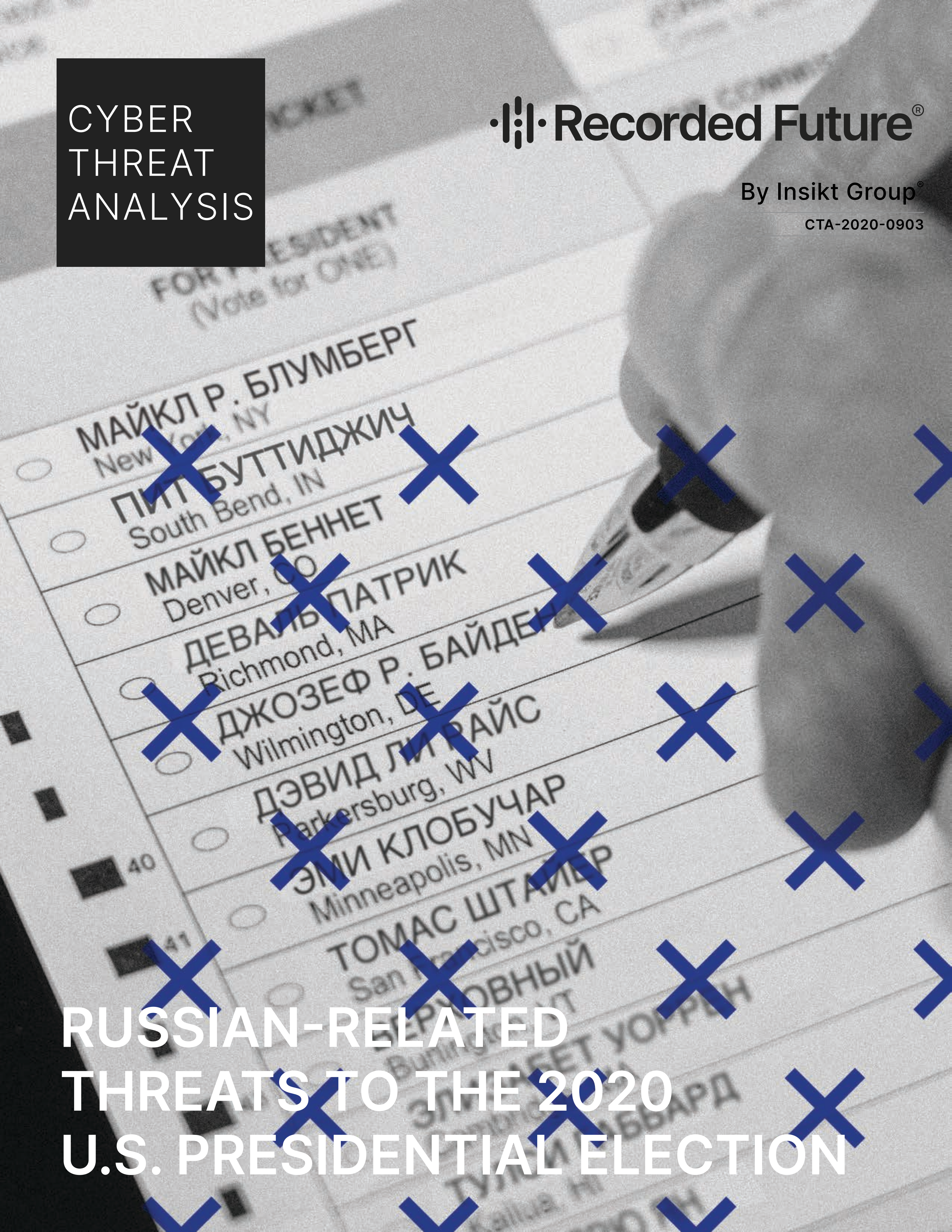
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-0903



RUSSIAN-RELATED THREATS TO THE 2020 U.S. PRESIDENTIAL ELECTION

CYBER THREAT ANALYSIS

In this report, Recorded Future provides an overview of Russia-nexus cyberespionage and influence operations activity related to the 2020 U.S. elections, including from advanced persistent threat (APT) groups, information operations (IO) entities, as well as likely front entities and non-state groups aimed at presidential candidates, political parties, elections infrastructure, media platforms, voting efforts, and the U.S. population at large. Assessments provided in this report are based on content in the Recorded Future Platform® and data from social media sites, local and regional news sites, academic studies, information security reporting, and other open sources available between January 1, 2020 and August 25, 2020. We compared this to historical data to determine changes in tactics, techniques, and procedures (TTPs) to reveal cyber threats, information operations (IO), and hybrid threats that incorporate aspects of both cyber and IO actions.

Executive Summary

The threat landscape of the upcoming election differs from 2016 and 2018; threat actors and activity groups who previously targeted elections have largely remained on the sidelines. Consistent with 2016 and 2018, however, is that Russia continues to pose the greatest threat to the 2020 U.S. presidential elections, based on past success in conducting phishing and cyberattack operations, a relentless persistence in directly targeting U.S. democratic institutions and organizations, and the conducting of information operations targeting the U.S. electorate via conventional and social media.

Contemporary Russian-directed information operations against the United States have been ongoing since at least 2016, with activity becoming more distributed internationally. Additionally, Russian threat activity groups continue to expand infrastructure and develop malware and exploits, but have been less active in targeting elections-related entities. Despite the lack of observable Russian state-sponsored hack-and-leak operations since January 2020, we cannot rule out the possibility of a leak appearing before the November election, given how damaging such activities were in advance of the 2016 vote. Russian threat actors and activity groups likely will continue to conduct cyberattacks and pursue information operations against the U.S. electorate up to, and even after, election day.

Unattributed threats to the election also remain a significant concern, the most salient of these being burgeoning conspiracy theories and their adherents in the form of the QAnon and Boogaloo movements. Additionally, non-attributable activity from cybercriminal or other elements possess capabilities to disrupt or harm the U.S. election and warrant constant vigilance on dark web and underground sources.

Key Judgments

- Russian advanced persistent threat groups likely pose the greatest threat to the 2020 U.S. presidential election, despite a lack of identified activity against these targets to date; this assessment is based on past efforts against the 2016 and 2018 U.S. elections as well as identified retooling, development, and ongoing activity by U.S. and U.K. intelligence agencies.
- Information operations likely continue to play a major role in disrupting the U.S. domestic social and political environments ahead of the election; ongoing research initiatives from Stanford Cyber Policy Center, Graphika, and others have described how these efforts have evolved since 2016 and indicated how such operations continue to target elections internationally to disseminate deceptive information.
- Although no election-related hack-and-leak operations linked to Russian threat actors have been identified to date, it remains likely that such content could appear in advance of the election; there is historical precedent for entities like APT28 to distribute such data in a delayed manner.
- Ransomware likely poses an additional threat to elections-related infrastructure; carefully timed ransomware attacks within key battleground states have the potential to cause some limitations but are deemed unlikely to fully disrupt the 2020 election.
- Non-state groups also likely pose an information operations, influence, or protest threat to the elections; although not directly linked to Russian threat actors, Russian overt and covert influence operations have taken an interest in these groups and are amplifying their content and could potentially hijack or leverage these groups to conduct disruptive activities.
- The U.S.'s defensive posture and response to real or perceived cyber operations can present challenges for any would-be attackers, but is unlikely to completely deter any determined threat group.

Russia-Sponsored Elections Interference Efforts: 2016 and 2018

In 2016 and in 2018, Russian state-sponsored threat actors conducted an unprecedented campaign against the United States presidential and midterm elections, targeting political parties, candidates, and infrastructure associated with the vote. A U.S. government investigation into the intrusions, information operations (IO), and other corresponding activities, conducted by Robert Mueller III, revealed that the effort was primarily led by entities associated with the Main Intelligence Directorate (GRU, also called the Main Directorate [GU]) with support from organizations like the Information Research Agency (IRA). The Russian Main Directorate/Main Intelligence Directorate of the General Staff of the Armed Forces is the primary military intelligence entity within the Russian Federation. This organization conducts strategic and tactical foreign intelligence tasks for the Russian government. It is composed of subunits, several of which are engaged in cryptography, signals intelligence, disinformation, and intrusion activity. The IRA is a commercial media entity that has specifically been engaged in social media influence operations.

