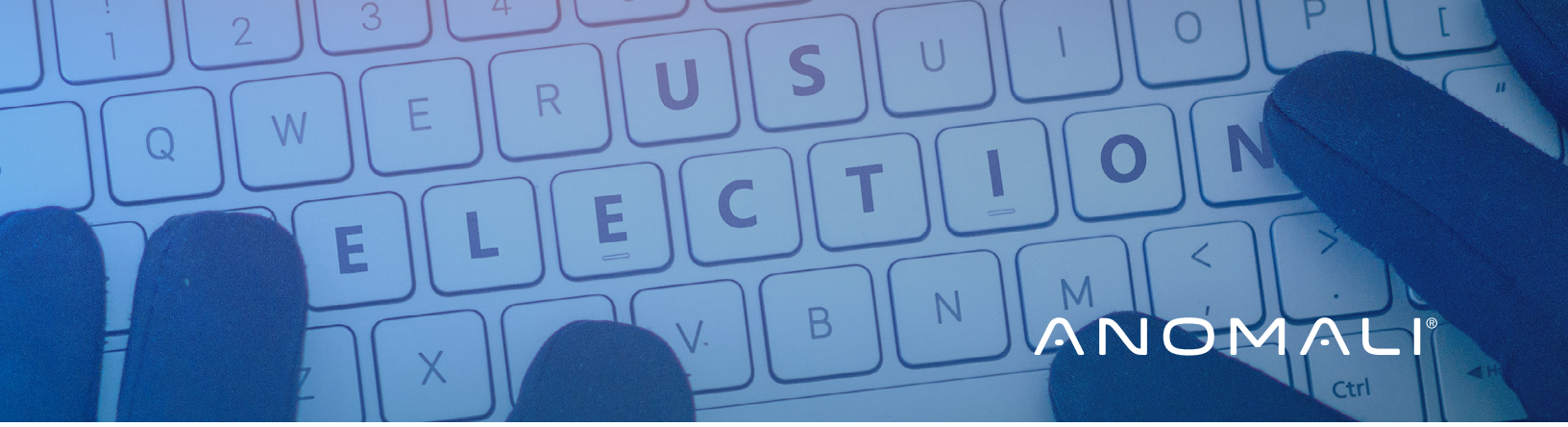

Gage Mele

Threatscape of the US Election

Overview

The cyber attacks targeting political elections is in full swing as the 115th United States midterm elections grow closer. The exploitation of vulnerabilities and direct cyber attacks targeting election-related entities are somewhat expected; however, a different form of cyber attack has the potential to have a disruptive impact to the elections: disinformation campaigns. The use of disinformation tactics in today's social media-obsessed society is the most prominent threat to the democratic process. This form of attack is at a significant and troublesome level that the average voter may not be fully aware of. The presence and overall use of social media on a global scale allows the sharing of information at astounding speeds, and threat actors can take advantage of this data sharing to propagate false narratives and influence the masses. Threat actors distributing such information utilize tidbits of truth, by posting true stories for a period of time (sometimes years) prior to sharing false information to establish credibility while gaining the trust and confidence of readers. This type of attack muddy's the already cloudy political water, causing the political climate to become even more fierce than it already is. Distributing disinformation to incite a sense of indignation, smear a politician who may have a stronger stance against a threat actor's home country, and contribute to a growing sense of disenfranchisement amongst voters participating in the election is one of the most prevalent threats facing this year's midterm election.

In the wake of the 2016 US Presidential elections, the topic of election security entered the consciousness of the mainstream highlighting the importance of free, fair, transparent, and credible elections to the preservation of democratic societies. However, what can arguably be observed as the first large-scale election meddling operation took place in 2014 when Russian-attributed threat actors targeted the Ukrainian Presidential election. This can be viewed as the beginning of election cyber attacks because since that time, it is difficult to go through election cycles around the globe, particularly presidential elections, without hearing or seeing the possibility of Russian and other state-sponsored or threat group activity.

Fast-forward to the US 2018 midterm election, and one would be hard-pressed to avoid seeing security researchers and media outlets discuss threats posed to nation's election infrastructure. A wide range of threat actors pose a risk to the elections from sophisticated, state-sponsored Advanced Persistent Threat (APT) groups, to hacktivist groups, and less-sophisticated threat actors (script kiddies). The potential attack vectors can vary depending on the complexity and skill of the culpable group, however, there are a series of common vectors that will remain constant.

These attack vectors include, but are not limited to:

- Disinformation / smear campaigns
- Distributed Denial-of-Service (DDoS) attacks
- Donation-themed fraudulent websites
- Doxing (public release of Personally Identifiable Information (PII) on the Internet)
- Phishing / spear phishing of political candidates and their staff members

- Targeting of voter databases
- Targeting of voting machines both physical and remote
- Targeting voting machine manufacturers
- Typosquatting (domains that impersonate legitimate websites)
- Website compromise

The objective of this report is to discuss the current state of election risk and the beliefs amongst security researchers regarding the security of the US election infrastructure and the plethora of threats posed to it. Candidates and their associated states and websites will also be examined to ascertain the relative security against malicious activity mentioned above. In addition, various groups who are known to attack election infrastructure or who have the capabilities to do so will also be explored.

Current State / Belief of Election Cyber security

The aftermath of the 2016 US Presidential election left many Americans curious about the state of their election infrastructure. The Russian Advanced Persistent Threat (APT) groups, APT28 and APT29, were widely reported to have gained illicit access to the Democratic National Committee's (DNC) network, and later confirmed by the US Intelligence Community. The internal conversations and documents related to DNC-related individuals was then published by "WikiLeaks," an organization that specializes in releasing secret information on an open-source platform. Snapshots of this once-sensitive information is often distributed on social media, notably Twitter, which demonstrates the rate at how information — true or false — proliferates via social media networks. While this is a severely limited overview, it is with this backdrop, along with current geopolitical relations between the US and Russia, that politicians and government officials enter into the 2018 midterm elections.

A potential response to the cyber-incidents that occurred during the 2016 presidential election took place, on January 6, 2017, when the Secretary US Department of Homeland Security (DHS) at the time, Jeh Johnson, stated that "election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector."[1] With the addition of election infrastructure, there are now 17 critical infrastructure sectors as designated by the DHS.

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Election Infrastructure (Newly Added)
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

This relatively recent change is important to note because some members of the National Association of Secretaries of State (NASS) contend that the designation of election infrastructure as critical infrastructure contradicts a key security element.[2] Specifically, the state and local autonomy over elections creates a decentralized voting process that, in turn, results in a complex voting system that assists in protecting against cyberattacks. In addition, the Election Assistance Commission (EAC), an agency created under President Obama, has come out of a five-year period in which it lacked commissioners to conduct meetings.[3] The EAC wants to focus on states who purchased voting machines in the last decade to

1 Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," Office of the Press Secretary, accessed August 10, 2018, published January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

2 "Who Oversees the Elections Process in the US," National Association of Secretaries of State, accessed August 10, 2018, https://www.nass.org/initiatives/election-cybersecurity

3 Dave Levinthal, "Want honest elections? Meet America's new election integrity watchdog," The Center for Public Integrity, access August 11, 2018, published February 24, 2016, https://www.pri.org/stories/2016-02-24/meet-nations-new-election-integrity-watchman

have the necessary funds to maintain the machines in accordance with current standards.[4] Furthermore, the EAC is also encouraging more states to institute online voter registration; as of December 6, 2017, 37 states plus the District of Columbia offer online registration. This comes as the US government increases its focus on election security at a local level.[5] While online voter registration can increase voter participation, in contrast, it exposes more attack vectors that could be targeted by malicious actors.

