Russia used similar tactics in Ukraine, pairing its invasion of Crimea with cyberassaults on more than 100 government and industrial organizations across Poland and Ukraine, in addition to attacks on the European Commission and Parliament.[39] Since the annexation of Crimea, Russia has continued to launch cyberattacks against Ukraine, targeting military communications, banks, railroads, the mining industry, and the power grid.[40] The cybersecurity firm LookingGlass has dubbed these attacks Operation Armageddon, and have found a correlation between Operation Armageddon attacks and Russian military activity in Ukraine.[41]

Unfortunately, the Europeans have long been the targets of Russian hacking and disinformation campaigns. In addition to the above reports, there is concern that the Russians were spreading disinformation during the recent Brexit vote in the United Kingdom, in addition to working against former Italian Prime Minister Matteo Renzi's government during the recent referendum on the Italian constitution. There are many other examples of the Russians trying to tip politics their way across Europe. What is particularly alarming about these Russian cybertactics is the fact that Russia is "the only country to date to have combined cyberwarfare with assaults by conventional guns and tanks."[42] And, as they have had some measure of success using these tactics, it is not likely that Russia will cease using them anytime soon.

Conclusion

Given the examples provided here of Russian hacking, both in the United States and abroad, it is clear that there needs to be a more thorough approach to understanding, preventing, and responding to cyberattacks across all sectors. The United States and Europe are plainly vulnerable to cyberattacks, and as the world continues to become more reliant upon electronic systems, these vulnerabilities will only grow.

In order to better understand the specific attacks outlined here, there must be a deeper investigation into Russia's cyberabilities, specifically regarding their involvement in the 2016 U.S. presidential election. To better prevent and respond to cyberattacks, U.S. government agencies, as well as other industries such as banking and finance, must develop comprehensive strategies for identifying, preventing, and responding to cyberattacks. It is also important to remember that these attacks are not only against institutions; they are also against ordinary citizens. Even when these attacks directly impact the government, there is a cost to all Americans. Russian hacking is a threat to American democracy and privacy rights. It cannot go unanswered.

Michael H. Fuchs is a Senior Fellow at American Progress. Carolyn Kenney is a Research Associate with the National Security and International Policy team at American Progress. Anna Perina is the Campaign Research Associate for the Center for American Progress Action Fund War Room. Francesca VanDoorn is a policy intern on the National Security and International Policy team at American Progress.

Endnotes

[1] Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (2017), available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[2] Ibid.

[3] Sen. Cory Gardner and Sen. Chris Coons, "Senators: U.S. Cybersecurity is Too Weak," *Time*, January 17, 2017, available at http://time.com/4636236/senators-cybersecurity-russia/.

[4] Owen Matthews, "Russia's Greatest Weapon May Be Its Hackers," *Newsweek*, May 7, 2015, available at http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.

[5] The U.S. domestic hacking attacks detailed in this paper have all been traced back to one of two groups, which have been linked by the FBI and DHS to Russian intelligence agencies. These groups are known variously as APT28/Pawn Storm/Fancy Bear and APT29/Cozy Bear.

[6] APT28/Pawn Storm/Fancy Bear

[7] root9B.com, "APT28 Targets Financial Markets: Root9B Releases Zero Day Hashes" (2015), available at https://www.root9b.com/sites/default/files/whitepapers/R9b_FSO-FACY_0.pdf.

[8] Ibid.

[9] APT28/Pawn Storm/Fancy Bear.

[10] TrendMicro, "Millions of iOS Devices at Risk from 'Operation Pawn Storm' Spyware," February 6, 2015, available at https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/millions-of-ios-devices-at-risk-from-operation-pawn-storm-spyware.

[11] Brooks Li, Feike Hacquebord, and Peter Pi, "New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries," TrendMicro, October 13, 2015, available at http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/; Reuters, "Microsoft says Russia-linked hackers exploiting Windows flaw," CNBC, November 1, 2016, available at http://www.cnbc.com/2016/11/01/microsoft-says-russia-linked-hackers-exploiting-windows-flaw.html.