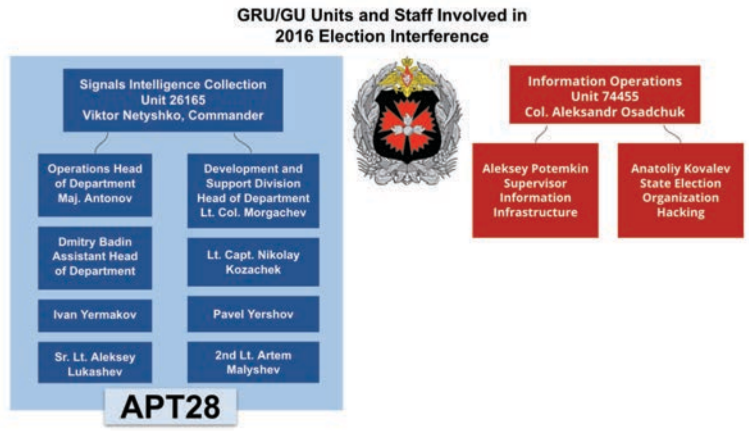
Threat Actors

Ahead of the 2016 U.S. presidential election, three Russian state-sponsored advanced persistent threat (APT) groups were involved in targeted intrusion activity; some of these threat actors also acted as "hybrid threats," due to their involvement in information operations as well as targeted intrusions. The primary threat actors were identified as APT28, APT29, and the Main Intelligence Directorate/Main Directorate (GRU/GU) Unit 74455, which is tracked as Sandworm.

APT28 and APT29 were engaged in targeted intrusions against the DNC, DCCC and other elections-related individuals and organizations. Additionally, personnel from GRU/GU Unit 26165 were identified in a Department of Justice (DoJ) indictment in association with both the APT28 activity, as well as engaging in separate, information operations efforts. Personnel from GRU/GU Unit 74455 — the organization associated with Sandworm activity — was also indicted by the DoJ for their role in elections interference efforts (such as hack-and-leak operations); however, none of the custom malware attributed to Sandworm was identified on networks impacted by the intrusions. For that reason, efforts to interfere with the 2016 election conducted by this organization are identified by unit name (Unit 74455) as opposed to threat activity group designator (Sandworm).

Several other Russian groups have been linked to election interference activities:

- On January 25, 2018, the Dutch Intelligence Agency (AIVD) publicly shared information identifying APT29 operators engaged in intrusions against the Democratic National Convention (DNC) and connecting it to the Russian Foreign Intelligence Services (SVR). The SVR is responsible for foreign espionage, active measures, conducting electronic surveillance in foreign nations, and more.
- Also in 2018, Estonian Intelligence Services released reporting that APT29 operations were associated with both the SVR and the Russian Federal Security Service (FSB).
- According to a Department of Justice indictment, two GRU/GU military units associated with APT28 and Sandworm — Unit 26165 and Unit 74455, respectively — used false front actors DCLeaks, Guccifer 2.0, and AnPoland, as well as employed Wikileaks, to launder exfiltrated data and to claim responsibility for intrusions against targeted resources.
- Finally, Russian-based troll farms — most notably the Internet Research Agency (IRA) — conducted mass dissemination of disinformation or inflammatory material in order to destabilize the U.S. domestic social environment ahead of the election, working as a force multiplier for other operations conducted by APT28, Sandworm, and APT29.



Organizational chart of GRU/GU units involved in 2016 election interference (Source: Ars Technica)

In 2018, some of these same threat activity groups and influence operations targeted the U.S. midterm elections. APT28 conducted spearphishing operations aimed at three candidates running for legislative office. Although it is unclear if these efforts were successful, Microsoft released information identifying the likely targets of this activity as the U.S. Senate, a political think tank, and a political non-profit. The DoJ also brought a criminal complaint against Russian influence operations entities for "...advertisements on social media platforms, registration of domain names, the purchase of proxy servers, and "promoting news postings on social networks," among other things. The U.S. reportedly took action to deter the latter by targeting the St. Petersburg-based IRA, taking them temporarily offline. Although some of their operations were purportedly disrupted, Russian efforts to target American democratic processes remained largely undeterred and, even at that time, it was apparent that the Russian state-sponsored threat actors were adapting their strategy.

Tactics, Techniques, and Procedures (TTPs)

Some of the main TTPs conducted by these threat groups in both the 2016 and 2018 elections can be broken down as follows:

APT28 Unit 26165	**Unit 74455**	**APT29** SVR/FSB	**Hybrid Threats** DCLeaks, Guccifer 2.0, AnPoland, and Wikileaks	**Influence Operations** St. Petersburg IRA
- Spearphishing - Use of typosquat domains to facilitate spearphishing operations - Use of URL shorteners in spearphishing - Targeted intrusions with bespoke tools - Use of encrypted tunnels for data exfiltration	- Purchase of domains with Bitcoin (BTC) - Establishment and use of personas (like DCLeaks and Guccifer 2.0) to launder information or claim responsibility (Hack and Leak operations) - Searched for state political party email addresses - Conducted intrusions against software vendors used to verify voter registration information	- Targeted intrusions with customized tooling for each target - Spearphishing campaigns against American political think-tanks and non-government organizations (NGOs) - Employed eFax links or documents pertaining to the election's outcome being revised or rigged in attacks - Maintained persistence on infected hosts to exfiltrate data	- Employed by Unit 74455 and Unit 26165 - Established actor controlled domains to release information - Posted information on social media claiming responsibility for activity - Reached out to journalists to conduct interviews - Released information obtained from intrusions via their own channels - Reached out to and exchanged information with an individual (Roger Stone) close to Donald Trump	- Distributed polarizing content on social media - Disseminated false data on social media - Incited protests between opposing groups in the U.S. - Employed multiple sock puppet accounts to amplify the impact of data distributed by hybrid threat actors

Victimology

These groups targeted a wide range of U.S. democratic institutions. In the 2016 presidential election, threat actors targeted political parties, candidates and campaign staff, elections contractors (such as VR Systems), states' boards of elections, voter registration data, charitable foundations, and think tanks, and the American populace as a whole. In the 2018 midterm election, the scope of the targeting was largely narrowed to candidates and campaign staff and Americans on social media. A narrowing of the target scope may have been the result of limitations to threat actor operations due to increasing security around vulnerable elections infrastructure, a byproduct of the midterm elections being viewed as less consequential to the threat actor, or the result of a lack of necessity (i.e. it may not be necessary to conduct intrusions into infrastructure hosting voter registration data frequently as that information does not change drastically in short spans of time).

Threat Actor Activity Since January 2020

Since January 2020, several Russian APT groups have been active against U.S.-based entities not related to the elections, as well as international entities with a potential nexus to the election. Although Recorded Future has not identified any direct intrusion activity by threat activity groups against U.S. elections infrastructure, candidates, political parties, or voting efforts as of this writing in advance of the 2020 presidential election, that does not preclude such efforts from materializing. Recorded Future has found that, in this same time frame, Russian APT groups have been developing malware which could potentially be used to target elections-related entities. Furthermore, Recorded Future identified infrastructure development, evolving TTPs, and changes to malware during this same time frame.

Although it is very likely that Russian threat actors have improved their operations, these threat groups have also continued to use some of the same approaches to intrusions that they have historically applied. Therefore, changes to operations and shifts in behavior are likely not indicative of a wholesale abandonment of previous tools, but rather an example of both flexibility in adapting operations when necessary and pragmatism in ensuring the mission is completed successfully.

Activity Targeting the Candidates and Political Parties

It is likely that threat actors maintain an ongoing interest in the candidates, their affiliates, and the U.S. political parties more broadly because of their role in the campaign or their relationships with those involved in the election. This assessment is based, in part, on a report which indicates that the Russian government is attempting to interfere in the 2020 U.S. presidential election. The reporting did not elaborate on what interference efforts would entail; however, Recorded Future searched for any Russian state-sponsored threat actor activity aimed at incumbent President Donald Trump, his family, or high-profile individuals associated with the campaign since January 2020, but found no references to any such efforts as of this writing. Open-source searches likewise did not yield any relevant content. We also searched for any activity attributed to Russian state-sponsored threat actors aimed at former Vice President Joe Biden, Senator Kamala Harris, the Biden family, the Harris family, or other high-profile individuals associated with the campaign since January 2020. There were no indicators of intrusion activity against these individuals.