US Political Views on Cyber Security

On April 20, 2017, Senator Ron Wyden (D-OR) wrote a letter to the Chairman of the Senate Appropriation Committee, Senator Richard Shelby (R-AL), and a Ranking Member of said Committee, Senator Amy Klobuchar (D-MN) regarding "basic cybersecurity practices."[6] Specifically, Senator Wynden implored the Senate to adopt two-factor authentication that, as he stated in his letter, is a basic security feature. The need for an influential member of the Senate Intelligence Committee to state the importance of a simple security feature that is employed in countless devices and software in the public and private sectors is a cause for concern. Albeit Senate members and staff use a Personal Identity Verification (PIV) card, this is still only a single source of verification.[7] If a malicious actor were to somehow gain the access to the PIV card, or data it holds, they could potentially access sensitive information without a secondary security check in place. This letter regarding the lack of protection was published on open sources, so any threat actor would have access to this information.

On December 18, 2017, House Democrats sent a letter (spearheaded by Ranking Member Robert A. Brady (D - PA)) to Speaker Paul Ryan regarding cyber attacks against the US election infrastructure.[8] In the letter, democrats urged Speaker Ryan to take immediate action to protect America's election infrastructure by requesting the assistance of the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). The representatives cite a report published by the "DEF CON" Conference in regards to the vulnerable condition of states' voting systems and hardware.[9] The letter represented 18 out of 21 states that had their voting systems targeted by Russian threat actors during the 2016 presidential election cycle.

Out of these 21 states, only Illinois confirmed that threat actors had breached its voting systems, however, seven other states are believed by some US officials to have also been compromised by Russian actors.[10] The investigation into the Illinois voter database breach is still ongoing, and the US special counsel headed by Robert Mueller has indicted 12 Russians believed to be responsible.[11] Director of the Illinois State Board of Elections, Steve Sandvoss, stated that "We determined that approximately 76,000 voter records were accessed."[12] The accessed information consisted of: addresses, birthdates, party affiliation, and the last four digits of some voter's social security numbers."[13] According to a report by NBC News, unnamed US officials informed reporters that the US intelligence community acquired evidence that seven states had their websites or voter registration systems breached by Russian actors before the 2016 presidential election.[14] NBC News

4 Dave Levinthal, "Want honest elections? Meet America's new election integrity watchdog," The Center for Public Integrity, https://www.pri.org/stories/2016-02-24/meet-nations-new-election-integrity-watchman
5 ONLINE VOTER REGISTRATION," National Conference of State Legislatures, accessed August 13, 2018, updated September 11, 2018, http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx
6 Senator Ron Wyden, "United States Senate: Washington, DC 20510-3703," US Congress, Senate, accessed August 13, 2018, published April 20, 2017, https://www.wyden.senate.gov/imo/media/doc/Two-Factor%20Authentication%20April%2020,%202017.pdf
7 Ibid.
8 "House Democrats from States Targeted by Russian Hackers call on Speaker Ryan to Take Action," Press Release, accessed August 13, 2018, published December 19, 2017, https://democrats-cha.house.gov/news/press-releases/house-democrats-states-targeted-russian-hacker s-call-speaker-ryan-take-action
9 Ibid.; Matt Blaze et al., "Voting Machine Hacking Village," DEFCON, accessed August 13, 2018, published September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf
10 Geoff Mulvihill and Jake Pearson, "Federal government notifies Illinois, 20 other states of election hacking," Chicago Tribune, accessed August 13, 2018, published September 22, 2017, http://www.chicagotribune.com/news/local/breaking/ct-states-election-hacking-russia-20170922-story.html
11 Cynthia McFadden and Kevin Monahan, "As midterms loom, Illinois toughens its defenses against election hackers," NBC News, accessed September 4, 2018, published September 4, 2018, https://www.nbcnews.com/politics/elections/midterms-loom-illinois-toughens-its-defenses-against-elec tion-hackers-n906351
12 Ibid.
13 Ibid.
14 Cynthia McFadden et al., "US intel: Russia compromised seven states prior to 2016 election," NBC News, accessed September 4, 2018,

was told by intelligence officials that the affected states were Alaska, Arizona, California, Florida, Illinois, Texas, and Wisconsin.[15]

Other states, including Colorado and Iowa, acknowledged reconnaissance activity against their systems via Trevor Timmons, spokesman for Colorado's Secretary of State's office, and Paul Pate (R), Iowa Secretary of State.[16] Politicians have also attempted to get a bill called the "Secure Elections Act" (SEA) passed in December 2017 that proposed to provide assistance and funds to local jurisdictions to defend their voting systems against cyberattacks.[17] The proposers of the bill, Senators James Lankford (R-TX) and Amy Klobuchar (D-MN), stipulated a proponent that desired to weed out the use of electronic voting in favor of post-election audits that would compare the overall vote with paper ballots.[18] However, as the bill was being introduced and discussed, it appeared that this stipulation would be removed and election-integrity groups pulled their support, which caused difficulty in gaining other politicians support for the bill and it was subsequently postponed.[19] The addition of auditory capabilities of election integrity via paper ballots is an odd component for politicians to want to remove because it should only increases voter faith in the electoral process; however, a counter-argument could be made that the stipulation would increase election spending and potentially delay releasing election results.

The current state of cyber security from a political perspective is complex, and there is bipartisan agreement that measures need to be taken to increase security of election infrastructure. One such measure came in the form of a proposed bill titled the "Secure Elections Act" that was introduced on December 21, 2017.[20] However, at the time of this writing the bill has not yet been voted into law. Nevertheless, Congress has taken steps to improve election security by appropriating $380 million in funds to assist in election infrastructure security. On March 23, 2018, President Trump signed into law the "Consolidated Appropriations Act" which, among other provisions, provided funds to assist states in protecting their elections.[21] The Consolidated Appropriations Act designated $380 million in grants to the Help America Vote Act, which was passed by Congress in 2002, for states to improve their election security.[22] The new appropriation of funds grants each state approximately $3 to $34 million dollars depending on the population of the state.[23]

Likely Targets: Who?

Candidates

Perhaps the most apparent target in the upcoming midterm election is the candidate. The most effective way to target a candidate is to target something that holds personal and sensitive information, such as a personal email address, a family member's or significant other's email address, or a campaign website. Thus, one of the most effective methods of compromise, is spear phishing. Actors could also attempt to compromise campaign websites via unpatched vulnerabilities or launch Distributed Denial-of-Service (DDoS) attacks during important moments, such as campaign speeches, fundraising events, or on an election day in attempts to dissuade potential voters.