[12] Dina Bass, "Microsoft Says Hacking Group Targeted Windows, Adobe Flash," *Bloomberg*, November 1, 2016, available at https://www.bloomberg.com/news/articles/2016-11-01/microsoft-says-hacking-group-targeted-windows-adobe-flash.

[13] The cyber security firm CrowdStrike identified this group as APT29/Cozy Bear.

[14] Evan Perez and Shimon Prokupecz, "Sources: State Dept. hack the 'worst ever,'" CNN, March 10, 2015, available at http://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html.

[15] Evan Perez and Shimon Prokupecz, "How the U.S. thinks Russians hacked the White House," CNN, April 8, 2015, available at http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html.

[16] David Martin, "Russian hack almost brought the U.S. military to its knees," CBSNews, December 15, 2016, available at http://www.cbsnews.com/news/russian-hack-almost-brought-the-u-s-military-to-its-knees/.

[17] Ibid.

[18] Ibid.

[19] APT28/Pawn Storm/Fancy Bear and APT29/Cozy Bear.

[20] Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," CrowdStrike, June 15, 2016, available at https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[21] Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.*

[22] APT28/Pawn Storm/Fancy Bear.

[23] Sheera Frenkel, "Meet Fancy Bear: The Russian Group Hacking US Elections," BuzzFeed, October 15, 2016, available at https://www.buzzfeed.com/sheerafrenkel/meet-fancy-bear-the-russian-group-hacking-the-us-election?utm_term=.hjnvBKK9r#.dedrkZZ6Y.

[24] Eric Lipton and Scott Shane, "Democratic House Candidates Were Also Targets of Russian Hacking," *The New York Times*, December 13, 2016, available at https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html?_r=0.

[25] Evan Perez, Shimon Prokupecz, and Wesley Bruer, "Feds believe Russians hacked Florida election-systems vendor," CNN, October 12, 2016, available at http://www.cnn.com/2016/10/12/politics/florida-election-hack/.

[26] APT29/Cozy Bear.

[27] Steven Adair, "PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs," Volexity, November 9, 2016, available at https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/.

[28] Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.*

[29] Adrian Chen, "The Agency," *The New York Times Magazine*, June 2, 2015, available at https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[30] Natasha Bertrand, "It looks like Russia hired internet trolls to pose as pro-Trump Americans," *Business Insider*, July 27, 2016, available at http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7.

[31] Chen, "The Agency."

[32] James Harris, "ISIS Takes Responsibility for the Explosion in Centerville, LA," YouTube, September 11, 2014, available at https://www.youtube.com/watch?v=E2J6RvajSaA.

[33] See Louisiana news available at https://www.facebook.com/louisiana.everyday.news/ (last accessed February 2017).

[34] Jessica Chasmar, "Yahoo News account hacked; tweets Ebola outbreak in Atlanta," *The Washington Times*, August 10, 2014, available at http://www.washingtontimes.com/news/2014/aug/10/yahoo-news-account-hacked-tweets-ebola-outbreak-at/.

[35] See Twitter, "#EbolaInAtlanta," available at https://twitter.com/search?q=%23EbolaInAtlanta (last accessed February 2017); See Jeremy Stone, "Infected with Ebola in Atlanta Airport, 13 December," *YouTube*, December 13, 2014, available at https://www.youtube.com/watch?v=GqsA71C6BDc.

[36] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 16, 2007, available at https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[37] David J. Smith, "Russian Cyber Strategy and the War Against Georgia," Atlantic Council, January 17, 2014, available at http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

38 David M. Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, January 6, 2011, available at http://smallwars-journal.com/jrnl/art/cyberwar-case-study-georgia-2008.

39 Matthews, "Russia's Greatest Weapon May Be Its Hackers."

40 Nolan Peterson, "How Russia's Cyberattacks Have Affected Ukraine," The Daily Signal, December 16, 2016, available at http://dailysignal.com/2016/12/16/how-russias-cyberattacks-have-affected-ukraine/.

41 Jason Lewis, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare," LookingGlass blog, April 28, 2015, available at https://www.lookingglasscyber.com/blog/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/.

42 Matthews, "Russia's Greatest Weapon May Be Its Hackers."