Since January 2020, there have been no indications of Russian APTs targeting the Republican National Committee (RNC), National Republican Congressional Committee (NRCC), or the National Republican Senatorial Committee (NRSC). Similar research into Russian APT groups' targeting of the DNC or the Democratic National Convention Committee (DNCC) identified a total of 20 instances — all to historical items; none were indicative of any present or imminent threat aimed at the DNC or DCCC. Although these searches do not appear to reveal any ongoing or imminent threat against the political parties, as of this writing, it also does not preclude such efforts from the list of potential threats either. These references may be summarized generally as follows:

- Two results were references in social media to historical reporting associated with the 2016 intrusion into the DNC.
- At least six of these references were found in forum posts focused on disputing the assessments and findings of the intelligence community and information security industry in attributing the 2016 U.S. presidential election interference operations to Russian APT groups.
- One local news website also disputed the intelligence community findings.
- 10 references were to news websites or court documents associated with the reporting of Russian APT activity against the 2016 U.S. presidential election.
- One item that referenced this activity has since been removed from social media.

Threat Actors

APT28

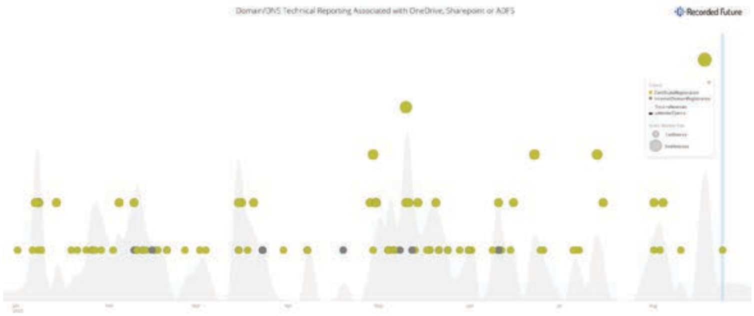
Since January 2020, APT28 has engaged in a number of activities, such as infrastructure development, attempted spearphishing, and malware development. Of these, only spearphishing has a potential nexus to the election, specifically an alleged phishing attack against Burisma Holdings.

Attempted Spearphishing Activity

On January 13, 2020, cybersecurity firm Area 1 released a report titled "Phishing Burisma Holdings," which outlined spearphishing attempts they attribute to the GRU/GU against Burisma Holdings, an energy company in Kiev, Ukraine. According to the report, the campaign, active since at least November 2019, employed domains which mimicked those used by legitimate partners or subsidiaries linked to Burisma Holdings. Burisma Holdings is of particular interest, as Joe Biden's son Hunter Biden previously served on the board of Burisma Holdings. A simultaneous effort unrelated to the phishing attempt, as reported in the Washington Post, detailed multiple attempts by current U.S. administration affiliates to solicit information regarding audio recordings of Biden in relation to former Ukrainian president Petro Poroshenko. This activity included the solicitation of information from Andriy Derkach, a Ukrainian parliament member with ties to Russian-sympathetic groups. Some of this audio has already been leaked, and is discussed in further detail in the "Purported Audio Leaks" section.

One of the TTPs described in the Area 1 report includes the use of websites which mirror genuine login pages across multiple attack surfaces (for example, mimicking a Roundcube installation and Outlook 365 logins via Sharepoint) in an effort to obtain credentials for the targeted entities. This TTP aligns with previous methodologies employed by APT28 during the 2018 U.S. midterm election as well as the 2016 U.S. presidential election. In the course of the campaign, the threat actor leveraged various email-related authentication technologies to establish legitimacy. In particular, the threat actor used Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) (cryptographic hash), both of which are used by a recipient to verify the identity of a sender. In doing so, the threat actor registered their SPF with a yandex[.]net Mail Exchange (MX) record, suggesting this action was conducted by a Russian-based threat actor.

APT28 has previously conducted "hack and leak" type operations, targeting entities to obtain sensitive information which is later dumped in an effort to harm either the targeted entity or affiliated organizations and individuals. These have included efforts against the campaign of former Secretary of State Hillary Clinton during the 2016 U.S. presidential election, in addition to organizations associated with international sports during the 2016 Olympics. Given its involvement in these campaigns and the nexus between Burisma Holdings and the U.S. and Ukrainian political climates, chances are about even that this threat activity group is conducting this campaign in an effort to obtain information for later distribution as part of an information operation.



Screenshot of Sharepoint, ADFS, OneDrive domain and certificate registrations (Source: Recorded Future)

Malware Development — Drovorub

A joint report released by the Federal Bureau of Investigation (FBI) and National Security Agency (NSA) on August 13, 2020, details a new Linux-based malware framework, which the threat actor called Drovorub. Industry experts, however, have hypothesized that an alternate understanding for the name may be obtained from the slang term for device drivers (дрова), reflecting the tool's targeting of the kernel. The report is more lengthy and in-depth than other similar NSA publications. The NSA characterized the toolset as part of military Unit 26165 cyberespionage operations and determined that the framework employed the following MITRE ATT&CK Techniques:

MITRE ATT&CK ID	Tactic	Enterprise	Sub-Technique
T1071.001	Command And Control	Application Layer Protocol	Web Protocols
T1041	Exfiltration	Exfiltration Over C2 Channel	No sub-techniques
T1059.004	Execution	Command and Scripting Interpreter	T1059
T1090	Command And Control	Proxy	T1090.001, T1090.002, T1090.003, T1090.004
T1014	Defense Evasion	Rootkit	No sub-techniques

An August 13, 2020 Reuters article noted that Linux-based systems are widely used among, "National Security Systems, the Department of Defense, and the Defense Industrial Base" and the recently announced multi-purpose malware poses a significant threat to U.S. domestic systems, if those resources are not adequately protected.

Sandworm

Since January 2020, Sandworm has engaged in vulnerability exploitation but without clearly identified links to specific targets. In particular, Sandworm's exploitation of a vulnerable version of the Exim Mail Transfer Agent (MTA) poses a serious threat to users with unpatched versions of this software, including elections-related entities and organizations. Sandworm, (affiliated with GRU Unit 74455) has conducted ongoing and aggressive cyber operations primarily against Ukraine but has also engaged in broader espionage, election interference, and disruptive operations that have impacted entities in Europe as well as the U.S. On February 20, 2020, the U.S. State Department announced that Unit 74455 was also responsible for disruptive attacks conducted on October 28, 2019 against the nation of Georgia.

Vulnerability Exploitation

In late May 2020, the NSA released an advisory detailing the exploitation of CVE-2019-10149 (The Return of the WIZard) by Sandworm.

CVE-2019-10149 pertains to a vulnerability in the Unix- and Linux-based Exim MTA version 4.92 and below, and how it handles inbound emails. Once the vulnerability is successfully exploited, a bash script provided by the threat actor runs a series of commands. It begins by adding a secure shell (SSH) key on a victim's machine, enabling remote access to the targeted mail server, and creates users, disables/manipulates the firewall, and manipulates the SSH service, among other tasks.

A review of the bash script attributed to Sandworm found that in several key areas, the script uses simplistic coding techniques, and sends out scattershot commands to restart services which would reside on different Linux distributions. This script takes a rather unsophisticated approach, especially with regards to the "flat" (lack of function definitions, minimal conditional statements) way in which the script is written, and the lack of conditional statements to check for various Linux/Unix distributions when restarting the firewall (ufw versus firewalld) or restarting the SSH daemon (ssh versus sshd). Employing the syntax in this fashion could allow an administrator to determine, via error codes and logging, whether an attacker had attempted to run, for example, a SysV Init daemon restart command on a systemd enabled operating system, or vice versa. The NSA advisory lists the indicators of compromise (IoC) for detecting a successful exploit of the Exim MTA. These indicators are included in Appendix A.

APT29

Although not directly tied to current targeting against elections-related entities, APT29's use of novel tool sets against COVID-19 research-related targets highlights the capabilities of this threat activity group and willingness to target U.S.-based entities. This threat activity group, which has historically targeted U.S. elections and was a prominent figure in the 2016 elections, has the ability to conduct operations against protected resources, a prior knowledge and ability of targeting election-related resources, and could pose a real threat to such entities in 2020.