If common Tactics, Techniques, and Procedure (TTPs)

published Fedbruary 27, 2018, https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296

15 Ibid.

16 Geoff Mulvihill and Jake Pearson, "Federal government notifies Illinois, 20 other states of election hacking," Chicago Tribune, http://www.chicagotribune.com/news/local/breaking/ct-states-election-hacking-russia-20170922-story.html

17 Sue Halpern, "ELECTION-HACKING LESSONS FROM THE 2018 DEF CON HACKERS CONFERENCE," The New Yorker, accessed August 14, 2018, published August 23, 2018, https://www.newyorker.com/news/dispatch/election-hacking-lessons-from-the-2018-def-con-hackers-conference

18 Ibid.

19 Ibid.; Tim Starks "What's next for postponed Secure Elections Act," Politico: Morning Cybersecurity, accessed August 14, 2018, published August 23, 2018, https://www.politico.com/newsletters/morning-cybersecurity/2018/08/23/whats-next-for-postponed-secure-elections-act-325469

20 US Congress, "All Information (Except Text) for S.2261 - Secure Elections Act," 115th Congress, accessed August 24, 2018, published December 21, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/2261/all-info

21 "ELECTION SECURITY: STATE POLICIES," National Conference of State Legislatures, accessed August 16, 2018, published August 16, 2018, http://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx.

22 Ibid,; "HELP AMERICA VOTE ACT," US Election Assistance Commission, accessed August 16, 2018, https://www.eac.gov/about/help-america-vote-act/.

23 "ELECTION SECURITY: STATE POLICIES," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx.

were to be compiled in regards to the most-used amongst actors of all levels of sophistication, from script kiddies (actors who use or purchase available code instead of writing their own) to nation state groups, spear phishing would likely rank among the most-used tactics. Approximately 68 documented threat groups are known to use spear phishing; including some of the most advanced threat groups in the world.[24] The spear phishing objective is simple: impersonate a legitimate person or company and attempt to convince the recipient to open a document with a malicious macro that installs malware on a machine, or redirect recipients to a fake webpage impersonating a legitimate service to steal credentials. Spear phishing tactics consistently evolve, from using new and often legitimate content that would be relevant to the target recipient to entice opening the email, fake or legitimate documents with malicious macros, to software vulnerability exploits, and vulnerabilities inside of the email client itself. Themes of spear phishing and phishing emails can vary depending on who is being targeted, what kind of data is being sought, or if network compromise is the objective.

Two examples of interesting phishing tactics were reported on by security researchers in August 2018. One of which, dubbed *"PhishPoint,"* is believed to affect approximately 10% of all Office 365 users and is used by threat actors to steal Office 365 credentials.[25] *PhishPoint* involves actors distributing emails that attempt to convince the recipient into following a link to a SharePoint file that impersonates a typical OneDrive file. The file presents an "Access Document" button that, if clicked on, leads to a fake login-page for Office 365.[26] This tactic bypasses Microsoft security methods because while Office 365 scans email bodies for malicious or suspicious links, this link leads to an actual SharePoint document that is not malicious, but rather the redirects to the actual phishing page.[27] The second method, observed to be used by the APT group "*Turla*" since 2009, involves controlling a custom backdoor via PDF files distributed through emails.[28] The actors first need to infect a target's machine with the backdoor, which could be accomplished via a typical phishing email, and the target must be using Microsoft Outlook. Once a machine has been infected with the backdoor, *Turla* would send an email with a custom-created PDF file attachment through which the backdoor receives its commands for data-theft by checking the email logs for the specially created PDF files.[29] Furthermore, the backdoor is able to achieve persistence by manipulating the Windows registry and utilizes the "COM object hijacking" tactic so that the backdoor is activated every time Outlook is opened.[30] Overall, there are numerous ways an actor could accomplish malicious activity via email, whether it be stealing credentials or infecting a machine with malware. Communications during elections are commonplace and abound, and much of this communication will take place through email and campaign websites so, from that perspective alone, email is a prime target for threat actors.

Campaign and candidate websites also represent a relatively easy target in the sense that the websites will typically be easy to find. The public availability of such websites can leave them open to DDoS attacks that could be conducted by actors at a nation-state or script kiddy level. DDoS attacks have already been observed in 2018 elections, specifically during a municipal primary in Knox County, Tennessee.[31] This attack targeted an election-results website and subsequently crashed it on election night (May 1, 2018) just as polls were closing.[32] The website was displaying the results of the election as it was struck with a DDoS attack that crashed the site and left it inaccessible for approximately one hour.[33] While

24 "Groups," Mitre Partnership Network, accessed August 14, 2018, https://attack.mitre.org/wiki/Groups
25 Reece Guida, "PhishPoint: New SharePoint Phishing Attack Affects and Estimated 10% of Office 365 Users," Avanan, accessed August 14, 2018, published August 14, 2018, https://www.avanan.com/resources/phishpoint-attack
26 Ibid.
27 Ibid.
28 "Turla: In and out of its unique Outlook backdoor," ESET, accessed August 14, 2018, published August 22, 2018, https://www.welivesecurity.com/2018/08/22/turla-unique-outlook-backdoor/
29 Ibid.
30 Ibid.
31 Lily Hay Newman, "THE MIDTERM ELECTIONS ARE ALREADY UNDER ATTACK," Wired, accessed August 14, 2018, published July 20, 2018, https://www.wired.com/story/midterm-elections-vulnerabilities-phishing-ddos/
32 Alfred Ng, "Cyberattack crashes Tennessee county's website on election night," CNET, accessed August 14, 2018, published May 4, 2018, https://www.cnet.com/news/cyberattack-crashes-tennessee-countys-website-on-election-night/
33 Ibid.

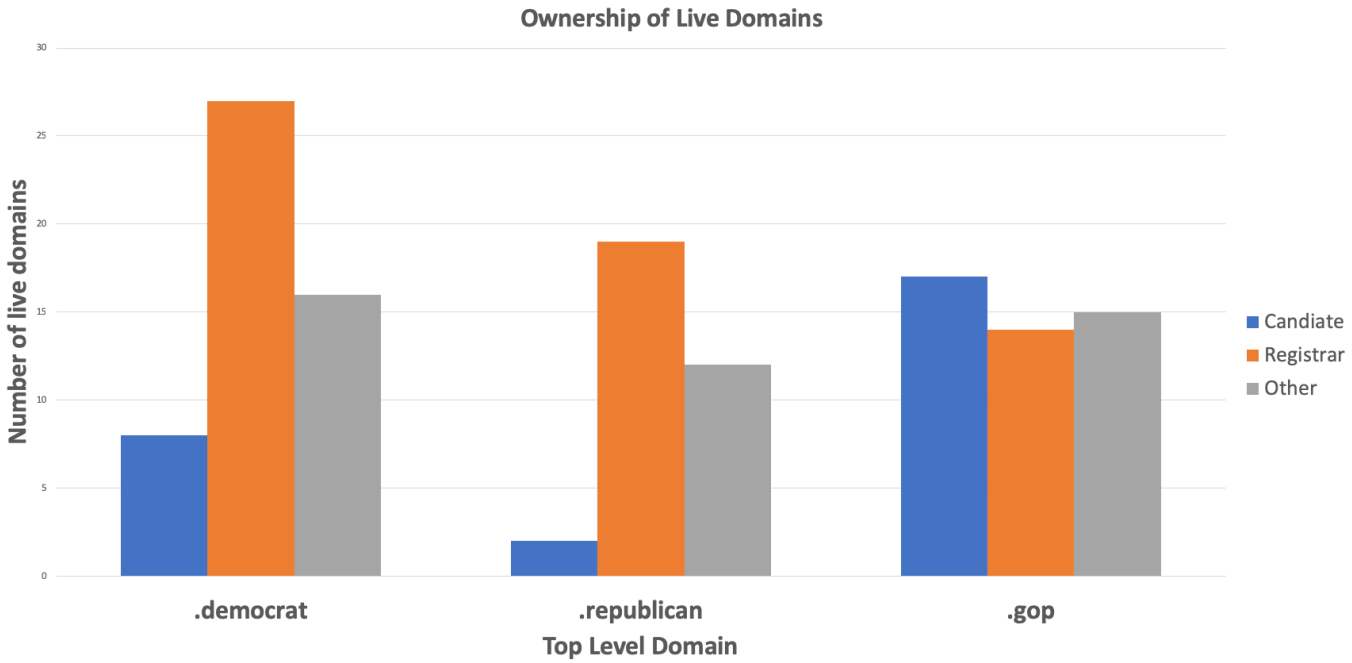

Figure 1: Diagram showing the ownership of live domains

this attack did not affect any vote tallies because the county's voting machines were not internet-facing, it still concerned officials because DDoS mitigation techniques do exist and could have potentially prevented this incident.[34] This type of DDoS attack, that is, timed at a moment that is important to a candidate, has occurred multiple times prior to the midterm election. Anonymous sources associated with Democratic municipal campaigns stated that campaign officials informed them of DDoS attacks that targeted two campaigns. The websites for the two unnamed campaigns were the subject of DDoS attacks at important moments including during an online fundraising event, and a different attack when a candidate was receiving good publicity after a giving a speech.[35] These attacks have not been confirmed nor denied by the DNC or the Democratic Congressional Campaign Committee (DCCC) when they were asked about it, however, the DNC's Chief Technology Officer, Raffi Krikorian, did mention that he was familiar with the attacks.[36]

Voters

Supporters can also be targeted via similar-looking (typosquatted) websites that impersonate a campaign or candidate website. For example, a politically-motivated threat actor could create a look-alike site but with some of the candidate's messaging selectively edited in an attempt to spread disinformation to discourage votes. Another possible attack targeting supporters is the use of typosquatted websites and domain for "donation phishing" scenarios. In this attack, a financially-motivated threat actor creates a donation page that instead sends the money to the threat actor instead of the candidate. The candidates can protect themselves and their voters by registering domains similar to their own campaign website, including those on different Top Level Domains (TLDs). Anomali researchers investigated the TLDs ".democrat," ".republican," and ".gop" because they have political party TLD names. The .gop TLD is owned by the Republican State Leadership Committee but it is free for anyone to register a domain name. The

34 "5 things to know about the cyber attack on Knox Co. election commission," WBIR, accessed August 14, 2018, published May 2, 2018, https://www.wbir.com/article/news/politics/elections/5-things-to-know-about-the-cyber-attack-on-kno x-co-election-commission/51-547980607
35 Chris Bing, "Two Democratic Campaigns hit with DDoS attacks in recent months," CyberScoop, accessed AUgust 14, 2018, published July 9, 2018, https://www.cyberscoop.com/ddos-democratic-campaigns-primary-dnc-dccc/
36 Ibid.

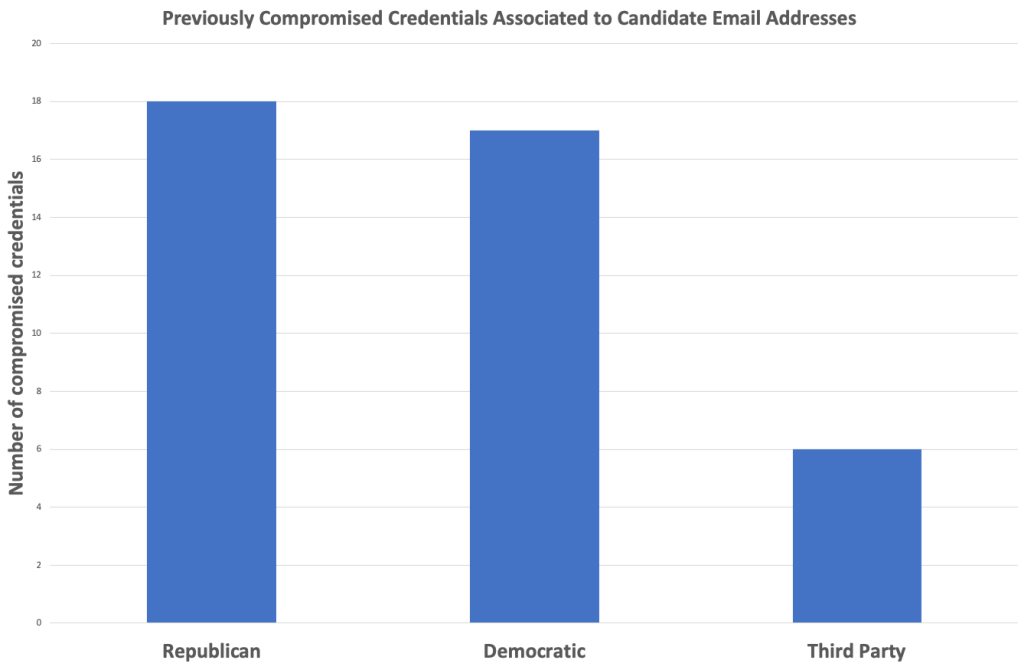

Figure 2: Previously compromised credentials associated to candidate email addresses

.democrat and .republican TLDs are not owned by any of the political parties and are also open for registration to anyone. Of all the domains with these TLDs, 130 domains were found to return an "A record" (address record) and had a candidate or campaign-related domain name. Only 21% of the live domains are owned by candidates or political parties. Most domains are held by registrars, which suggests that they have expired. *Figure 1* is showing a breakdown based on the TLDs.

Out of approximately 3,247 candidates running for seats in both the House and Senate (some candidates are running for multiple positions), Anomali researchers identified emails being used for the candidates' campaigns in 384 instances. Of these 384, 41 candidate emails were found to have been associated with previously compromised accounts, and researchers found credentials associated with the email account. The 41 email addresses broken down into political parties results in 17 Democratic, 16 Republican, and 6 Third-Party candidates. To note, there are possibly other compromised candidate email addresses, those mentioned here were found specifically associated with candidate campaign websites. This data may indicate that third-party candidates have adopted better security practices than their Democrat and Republican counterparts. Additionally, the third-party candidates have embraced stronger email security practices than Democratic and Republican. It could be said however, the lower trend for third-party candidate breaches could be the offset of third-party candidates to Democrat and Republican candidates.

Likely Targets: What?

As midterm elections grow nearer, speculation is abound regarding the state of cyber security of the US election infrastructure. One of the most notable incidents was the controversy of Hillary Clinton's private email server. These occurrences were widely debated on social media, and if one solely relies on social media, or just one media source, for information they would likely be ingesting a biased view of events. The evidence and conclusive agreement amongst the US intelligence community is that the Russian Federation government, mandated by President Putin, interfered in the electoral process with the purpose of undermining Clinton and subsequently assisting Trump in the election.[37] These attacks came in different forms; from compromising high-level Democratic official's email accounts and leaking sensitive information, to breaching the Democratic National Committee's network, to targeting individual state voting systems, and conducting disinformation

37 Karen Yourish and Troy Griggs, "8 US Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture," New York Times, accessed, August 22, 2018, published August 2, 2018, https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html.

campaigns on open sources and social media with an army of bots, amongst others that may not be known to the public. Knowledge of these attacks in combination with historic references and current threat actor TTPs, can assist the American public in not only being aware of how these attacks occur, but also help restore and/or maintain faith in the electoral process whose reputation may have been called into question after the 2016 presidential election.