Use of Novel Tool Sets

On July 16, 2020, Canada's Communications Security Establishment (CSE), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S.'s NSA issued a joint statement stating that APT29 was targeting institutions conducting COVID-19 vaccine-related research with previously unattributed malware.

The reporting indicated that, through 2020, APT29 had been employing a previously unattributed backdoor called WellMess, a first-stage downloader called SOREFANG, several VPN vulnerabilities — CVE-2019-19781, CVE-2019-11510, CVE-2018-13379, and CVE-2019-9670 — as well as a lightweight framework called WellMail to target unidentified organizations engaged in vaccine research.

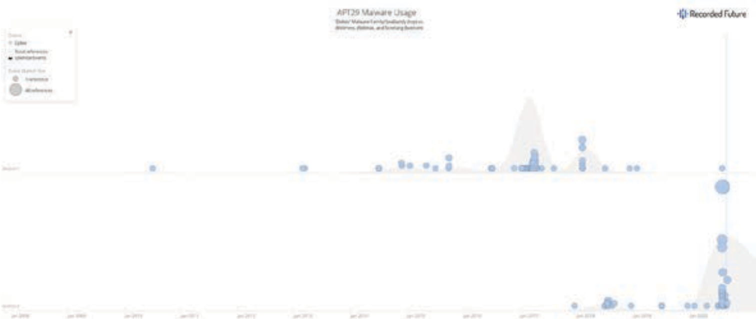


Figure N: APT29 decreasing use of highly identifiable malware sets to newer tooling (Source: Recorded Future)

According to the NCSC report, Wellmail is "written in either Golang or .NET," and has an ELF variant, allowing it to target Windows and Linux systems; it was first observed in 2018, targeting organizations in Japan. Instead of building new tools, APT29 appears to have focused on fine-tuning aspects of the existing malware, adding C2 functionality to the Golang iteration.

It is equally unusual for APT29 to reuse a tool in a different targeting set, shifting from an obvious Asia-Pacific (APAC) focus against government entities to targeting research organizations in the West. APT29 put extensive effort into improving the code in this campaign for encrypting and encoding the data in multiple layers before transit. The campaign's infrastructure was also devolved compared to previous campaigns. APT29 previously made extensive use of compromised domains, and used tricks including domain fronting, encoded data on social media websites, or heavily compartmentalized and obfuscated C2 networks. In contrast, the WellMess campaign used straightforward infrastructure, with each malware sample pointing directly to one or more IP addresses. The IP addresses used were easily linked to one another because they all used the same SSL certificate serial number, an operational security error reminiscent of APT28's XTunnel infrastructure sharing a certificate.

There are some overlaps in TTPs between this activity and prior APT29 efforts, like the use of OpenSSL, which is employed by Wellmail and FatDuke. Similarly PWC found that the command and control server use of base64 encoded HTTP requests and encrypted cookies to transfer data was similar to SeaDuke; however, there were no distinct, technical overlaps in the tooling to suggest that this activity would be uniquely attributable to APT29. Similarly the other TTPs associated with this activity (spearphishing, vulnerability use, and so on) are not unique to APT29 and cannot be used solely to attribute this activity to that threat activity group. Attribution for this activity was obtained from the joint CSE, NCSC, and NSA report, which likely made their determination using information derived from a variety of intelligence sources.

Potential Hybrid Threats

The Russian hybrid threats from 2016 have thus far been largely inactive in 2020. Of the four known threat actors used by Russian APT groups to leak information, claim responsibility, or amplify disinformation — DCLeaks, Guccifer 2.0, AnPoland, and Wikileaks — only Wikileaks remains active. The websites for DCLeaks and Guccifer 2.0 are still up, but there has been no active content posted to the websites since November 1, 2016 and January 12, 2017, respectively. Additionally, the social media account for AnPoland (@anpoland) has been suspended. Wikileaks has continued to post to its social media account, @wikileaks, and periodically provides updates to its website, wikileaks[.]org. The decreasing activity from the existing front groups may be the result of a shifting dynamic with Russian threat actors and activity groups moving away from a reliance on entities which they directly control (such as Guccifer 2.0 and @anpoland) and can be tied back to them, towards groups that are more loosely affiliated.

Wikileaks

On August 11, 2020, Wikileaks released what it claims to be "documents on newly announced Vice Presidential Running Mate Kamala Harris." This largely consisted of 137 results dated between December 2013 through November 2016; 53 of the results were contained within a folder named "The Podesta Emails," which is likely a reference to email data which APT28 obtained during intrusions into the email account of John Podesta. Given that Wikileaks is still active, is still employing data that was obtained via targeted intrusions conducted by Russian APT groups, and is taking aim at current political candidates for office, we believe Wikileaks remains an ongoing threat.

Purported Audio Leaks

The Washington Post reported in May and July, 2020, that the domain nabu-leaks[.]com had posted likely edited, leaked audio, which purported to contain conversations between Joe Biden and former President of Ukraine Petro Poroshenko. The Washington Post indicated the audio recordings likely originated from Andriy Derkach — the same pro-Russia Ukrainian parliamentarian referenced in relation to the Burisma Holdings targeting. The Washington Post also suggested that there was additional material which had not yet been released and that more material will likely come to light closer to the election. To date, no seriously compromising material has been posted and the two leaked audio files this year appear to be heavily edited, calling into question their veracity.

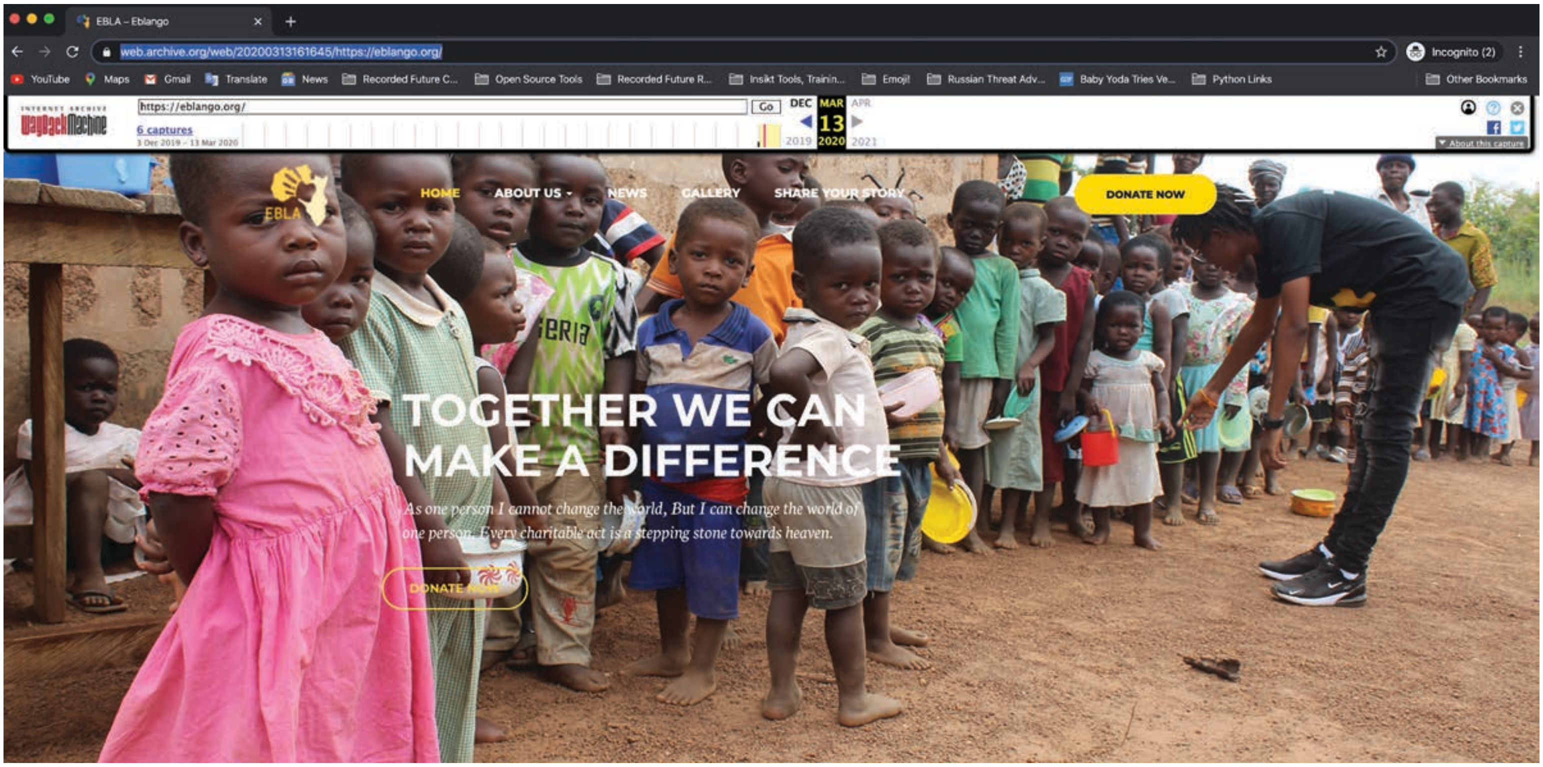
Even though no documents or other information has been released attributed to these attacks at the time of writing, Recorded Future believes that it is likely that if such compromising information exists, the attackers will wait until the most opportune and damaging moment to release any documents or information obtained from the attacks. For example, in 2016, Russian threat actors released emails stolen from intrusions conducted against John Podesta in late October likely for greatest impact ahead of the election. Even in the event that such information does not exist, it is likely that Russian-based influence operations threat actors could fabricate it — on April 8, 2020 Recorded Future detailed covert activity believed to originate from Russia in which forged documents were distributed via online forums with the likely intent of shaping perceptions.

Influence Operations

Russian influence operations observed since the beginning of 2020 focus on many of the same issues as in 2016 and 2018, but the established logistical framework is much different. In late 2019 and early 2020, Russia-backed "troll operations" were partially outsourced to Africa, and it is likely that there are other operations elsewhere which have gone unnoticed. These efforts likely indicate an expanded approach to disinformation operations, leveraging partnerships very likely established by the Russian government, which would assist in obfuscating influence operations by delegating activity to extranational citizens.

CNN and Graphika reported on the discovery and takedown of a group called "Eliminating Barriers to the Liberation of Africa" (EBLA), a purported NGO in Ghana with a nexus to Nigeria.

The CNN investigation found that accounts associated with the group "focused almost exclusively on racial issues in the U.S., promoting black empowerment and often displaying anger towards white Americans." EBLA operatives generally did not create original content, but rather used existing content from elsewhere online, such as popular memes and copied and pasted content from known historic IRA influence material.



web.archive.org/web/20200313161645/https://eblango.org/

https://eblango.org/

TOGETHER WE CAN MAKE A DIFFERENCE

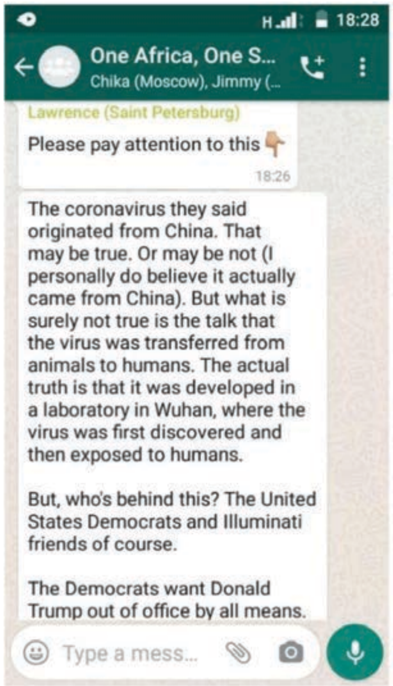
As one person I cannot change the world, But I can change the world of one person. Every charitable act is a stepping stone towards heaven.

Screenshot of the online presence for EBLA (Source: Internet Archive)

EBLA content closely aligned to social issues that were, and most likely continue to be, the focus of Russian influence operations; these included racial justice issues and police brutality, per the CNN reporting. At the time of discovery, these accounts were observed engaging in audience building, using, resharing, and creating (though rare) content used to go viral. This content included "focusing on topics like black history, black excellence and fashion, celebrity gossip, news and events related to famous Americans like historical figures and celebrities, and LGBTQ issues." Facebook further stated that this activity rarely focused on elections for/against political candidates. Much of the involved activity shared content about "oppression and injustice, including police brutality."

At the time of discovery, the EBLA was found looking to recruit a Charleston, South Carolina-based "Chapter Coordinator" via LinkedIn and low-tier job board websites, such as helpwanted[.]com. Recruitment of U.S. citizens to operate on behalf of covert Russian threat actors has been, and is likely to continue to be, a keystone tactic used by covert operatives. Recorded Future cannot rule out the possibility of U.S. citizens being unwittingly recruited to participate in protests and forms of domestic unrest via unsuspecting mediums with a nexus to Russian individuals or organizations. It is likely that individuals or groups engaging in domestic unrest or other forms of physical political organizing have adjusted their tactics from 2016 to a more layered and complex connection between Russian handlers and American citizens, unwittingly manipulated as a means of disassociating any connection back to Russia as much as possible. To our knowledge, EBLA was dismantled in February 2020, but it remains likely that restructured organizations took its place in the following months.

Reporting from the Daily Beast determined that Russian influence operations also leverage WhatsApp to spread disinformation. Exchange students from Nigeria studying in St. Petersburg and Moscow, likely on Russian government scholarships, posted messages to a WhatsApp group called "One Africa, One Success." Although the accounts distributing the messages had described themselves as having links to Africa or African interests, they often focused on issues pertaining to the U.S. Sample posts provided by the Daily Beast included content that suggested COVID-19 was developed by "Democrats" or Microsoft founder, Bill Gates. An August 2020 U.S. Department of State report referenced a similar example of a Russia-linked media platform distributing disinformation surrounding Bill Gates and COVID-19 research.



Lawrence (Saint Petersburg)

Please pay attention to this 👇

18:26

The coronavirus they said originated from China. That may be true. Or may be not (I personally do believe it actually came from China). But what is surely not true is the talk that the virus was transferred from animals to humans. The actual truth is that it was developed in a laboratory in Wuhan, where the virus was first discovered and then exposed to humans.

But, who's behind this? The United States Democrats and Illuminati friends of course.

The Democrats want Donald Trump out of office by all means.

'One Africa, One Success' WhatsApp screenshot (Source: The Daily Beast)

Comparative Analysis: Past and Present Activity

A comparative analysis of past Russian APT group activity behavior and current activity reveals an evolving approach to operations, and suggests that if any targeting of the 2020 elections is to occur, it would likely not look the same as it did in 2016 or 2018. To date, there has been no direct indication of Russian APT activity against political parties, candidates and campaign staff, elections contractors, states' boards of elections, voter registration data, or charitable foundations and think tanks.

Nevertheless, there has been activity with a nexus to the elections. The previously mentioned APT28 spearphishing efforts targeting Burisma Holdings could potentially play a role in leak operations similar to the successful targeting of Hillary Clinton's campaign in 2016. Additionally, the Exim vulnerability exploited by Sandworm could be used to target vulnerable elections-related entities.

Since January 2020, Russian threat activity groups appear to have shifted their attention to other targets, electing to engage in credential harvesting operations at the San Francisco Airport and attempting to conduct intrusions against organizations engaging in COVID-19 research. These threat activity groups have also very likely been engaged in infrastructure and malware development.

This shift may indicate that Russian threat actors or activity groups are biding their time and waiting to conduct activity closer to the election, in an attempt to disrupt the vote by having maximum impact releasing information as close to election day as possible. There is precedent to suggest that Russian threat activity groups may conduct operations or leak documents closer to election, as APT28 has been noted to "let time pass before leaking stolen documents" and the New York Times reported that, "Weeks before the election, about 60,000 hacked emails from the account of John D. Podesta, Hillary Clinton's campaign manager, were released, in small amounts, spread over many days."