Voting Systems

By their very nature voting databases, voter registration websites, and voting systems represent lucrative targets from the view of a threat actor. Not only would these systems contain Personally Identifiable Information (PII) but also an individual's political leaning. This information could then be leveraged to show individuals with certain political opinions specifically-catered political information, which could be false or part of smear campaigns, in attempts to steer individuals into voting for a certain candidate. In addition, the mere mention of compromised voter databases has the potential to cause non-party-affiliated individuals to vote for the party not mentioned in disinformation campaigns, or vote for the party who did not have a party-owned voter database compromised. Furthermore, perhaps the most damaging risk posed to these systems is not an actual compromise, whether via physical or remote means, but the undermining of US citizens' faith in the electoral process.

Voter Databases

PII has always been, and will always be valuable to threat actors, whether that value is observed via selling the information on underground forums or using it for other malicious purposes. However, in regards to political elections, the value is not only in the information itself, but the actual breach of systems that hold voter registration details and other forms of PII that can cause mistrust in the election system. For example, if voter databases can be breached, or even configured for public access, what does that mean for the systems that do the actual voting tallies? As of this writing, it does not appear that data leaks have impacted voting behavior, but this could be because malicious activity using leaked voter data has not yet occurred on a significant level.

In late August 2018, DNC officials contacted the US FBI about an attempted cyber attack targeting its voter database.[38] The cyber attack comes approximately two years after APT28 and APT29 successfully gained illicit access to DNC networks, stole information, and gave it to WikiLeaks to publish for the world to see. The attack this year took place in the form a fake website that impersonated the real DNC login page with the objective to steal DNC officials' and employees' credentials, according to an unnamed Democratic official.[39] Interestingly, later on the same day (August 22) open sources reported this phishing attack designed to steal credentials that could be used to access the DNC voter database was actually an unauthorized penetration test conducted by the Michigan Democratic party, according to the DNC's Chief Security Officer, Bob Lord.[40] While this instance turned out to be an unauthorized test, it did, rightfully so, cause a significant reaction by the DNC and the media. This reaction and quick debunking portrays the current state of the interest and importance of election security. The quick response to an "attack" targeting PII is good news for security posture and this stance is likely a reaction to a significant voter data leak that took place in 2017.

In June, 2017, UpGuard's Cyber Risk Team confirmed that they had discovered a misconfigured database that contained PII associated with 198 million registered American voters. The researchers found that the database was owned by Republican party data firm called "Deep Root Analytics" (DRA) who had worked with at least two other similar firms (Data Trust, TargetPoint Consulting, Inc.) in compiling the 1.1 terabytes that resulted in a dataset that covered nearly all of the US's 200 million registered voters.[41]

38 Ellen Nakashima and Craig Timberg, "Democratic National Committee says hackers unsuccessfully targeted voter database," The Washington Post, accessed August 22, 2018, published August 22, 2018, https://www.washingtonpost.com/world/national-security/democratic-national-committee-says-hackers-unsuccessfully-targeted-voter-database/2018/08/22/e9489d60-a62b-11e8-97ce-cc9042272f07_story.html

39 Ibid.

40 Bill Barrow and Colleen Long, "Apparant DNC Voter Hack Attempt Was Unauthorized Test," NBC: Washington, accessed August 23, 2018, published August 22, 2018, https://www.nbcwashington.com/news/politics/DNC-Says-it-Thwarted-Hacking-Attempt-on-its-Voter-Database-491486921.html

41 Dan O'Sullivan, "The RNC Files: Inside the Largest US Voter Data Leak," UpGuard, accessed August 15, 2018, updated May 1, 2018, https://www.upguard.com/breaches/the-rnc-files

Researchers estimate that every three out of five Americans had some sort of data associated to them in this database. Worryingly, this data, whose compiling began in 2012 after Republican Mitt Romney lost to incumbent President Barack Obama, was stored on an Amazon Web Services S3 bucket that had no protection against public access.[42] Any individual who navigated to the Amazon subdomain "dra-dw" would have been able to download the data. [43]

The database contained the following data:

- Date of birth
- Full name
- Home address
- Phone numbers
- Voter registration details

There was also data described as "modeled" voter ethnicities and religions.[44]

The lack of protection on a significant amount of voter data is disconcerting, especially with an increased focus on PII protection, as can be seen with the Global Data Protection Regulation (GDPR) law that went into effect in Europe on May 25, 2018[45]. The concept of the law is to hold companies responsible for protecting European citizens' PII, to levy fines on organizations who do not comply with the specified data protection standards, and require public disclosure if a data breach occurs. It is likely that a similar law is on the horizon for the US as individuals become more aware of how their data is being used and shared by companies and organizations throughout the country.

Voting Security / Voting Machines

Data leaks and breaches pose a high risk to voters' PII being illegally obtained by threat actors. These actors can exploit that information in malicious manners such as identity theft or buying/selling PII to other threat actors. On top of these dangers, voter data breaches can also lead voters to becoming disenfranchised with the sanctity of the democratic electoral system. However, with cyber security conferences like DEF CON holding events like the "Voting Machine Hacking Village," vulnerabilities and exploitation of voting machines are more openly discussed in public sources and in government.[46]

Following the conclusion of the 26th annual DEF CON conference in mid-August 2018, four senators and members of the US Senate Select Committee on Intelligence sent a letter to Election Systems and Software (ES&S), which is the largest voting machine vendor in the US[47] The letter was in regards to the ES&S dismissing the findings of security researchers who took part in the "Voting Village" at DEF CON and discovered multiple vulnerabilities in the company's products.[48] The environments created by the Voting Village officials were replications of 13 Secretary of State websites, many of which were successfully exploited and information within changed. The ES&S does not believe that researchers at DEF CON and their exploitation of their products realistically represents how an actor could act in the wild stating that the "voting village environment does not operate under the same conditions, rules, and regulations as your polling place."[49] To note, the National Association of Secretaries of State (NASS) agrees with ES&S's stance on DEF CON's Voting Village.[50] ES&S's stance on this issue has contributed to a rift between the company and security researchers that results in a lack of open dialogue. Furthermore, ES&S admitted in a letter sent to Senator Ron Wyden (D-OR) that it had sold election-management systems for over six years that had remote-access software installed on them.[51]

42 Ibid.
43 Ibid.
44 Ibid.
45 "2018 reform of EU data protection rules," European Commission, accessed August 16, 2018, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
46 DEF CON, https://www.defcon.org/html/defcon-26/dc-26-villages.html
47 Catalin Cimpanu, "Senators Demand Voting Machine Vendor Explain Why It Dismisses Researchers Prodding Its Devices," Bleeping Computer, accessed August 24, 2018, published August 24, 2018, https://www.bleepingcomputer.com/news/government/senators-demand-voting-machine-vendor-explain-why-it-dismisses-researchers-prodding-its-devices/
48 Ibid.; Sue Halpern, "ELECTION-HACKING LESSONS FROM THE 2018 DEF CON HACKERS CONFERENCE," The New Yorker, https://www.newyorker.com/news/dispatch/election-hacking-lessons-from-the-2018-def-con-hackers-conference.
49 Catalin Cimpanu, "Senators Demand Voting Machine Vendor Explain Why It Dismisses Researchers Prodding Its Devices," Bleeping Computer, https://www.bleepingcomputer.com/news/government/senators-demand-voting-machine-vendor-explain-why-it-dismisses-researchers-prodding-its-devices/
50 Ibid.
51 Kim Zetter, "Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States," Motherboard: Vice, accessed August 18, 2018, published July 17, 2018, https://motherboard.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-