Hybrid threats, or the use of identified front groups by Russian threat actors or activity groups to claim responsibility, amplify disinformation, or leak documents, has not yet been observed in relation to the 2020 U.S. presidential election. It is likely that Russian threat actors or activity groups may have determined that the risks associated with the use of such entities outweighs the rewards. On July 13, 2018, Special Counsel Robert Mueller identified the DCLeaks and Guccifer 2.0 personas to be controlled by GRU/GU Unit 74455, effectively allowing the U.S. government the ability to tie election interference efforts to the Russian government. It is likely that the Russian government would like to avoid further claims of involvement in elections meddling; therefore, should they elect to employ any such front groups, it will likely be a part of a broader organization whose actions cannot be tied directly back to their intelligence services.

Information operations are very likely an indispensable part of the Russian government strategy both in relation to elections as well as more broadly. Such operations are relatively low cost, difficult to attribute, and disruptive to the environments they target. Russian information operations have been ongoing since the 2016 U.S. presidential election and have shifted away from a centralized operation within the IRA in St. Petersburg, Russia to more distributed operations across the globe. This shift in TTPs is exemplified by the aforementioned operation of Russian troll farms, operating under the auspices of an NGO in Ghana and Nigeria, and the use of African exchange students in Russia to conduct influence activity on WhatsApp.

Non-Attributed Activity or Threats to the Election

In addition to researching explicitly Russia-linked APT or influence operations activity, we have also observed a variety of more general threats aimed at the candidates and their associates, political parties, campaign staff, elections contractors, states' boards of elections, voter registration data, charitable foundations and think tanks, and the American populace as a whole.

While we cannot, at this time, attribute these activities to a particular nation, threat actor, or threat activity group, Russia has a history of exploiting online campaign infrastructure as well as ostensibly organic social movements and societal divisions to further its interests. Potential threats include the presence of personally identifiable information (PII) on dark web sources, which could enable social engineering or fraudulent activity. Additionally, potentially harmful domain registrations and typosquats can enable spearphishing campaigns or redirects that create confusion or disruption. A threat actor or threat activity group could employ ransomware attacks against election infrastructure. Finally, threat actors and threat activity groups can infiltrate and amplify the influence and voice of non-state groups.

Credential Leaks

The Candidates and the Campaigns

It is likely that as the November 2020 presidential election nears, the campaign will face increased phishing and spearphishing attempts, as well as potential leaks of credentials and PII as they relate to campaign staffers, the candidates, and other third-party contractors related to the campaign. Third-party contractors are a particularly attractive target to threat activity groupsors, as they present a springboard from which to gain access to campaign infrastructure without raising initial alarm within the campaign itself. Via an extensive search of the dark web and underground forums, paste sites, and open sources since January 2020, Recorded Future analysts did not identify leaked credentials pertaining to the Biden campaign through its email domain, "@joebiden[.]com," or variants of that email, at the time of writing. Even though we did not uncover any leaked credentials at this time.

Similar research since January 2020 for leaked credentials or mentions of dumps of credentials pertaining to President Trump's campaign likewise found no evidence of leaked credentials related to the campaign using the "@donaldjtrump[.]com" (or variations of this) domain. A June 2, 2020 Pastebin post claimed to have been leaked by the online collective "Anonymous," and contained the email addresses (without associated passwords) of several organizations related to the Trump campaign, the Trump Organization, and the White House. The paste shows five email addresses pertaining to @donaldjtrump[.]com; approximately 133 email addresses pertaining to the Trump Organization, including subdomains of @plaza.trump[.]com, @ca.trump[.]com, @taj.trump[.]com, @marina.trump[.]com; and approximately 1,193 email addresses ending in @whitehouse[.]gov. Recorded Future analysts have not been able to independently verify that these email addresses are in fact from the organizations they claim to represent; however, some of the addresses, such as hussein-obama-undeniable-confirms-that-he-is-no-muslim@whitehouse[.]gov suggest that at least a subset are illegitimate. Even though these were posted without a password and likely already public, this easily parsable and accessible list could enable a threat actor or activity group to more easily spearphish individuals operating the accounts in question.

The Democratic and Republican National Committees

Because the DNC was a direct target of Russian military intelligence, in the form of a nation-state threat activity group, as well as the fact that the U.S. intelligence community has stated Russia's preference for President Trump to defeat Joe Biden in the November 2020 election, the DNC likely remains a target for nation-state cyberespionage, hack-and-leak operations, as well as destructive malware. Like the DNC, we believe the RNC to be a likely target of future hack-and-leak operations.

Despite the highly publicized Russia-backed attacks against the DNC during the 2016 election season, we have not observed leaked credentials or dumps pertaining to the DNC since January 2020. However, multiple GitHub repositories were discovered containing references to individuals' emails within the DNC, many of which appear to be anti-phishing training datasets and could still be used for targeting individuals. Additionally,we identified 20 DNC-related credentials from an exposed MongoDB database belonging to Verifications[.]io exposed and unencrypted records, including PII and email addresses. The early 2019 Collection #1 data dump contained eight email address/password combinations pertaining to the DNC. Approximately 100 DNC email addresses appeared in the 2016 Dropbox credential leak, forming the majority of leaked DNC credentials.

In addition to the 2016 attacks on the DNC, reports suggest that the RNC was successfully targeted by Russian state-sponsored threat activity group, who chose not to release damaging information gathered ahead of the election. Queries for activities targeting the RNC since January 2020 uncovered approximately 18 email addresses of the @gop[.]com domain, which appeared in the aforementioned Verifications[.]io dump. The RNC was a direct target of Russian state-sponsored activity in the 2016 elections, even though they declined to release potentially damaging stolen information.

Domain Registrations and Redirects

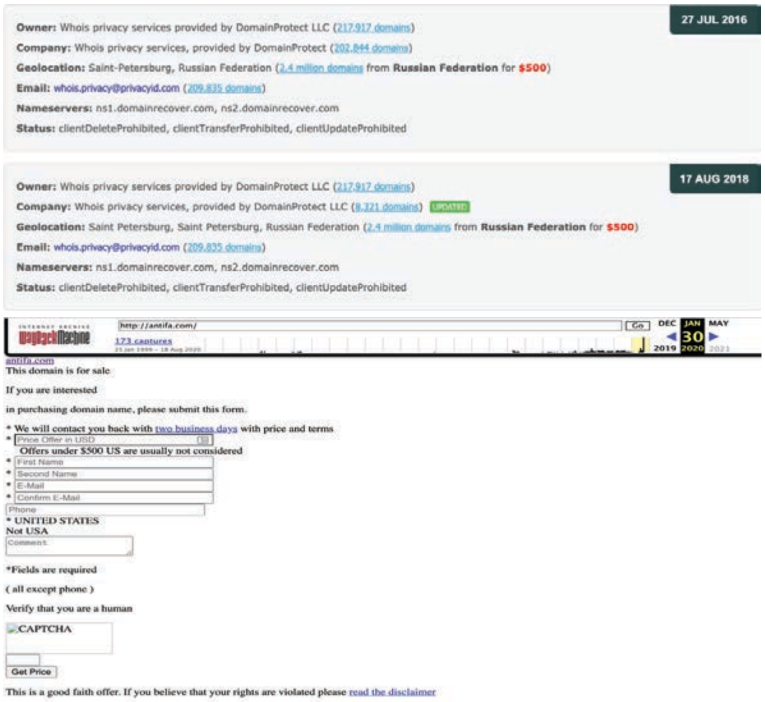
Former Vice President Joe Biden

A search for recent domain registrations identified many references to largely non-attributable, privacy protected domain registrations that employ variations of former Vice President Joe Biden's name, that appear similar to the official campaign website, joebiden[.]com, or that include oblique references to Biden. For example, at least 90 domains similar to the official Biden campaign domain were registered since January 2020. The top 10 domains ranked by the Risk Score, known associated malware or threat actor activity, or those assessed to be effective for use as a spearphing domain or within targeted intrusion or eCrime-related activity have been included in Appendix B, with the respective, known registration information and most recently observed resolution data.

Many of these domains appear to be linked to parked pages offered for sale that contain similar templatized content. Some of the pages solicit information from visitors to the site, purportedly as part of an offer to sign up for information, while a small subset contained information related to the candidate. Many of the IP addresses associated with the typosquat domains have been previously linked to botnet or phishing activity. As of this writing, however, we have not observed spearphishing activity associated with these domains directed at the Biden campaign or supporters.

Additionally, we identified efforts by external web addresses to redirect traffic to Biden's official campaign website. One effort was observed in August 2020 when antifa[.]com temporarily redirected traffic to joebiden[.]com. On August 12, President Trump was asked by One America News Network employee Chanel Rion at a White House Press Briefing if Joe Biden, Kamala Harris, and the Democratic Party should denounce antifa as a domestic terrorist organization to which Trump replied that they should but he believes that they are afraid to and that "it's virtually a part of their campaign." Users on social media seized on the redirection to promote the belief that the Biden campaign was somehow affiliated with Antifa, a U.S.-based, loosely organized, anti-fascist protest movement whose activities have frequently opposed those of white supremacists and right-wing extremists, sometimes including instances of violent conflict.

In April 2020, the antifa[.]com domain was registered via privacy protection service WhoisGuard, thereby obscuring its ownership. As of August 19, 2020, the registrar was listed as Namecheap and the contact information for the registrant is a post office box in Panama. This domain was linked broadly to Russia via a Yahoo media report on August 12, 2020, likely because it was previously owned by the domain registrar service Domerg Ltd. on the libris[.]com server, a privacy protected domain service out of St. Petersburg, Russia. This entity has owned antifa[.]com since at least April 2013. The claims of the domain as being associated with Russia were criticized by U.S. domestic outlet Mashable on August 13, 2020, with Russian state-funded media outlet RT echoing the criticisms on August 15, 2020. The domain was parked and advertised for sale to a bidder seeking this domain name; in April 2020 the domain changed hands and was transferred from the libris[.]com server to Namecheap ownership.



27 JUL 2016

Owner: Whois privacy services provided by DomainProtect LLC (217,917 domains)
Company: Whois privacy services, provided by DomainProtect (202,844 domains)
Geolocation: Saint-Petersburg, Russian Federation (2.4 million domains from **Russian Federation** for **$500**)
Email: whois.privacy@privacyid.com (209,835 domains)
Nameservers: ns1.domainrecover.com, ns2.domainrecover.com
Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited

17 AUG 2018

Owner: Whois privacy services provided by DomainProtect LLC (217,917 domains)
Company: Whois privacy services, provided by DomainProtect LLC (8,321 domains) UPDATED
Geolocation: Saint Petersburg, Saint Petersburg, Russian Federation (2.4 million domains from **Russian Federation** for **$500**)
Email: whois.privacy@privacyid.com (209,835 domains)
Nameservers: ns1.domainrecover.com, ns2.domainrecover.com
Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited

antifa.com
This domain is for sale

If you are interested

in purchasing domain name, please submit this form.

* We will contact you back with two business days with price and terms
* Price Offer in USD
Offers under $500 US are usually not considered
* First Name
* Second Name
* E-Mail
* Confirm E-Mail
Phone
* UNITED STATES
Not USA
Comment

*Fields are required

(all except phone)

Verify that you are a human

CAPTCHA

Get Price

This is a good faith offer. If you believe that your rights are violated please read the disclaimer

Screenshot of the domain registration showing historic Russian ownership of the antifa[.]com domain and a cached page of the domain, showing it advertised for sale (Sources: Whoxy, Wayback Machine)

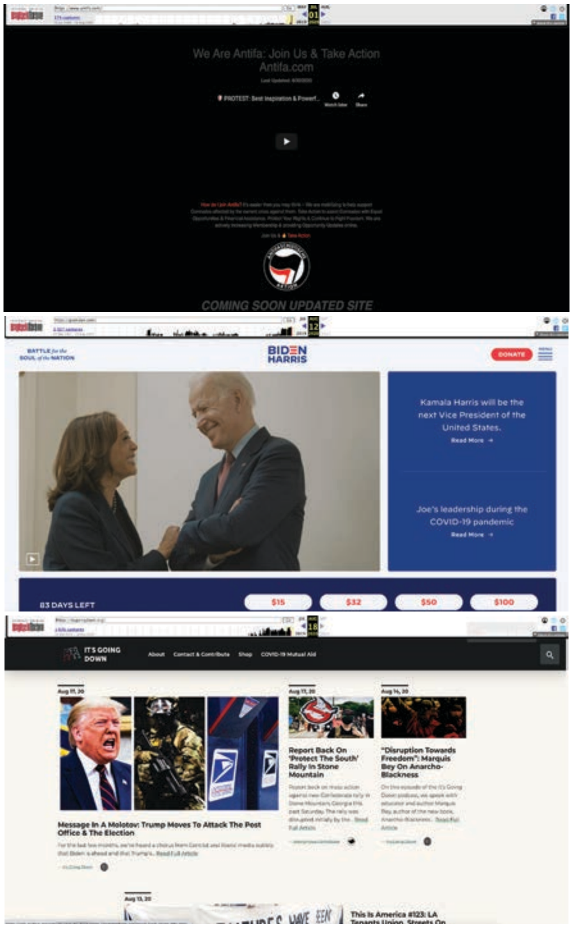
According to available data via the Internet Archive, antifa[.]com began redirecting to joebiden[.]com as early as August 12, 2020. It may have been redirecting to this domain prior to this date; however, that is the earliest snapshot of the website that definitively shows a redirect to the official website for the former Vice President. Prior to this date, on July 1, 2020, the website styled itself as a pro-Antifa resource which linked to a video on its YouTube page and provided the following invitation:

> *"How do I join Antifa? It's easier then [sic] you may think — We are mobilizing to help support Comrades affected by the current crisis against them. Take Action to assist Comrades with Equal Opportunities & Financial Assistance. Protect Your Rights & Continue to Fight Fascism. We are actively increasing Membership & providing Opportunity Updates online."*

The website also included popular hashtags used by the Black Lives Matter (BLM) movement, #JusticeForGeorgeFloyd and #NoJusticeNoPeace, and linked to their external social media presence. The antifa[.]com social media presence consists of a YouTube page that was created April 17, 2020 that has 14,065 views and other social media presence including one created in April 2020 with 145 followers at the time of this writing. The fact that the domain, social media account, and YouTube page were all created in April 2020 suggests it is very likely there is coordination between the websites and suggests one entity is behind all of these online accounts.

RT seized on the Mashable criticism of the Yahoo report linking antifa[.]com to Russia and echoed the negative sentiments included in the Mashable report. The RT reporting used the Mashable report as an initial point to suggest that there is a broader effort at play to blame Russia for foreign interference and claimed that, "Yahoo News, a major player in the 'Russiagate' conspiracy narrative."

As of August 27, 2020, antifa[.]com no longer redirects to joebiden[.]com, but instead is redirecting to itsgoingdown[.]org, a website that has historically posted anarchist content. Recorded Future analysts have observed this redirect changing periodically, between biden[.]com and the itsgoingdown[.]org The itsgoingdown[.]org domain is also registered with privacy protection via the Namecheap service and lists an address in Panama. The website claims the following: "It's Going Down is a digital community center for anarchist, anti-fascist, autonomous anti-capitalist and anti-colonial movements. Our mission is to provide a resilient platform to publicize and promote revolutionary theory and action" and "As a news and media platform, It's Going Down does not plan or organize protests or demonstrations. However, we signal boost what people are already organizing in their locality." The website maintains a social media presence with an Instagram page with at least 23,400 followers, a Facebook page with 31,988 followers, and elsewhere with close to 88,000 followers on other social media sites. The websites promote content that depicts protests, BLM, rent strikes, and encourages followers not to vote. Content that promotes abstaining from democratic engagement aligns with past and recent Russian affiliated influence efforts. A March 5, 2020 report from the Brennan Center for Justice on Russian influence operations reveals that, in line with historical Russian interference efforts in U.S. elections, some of the recent activity suggests that current operations are focused on dissuading voters in swing states from casting a ballot.