The remote software, called "pcAnywhere," was denied by the company to have been installed on any systems prior to its response to Senator Wyden's letter, after which the ES&S said that it had been installed on some systems sold between 2000 and 2006.[52] Any type of remote access software has the potential to be used for malicious purposes especially if the software is used for legitimate purposes because it will make potentially malicious activity appear authentic. As to whether the pcAnywhere is still in use today, ES&S stated that companies to whom it was sold to "no longer have the application installed." Interestingly, Motherboard reporters state that "[a]s late as 2011 pcAnywhere was still being used on at least one ES&S customer's election-management system in Venango County, Pennsylvania."[53] Even if the remote software is now mostly removed from ES&S systems, the situation has degraded trust in a company responsible for creating a significant amount of the US's election machines. A positive outcome of DEF CON is that the media widely reports on researchers' findings so that the identified vulnerabilities receive plenty of attention even if associated companies choose to disregard them.

Voting security in regards to cyber security has not been so heavily discussed in government and private sectors following the 2014 Russian annexation of Crimea, and this section depicts some examples of what threat actors could potentially target to disrupt and sow doubt in the overall election process. Even the slightest change of a registered voters' information could cause problems. A single character change in an individual's name could cause issues when arriving at the polls, and the same logic could be also applied to address and date-of-birth. While this may not prevent someone from voting, it would likely require voting officials to take additional time to ensure the person is who he/she says they are, which would align with Russia's tactic of generating doubt in the democratic process.

Disinformation

While hardware and software represent visible targets for threat actors during political elections, there is another target: the information people receive from seemingly legitimate news and media outlets.

The National Public Radio (NPR) discovered that the Internet Research Agency (IRA) based in St. Petersburg, Russia, not only created numerous social media accounts to contribute to disinformation campaigns, but also created Twitter accounts that posed as small-town news outlets.[54] The IRA employees are scattered across Russia with the objective to promote pro-Putin content on Russian blogs.[55] Some of the names of these Twitter accounts were found to be *"CamdenCityNews," "@ElPasoTopNews," "MilwaukeeVoice,"* and *"@Seattle_Post."* In one instance in May 2014, the IRA created an account impersonating the Chicago Daily News, a newspaper that closed in 1978.[56] Interestingly, the account never actually distributed false information but instead posted articles of authentic origin for approximately two years and garnered approximately 19,000 followers. The key takeaway from NPR's findings is the significant patience that Russian threat actors engage into achieve their long-term objectives, and in this case two years of building credibility for their Twitter account. This sort of reputation building has the potential to be highly effective because followers may be used to seeing genuine news and, if false stories were to be shared, a user would have no reason to assume it is anything other than authentic. This point was iterated by Representative Adam Schiff (D-CA) who stated that "The Russians are playing a long game. They've developed a presence on social media. They've created these fictitious persons and fictitious organizations that have built up over a period of time a certain trustworthiness among people that follow them."[57] These types of disinformation campaigns, at long last, are being observed and responded to by social media companies.

remote-access-software-on-systems-sold-to-states
52 Ibid.
53 Ibid.
54 Tim Mak, "Russian Influence Campaign Sought To Exploit Americans' Trust In Local News," NPR, accessed August 19, 2018, published July 12, 2018, https://www.npr.org/2018/07/12/628085238/russian-influence-campaign-sought-to-exploit-americanstrust-in-local-news
55 Max Seddon, "Documents Show How Russia's Troll Army Hit America," BuzzFeed News, accessed August 22, 2018, published June 2, 2014, https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america
56 Tim Mak, "Russian Influence Campaign Sought To Exploit Americans' Trust In Local News," NPR, https://www.npr.org/2018/07/12/628085238/russian-influence-campaign-sought-to-exploit-americanstrust-in-local-news
57 Ibid.

On July 31, 2018, Facebook announced that it had discovered and subsequently "removed 32 Pages and accounts from Facebook and Instagram because they were involved in coordinated inauthentic behavior."[58] The threat group(s) behind these social media campaigns is unknown as of this writing, however, Facebook did note that at least one administrator account for one of the pages was known to be associated with the IRA.[59] It is likely that these efforts, as evidenced by Facebook's findings, expanded to other online locations and subsequently the physical locations of the actors also expanded to other countries around the world such as Germany, India, and Thailand.[60] The extensiveness of these disinformation campaigns is only matched by the threat actors' patience in creating and maintaining these individual accounts and personas. These accounts comment on open source publications in attempt to steer conversations into different areas such as negative information regarding a candidate, a proposed bill, or rally-type events that promote political agendas. Media outlets and social media companies are beginning to take steps to mitigate these disinformation campaigns, and earlier in 2018, Reddit banned approximately 1,000 accounts linked to the IRA.[61] The social media bot accounts, also known as trolls, are likely still prevalent throughout the internet and will continue to be so in the foreseeable future. Therefore, it is paramount for individuals to be aware of this style of information warfare, to not rely on information only reported in one source, and to verify information via multiple reputable media outlets.

In response to the large-scale disinformation campaigns, the Democratic Congressional Campaign Committee (DCCC) launched new software designed to identify automated Facebook and Twitter accounts (bots).[62] Specifically, accounts that regularly post about important electoral races that are likely in reference to political seats that could affect Senate and House majorities. The DCCC and its Republican equivalent, the National Republican Congressional Committee (NRCC), are both focused on social media campaigns for conducting campaigning activity and identifying bot-driven disinformation and disinformation efforts.

The prominence of social media to attain news and information is contributing to threat actors utilizing social media as a platform for their own objectives. The persistence of Russian actors in building the legitimacy of their bot accounts will make it difficult for an unsuspecting individual to identify potential disinformation campaigns when the account was previously posting legitimate news for an extended period of time. Social media platforms have begun to take notice, albeit sometimes at the request of government officials or because of negative backlash, and the awareness of this style of attack can contribute to a positive outcome.

Threat actors

The abundance of threat actors/groups known to target political entities can make it difficult to discern which TTPs will be most prominent in cyberattacks targeting election infrastructure. Security researchers have identified that some of the most sophisticated and seemingly well-funded APT groups in the world are interested in targeting political-related entities and individuals. These groups use a variety of TTPs to distribute malware and accomplish their malicious objectives. For example, the "Turla" APT group has used spear phishing with their PDF-controlled backdoor tactic; the Lazarus Group has targeted Managed Service Providers (MSPs); APT28 has created Twitter accounts that share legitimate news (sometimes for years) to then share false information. In addition, the US classified election infrastructure as critical infrastructure in January 2017. Furthermore, some well-documented groups are known to target political, government entities, and critical infrastructure. These groups include the following:

58 "Removing Bad Actors on Facebook," Facebook: Newsroom, accessed August 22, 2018, published July 21, 2018, https://newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/

59 Nicholas Fandos and Kevin Roose, "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts," The New York Times, accessed August 22, published July 31, 2018, https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html

60 Max Seddon, "Documents Show How Russia's Troll Army Hit America," BuzzFeed News, https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america

61 Zeeshan Aleem, "Reddit just shut down nearly 1,000 Russian troll accounts," Vox, accessed August 20, 2018, published April 11, 2018, https://www.vox.com/world/2018/4/11/17224294/reddit-russia-internet-research-agency

62 Michael Scherer, "Democrats seek stronger social media presence to guard against potential Russian interference in midterms," The Washington Post, accessed August 23, 2018, published August 11, 2018, https://www.washingtonpost.com/politics/democrats-seek-stronger-social-media-presence-to-guard-against-potential-russian-interference-in-midterms/2018/08/10/7345fcd4-972b-11e8-80e1-00e8-0e1fdf43_story.html

Group	Aliases	Country of Origin
APT19	Deep Panda, Group 13, KungFu Kittens, PinkPanther, Shell Crew, Sh3llCr3w, SportsFans, Web Shell	China
APT28	Fancy Bear, Pawn Storm, Sofacy, Sednit, Strontium, Threat Group-4127, Tsar Team	Russia, Main Intelligence Directorate (GRU)
APT29	Cozy Bear, Cozy Duke, Mini Duke, The Dukes	Russia
Dragonfly	Crouching Yeti, Energetic Bear, Koala Team	Russia
Dragonfly 2.0	Berserk Bear	Russia
Lazarus Group	Dark Seoul, Dubnium, Guardians of Peace, Hidden Cobra, KimSucky, New Romanic Cyber Team, Whois Hacking Team	North Korea, Reconnaissance General Bureau, Bureau 121
Turla	Krypton, Snake, Venomous Bear, Waterbug, WhiteBear, Wipot	Russia

An overview of these threat groups can be found in Appendix A.

Conclusion

The 2018 US election is a complex cyber security landscape. Threat actors have a multitude of vectors that could be utilized for malicious purposes. Whether that be targeting a candidate (or relative or friend) directly with attempted phishing attacks, or attempting to compromise a candidate's home network to sniff out sensitive data. Typosquatting attacks impersonating a candidate's legitimate website is also a concern because the fake website could be used to spread disinformation, steal donation funds, or distribute malware. The voter him/herself is also at risk due to the significant data breaches that affected nearly all registered voters in June 2017, and the Equifax breach that exposed approximately 143 million Americans social security numbers in September 2017. The leak of PII causes the likelihood of identity theft to increase substantially as well as contributing to a lack of trust amongst voters who see their data being mishandled in drastic ways. This lack of trust can then be compounded by threat actors using armies of bots on social media platforms and the internet as a whole to spread disinformation. Whether that fake information be in the form of a candidate's policy on a certain issue, or the data being used in fraudulent voting activity. At the time of this writing, no purposeful or fraudulent voting occurrences have been reported in the US which may indicate that security measures in place to protect the voting process are effective, however, the trust of voters in companies who store voter registration data, or who are counting the ballots, could be affected via disinformation campaigns. Disinformation, in the shape of typosquatting or bot activity, is the most prevalent threat posed to this year's midterm election. Individuals and candidates alike must be vigilant and take the extra steps to validate information through multiple sources to discern if what is being reported is factual. The fact that some social media platforms, particularly Facebook and Reddit, have taken steps to ban accounts associated with threat actors and disinformation exemplifies the reality of this threat. However, with state-sponsored actors engaging in this tactic, social media platforms will be hard-pressed to keep up with the sheer amount of bot accounts as well as the resilience and patience actors utilize to accomplish their goals. It is the responsibility of the individual to be cognizant of this ongoing threat and take the necessary actions to ascertain what is false, what is factual, and what is intentionally misleading.

Appendix A

APT19

Deep Panda is a Chinese Advanced Persistent Threat (APT) group that is composed of freelancers that have sponsorship from the Chinese Government. The group appears to work closely with other groups such as "Axiom" and "Black Vine." Similarities between the tactics and malware used by Axiom and Deep Panda have led many security firms to hypothesize that they are the same group. Deep Panda conducts cyber espionage campaigns targeting governmental organizations, mostly in the United States. Deep Panda highly target companies in the following industries: defense, healthcare, financial, legal, and telecommunications. In particular, they have targeted senior individuals, in the United States, that are involved in geopolitical policy issues in the China/Asia Pacific Region.

Known Tactics and Techniques:

- Accessibility Features
- Cron Job/Scheduled Tasks
- Indicator Removal from Tools
- Object Linking and Embedding
- PowerShell
- Process Discovery
- Process Injection
- Regsvr32
- Scripting
- Spear phishing
- Web Shell
- Windows Admin Shares
- Windows Management Instrumentation

APT28

APT28 has been attributed to multiple campaigns and instances of malicious activity and, similar to other APT groups, APT28 primarily uses spear phishing emails to distribute malware. What separates APT28 from other groups, however, is their sophistication in their phishing content, custom malware, platforms, and tools, as well as a network of phishing websites. Additionally, the group also compromises target organization's websites to display fake information.

Spear phishing campaigns are sometimes conducted on a large-scale in regards to distribution, while others are more selective. For example, APT28 was found to have sent a significant amount of spear phishing emails to the then US presidential candidate Hillary Clinton's campaign staff. This resulted in the group compromising the email account of Clinton's campaign chairman, John Podesta. Former US Secretary of State, Colin Powell, also had his email compromised; the email conversations of said individuals, among others, was found to have later been published to the "DC Leaks" website. This indicates that the group is in favor of not only conducting cyber espionage on its targets, but also releasing potentially damaging information.

The group's objective during spear phishing campaigns is not only to trick the users into downloading their custom malware or downloaders, but also to steal user credentials. One such example of this activity can be observed in the Trend Micro's report on the APT28 campaign "Operation Pawn Storm." The group used geopolitical-themed spear phishing emails that were distributed to US defense contractors, as well as an unnamed national security department of a US ally, in addition to international media organizations, embassies, and militaries around the globe.

Known Tactics and Techniques:

- Bootkit
- Communication Through Removable Media
- Connection Proxy
- Credential Dumping
- Data from Local System
- Data from Removable Media
- Deobfuscate/Decode Files or Information
- Dynamic Data Exchange (DDE) Exploitation
- File Deletion
- Logon Scripts
- Malicious Macro
- Multi-stage malware VPNFilter technical breakdown
- Network Sniffing
- Office Application Startup

- Peripheral Device Discovery
- Process Injection
- Replication Through Removable Media
- Rundll32
- Screen Capture
- Spear Phishing
- Spear Phishing Attachment
- Standard Application Layer Protocol
- System Information Discovery
- System Owner/User Discovery
- Timestop

APT29

APT29 is a highly sophisticated group that employs a variety of tactics to accomplish their malicious objectives. Similar to other APT groups, APT29's primary initial infection is spear phishing; APT29 will also wrap its malware with legitimate applications for distribution. These spear phishing emails are crafted with information gathered from legitimate locations that would be relevant to the target recipient. For example, the group was found to use news articles and paste the content into Word document attachments with malicious macros. Enabling of the macro begins the infection process for one of numerous APT29 malwares; typically the first infection is a backdoor, such as HammerToss, or a toolset, such as CosmicDuke. APT29 backdoors often have the ability to download a secondary backdoor, such as POSHSPY, that is used as insurance to continue to have access to an infected machine if a first-stage backdoor, such as PowerDuke, is discovered.

The spear phishing campaigns can be broad, targeting organizations in various industries, or highly targeted using geopolitical themes to entice targets into opening malicious attachments, or following provided links. The links lead to ZIP files that contain a Microsoft shortcut file (.LNK) that, if followed, will launch PowerShell commands that check to see if a virtual machine is being used, followed by dropping the PowerDuke backdoor, and lastly launching a new clean decoy document.

Known Tactics and Techniques:

- Accessibility Features
- Bypass User Account Control
- Configuration/Environment Manipulation
- Domain Fronting
- Exploitation for Client Execution
- Identity Spoofing
- Indicator Removal on Host
- Malicious Macro
- Multi-hop Proxy
- Pass the Hash
- PowerShell
- Registry Run Keys / Start Folder
- Remote Access Trojan
- Scheduled Task
- Scheduled Task
- Scripting
- Social Engineering
- Software Packing
- Spear Phishing
- Spear Phishing Attachment
- Spear Phishing Link
- Spear Phishing Link
- User Execution
- Windows Management Instrumentation
- Windows Management Instrumentation Event Subscription

Dragonfly

The Advanced Persistent Threat (APT) group "Energetic Bear" are a Russian APT group that targets Western industries in cyber espionage campaigns. The group is believed to be sponsored by the Russian government as they are very well resourced, highly skilled, and have a large range of tools at their disposal. Energetic Bear appears to have been in operation since 2011. The cyber espionage campaign is primarily conducted by using multiple infection vectors to upload trojans and backdoors onto a victim's system. They have been observed heavily targeting the energy sector post-2013.

Energetic Bear will send emails, from a Gmail account that has the subject lines "The Account" or "Settlement of Delivery Problem, containing malicious XML Data Package (XDP) file attachments. An XDP file allows

a Portable Document File (PDF) file to be packaged within an Extensible Markup Language (XML) container. This aided in obfuscation and serves as an additional layer of anti-detection. The file contains a Small Web Format (SWF) exploit, and stored in the PDF file are two files obfuscated with XOR. One file is the Havex Loader DLL and the other is a JAR file which copies and runs the DLL. When the SWF exploit is initiated, it drops a new SWF file which in turn is used to run the PDF/SWF exploit (CVE-2011-0611) to execute shellcode.

Known Tactics and Techniques:

- Brute Force
- Cloned Software/Installers
- Commonly Used Port
- Create Account
- Credential Dumping
- Disabling Security Tools
- Email Collection
- Exploit Kit
- External Remote Services
- File Deletion
- Forced Authentication
- Indicator Removal on Host
- Masquerading
- Network Share Discovery
- PowerShell
- Remote Desktop Protocol
- Remote File Copy
- Scheduled Task
- Screen Capture
- Scripting
- Spear Phishing
- Web Shell

Dragonfly 2.0

The Advanced Persistent Threat (APT) group, "Berserk Bear," is believed to be a Russian-based group that has been active since 2004. The group's primary objective is to steal sensitive information pertaining to diplomacy, international law, non-profit organization, and domestic threats related to political dissent and terrorism. The targets align very closely with the collection priority of the Russian intelligence services. The group has also been observed to provide support in Russia's offensive operations, most notably in the August 2008 Russia/Georgia conflict. According to CrowdStrike, the group has some technical and operational overlaps with other Russian APT groups such as Energetic Bear, Team Bear, and Voodoo Bear.

In the September 2017 phishing campaign found to be associated to Berserk Bear. This activity was attributed to Energetic Bear by Symantec, however, CrowdStrike disputed this and instead attributed the campaign to Berserk Bear. Email themes and subjects commonly focus on control systems or process control systems. The body of the email will use references to industrial control equipment and protocols. Some emails contained attachments for legitimate resumes for industrial control systems personnel, invitations and policy documents, which would entice a target to open the attachment. The threat group has been observed using a Microsoft Office attachment in their phishing emails that used a "Template Injection" technique. The template injection is used to leverage legitimate Office functions that attempt to retrieve a document from a rouge file server of the actor using Server Message Block (SMB) protocol. The request authenticates a client with the server, sending the user's credential hash to the C2. The actor would then brute force the credentials to obtain access to the victim's network as an authenticated user.

Known Tactics and Techniques:

- Cron Job/Schedules Tasks
- Microsoft Office Open XML Template Injection
- PowerShell
- Spear Phishing
- Watering Hole

Lazarus Group

The most common initial vector for Lazarus Group is spear phishing emails. Lazarus Group will use decoy documents that are likely of interest to the intended document. Commonly these decoy documents have political themes such as media reports discussing South Korean parliamentary elections, or information about government conferences. These documents have either exploited macros. In other cases Lazarus Group have been noted to exploit vulnerabilities in the

indigenous Korean Hangul Word Processor (한/글), using ".hwp" decoy documents, which is a popular attack vector as 80% of the documents attached to South Korean and public agencies websites are HWP files.

Once Lazarus Group has gained access to a system they will often deploy a Remote Access Trojan (RAT) as well as a wiper component. Lazarus try to pivot and infect as many systems they can within a target network. They have been observed to use Server Message Block (SMB) worming components to propagate through a network. The worm uses a brute force authentication attack to propagate through Windows SMB shares. If it successfully infects another system, it will send log data to its Command and Control (C2) server.

They have been known to use multiple types of persistence for their malwares. In the case of malware targeting South Korean financial institutions, the malware "Castov" created a copy of itself in "%System%" creates registry entries. Lazarus Group have also injected malicious code into DLL files that enable the malware to run on Windows startup.

Known Tactics and Techniques:

- Application Window Discovery
- Bootkit
- Brute Force
- Code Injection
- Custom Cryptographic Protocol
- Data from Local System
- Denial of Service
- Disabling Security Tools
- Disk Wiping
- Exploit Kit
- Malicious Macro
- Modification of Regsitry Keys
- New Service
- Process Injection
- Process Injection
- Reflective DLL Injection
- Remote Access Trojan
- Spear Phishing
- Standard Application Layer Protocol
- System Information Discovery
- System Owner/User Discovery
- Timestop
- Uses RC4 Encryption
- Windows Management Instrumentation

Turla

The Advanced Persistent Threat (APT) group "Turla" is believed to be a Russian based group that has been active since at least 2007. Turla conducts cyber espionage against government entities around the world. The group is connected to the "Epic" cyber espionage campaign that targets government agencies around the globe, and is also connected to the Agent.btz worm that infected the network of the US Department of Justice in 2008.

In April 2016, Kaspersky Lab researchers hypothesized that one of the first documented APT groups called "Moonlight Maze" is connected to Turla. In April 2017, the researchers provided further evidence to substantiate their claim. Additionally, Kaspersky researchers discovered that the Penguin Turla backdoor is based on the open-source LOKI2 backdoor, a favorite tool of the Moonlight Maze group.

Known Tactics and Techniques:

- File and Directory Discovery
- Hijacking a privileged process
- Indicator Removal from Tools
- Process Discovery
- Process Injection
- Query Registry
- Remote Access Trojan
- Remote System Discovery
- Spear Phishing
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Service Discovery
- System Time Discovery
- Uses Compromised Websites
- Uses RC4 Encryption
- Watering Hole
- Windows Admin Shares