We Are Antifa: Join Us & Take Action
Antifa.com
COMING SOON UPDATED SITE
BATTLE for the SOUL of the NATION
BIDEN HARRIS
DONATE
Kamala Harris will be the next Vice President of the United States.
Read More →
Joe's leadership during the COVID-19 pandemic
Read More →
83 DAYS LEFT
$15
$32
$50
$100
IT'S GOING DOWN
About
Contact & Contribute
Shop
COVID-19 Mutual Aid
Message In A Molotov: Trump Moves To Attack The Post Office & The Election
Report Back On 'Protect The South' Rally In Stone Mountain
"Disruption Towards Freedom": Marquis Bey On Anarcho-Blackness
This Is America #123: LA Tenants Union, Streets On

Screenshots of antifa[.]com from July 1, August 12, and August 18, 2020 (Source: archive.org 1, 2, 3)

President Donald Trump

Recorded Future analysts also searched for domain registrations similar to the official domain (donaldjtrump[.]com) used by the re-election campaign for President Donald Trump and identified at least 78 references. The top 10 domains ranked by the Risk Score, known associated malware or threat actor activity, or those assessed to be effective for use as a spearphishing domain or within targeted intrusion or eCrime-related activity have been included in Appendix B, with the respective, known registration information and most recently known resolution data.

Many of these pages are parked and contain similar templatized content. Some of the pages solicited information from visitors to the website, purportedly as part of an offer to sign up for stock related information, while a small subset contained information related to the candidate. Many of the IP addresses associated with the associated typosquat domains were identified as having previously been associated with historical phishing activity and banking trojans. As of this writing, there does not appear to be any known or active threat associated with any of these domains aimed at President Trump.

One particular domain, donaldntrump[.]com, redirects to a YouTube video titled, "I have killed the dog," which was posted to the account GlassTastesGood on May 12, 2019, and has 138 views as of August 21, 2020. According to open-source records, the domain was registered on July 30, 2020 with privacy protection, therefore it is not possible to determine who may be associated with the page and why they would redirect it to this YouTube video.

Ransomware

On August 20, 2020, Recorded Future released a report that examined ransomware threats posed to three major elections-related entities — voter registration databases (VRDB), voting results databases, and poll books — to provide suggestions on how to protect against these resources against the threat. It is extremely unlikely that ransomware attacks would be capable of fully disrupting the 2020 election; however, it is possible that such attacks could result in localized disruptions, depending on the states targeted, as well as the timing of any attack(s). For example, the most impactful attacks may not necessarily occur on the day of the vote, but rather could occur 45-60 days before the election as states attempt to disseminate mail-in ballots, the first day of early voting, or even after the election when poll workers are attempting to verify mail-in ballots.

Moreover, in the last six months, ransomware attacks have repeatedly exploited Citrix systems and many VRDB rely on Citrix to manage their infrastructure. Another concern related to VRDBs is that many ransomware variants have trouble decrypting large file sizes. Given the size of VRDBs, even some of the tables stored as backup may be larger than a ransomware's decrypter can support. If a state is forced to pay the ransom, there is a real possibility that the decrypter will not work on VRDBs.

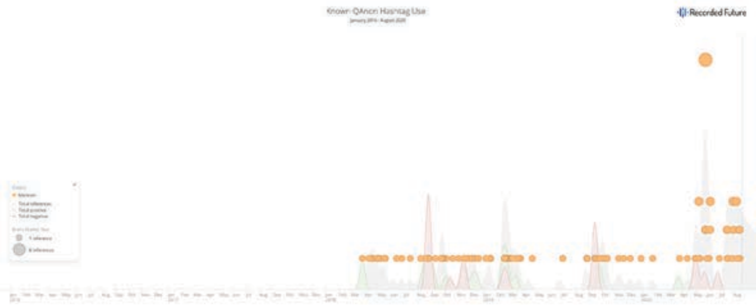
Although there has been no evidence or indications of ransomware attacks against election infrastructure as of this writing, the reporting outlines the threats clearly and reveals a lack of preparedness should one occur. Russia-based threat activity groups have used ransomware as a cover for destructive operations in the June 2017 NotPetya attacks, which initially impacted Ukrainian entities but quickly spread to organizations worldwide. In that instance, the threat activity group Sandworm employed malware which resembled ransomware which effectively served as a wiper against targets. Given that there is a precedent for this type of action by Russian threat activity group, there is a possibility that a similar scenario could play out against election-related targets in the U.S.

Non-State Groups

QAnon

There have already been indications that Russian overt and covert information operations entities have taken an interest in the QAnon movement and are actively amplifying its related content and distributing reporting on the group's activity. Its adherents are already primed to engage in wide scale online information operations, and it would not be difficult for an Russian threat actor or activity group to infiltrate and direct the movement to conduct operations on their behalf. QAnon adherents have also been associated with real world violence including murder, kidnapping, and domestic terrorism, and there is a risk that foreign interference threat actors or activity groups could incite elections interference or take other actions in the name of Q.

QAnon is the name given to an expansive conspiracy theory that is reported to have first emerged in October 2017 on the imageboard 4chan. The theory is predicated on the belief that there are shadowy forces that inhabit a "deep state" working to undermine President Trump.

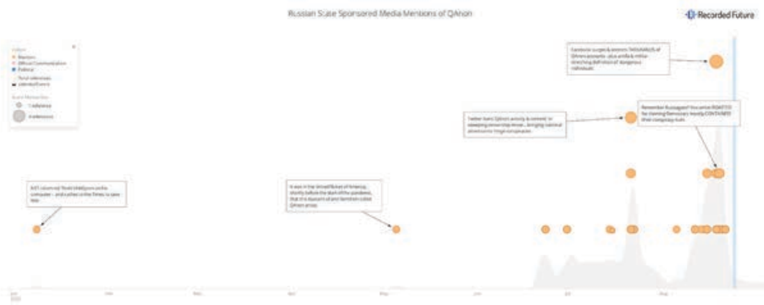


Timeline view of QAnon hashtag use since January 2016 (Source: Recorded Future)

The theory contains several similarities to the "Pizzagate" conspiracy that emerged during the 2016 presidential election following the release of APT28 hacked emails belonging to John Podesta, the campaign chair for Hillary Clinton. Both Pizzagate and QAnon theories were supported by content proliferated on anonymous message boards and via social media, and some of the general theories associated with the conspiracies are similar. An FBI intelligence bulletin, dated May 30, 2019, warned that conspiratorial beliefs pose a domestic security threat. Wired reported that, in February 2019, a QAnon post on the Endchan image board titled "Welcome to Information Warfare" invited followers to "[g]et ready for a new phase in the battle anons: the fight to take back the narrative from the [mainstream media]" with a goal of flooding the online space with partisan content.

In 2020, social media outlets worked to block QAnon-related hashtags as well as remove pages, accounts, and groups that are promoting the conspiracy theory. In April 2020 alone, Facebook reported the removal of five pages, 20 Facebook accounts, and six groups which were engaged in coordinated inauthentic behavior related to the QAnon conspiracy. Graphika conducted an investigation in association with this activity and identified that the groups efforts expanded beyond Facebook and that the accounts proliferated their messaging across multiple platforms. Therefore, despite efforts to take down content from social media platforms, the theory has continued to proliferate and has expanded in its reach. In fact, several QAnon adherents are on the ballot in November 2020 and projected to win seats in Congress in some states.

On August 24, 2020, Reuters reported that Russian overt information operations activity conducted by state-owned media platforms RT and Sputnik had increased their coverage of QAnon activity and IRA social media accounts had, "sent a high volume of tweets tagged with #QAnon and the movement slogan #WWG1WGA, short for Where We Go One, We Go All" in 2019. Additionally, the New York Times quoted Graphika Chief Innovation Officer Camille Francois as stating, “Russia is increasingly interested in QAnon, and it’s being reciprocated.” Also, in a recently released report by Graphika about Russian engagement with QAnon communities online they found that, “Russia also appears to have made the most effort to gain credibility within the community thus far.” Given that QAnon is such a wide ranging conspiracy with no identified or known leader, and Russian covert and overt influence entities online have taken an interest in this group, it is likely that Russian threat actors or activity groups could attempt to employ this movement to its own benefit.



Russian State Sponsored Media Mentions of QAnon (Source: Recorded Future)

As of this writing there are not clearly identified threats or known links between QAnon and foreign threat actors. However, there is clear evidence to show that QAnon represents a threat in both the physical and the online space. Furthermore, historical precedent reveals that Russian APT groups are willing to co-opt anonymous online entities to interfere in the election or provide cover for their activity. In August 2016, the online entity @anpoland claimed to have conducted intrusions into the non-profit Bradley Foundation and proceeded to leak files purportedly belonging to the organization. In August 2016, ThreatConnect revealed links between the @anpoland activity and activity conducted by APT28.

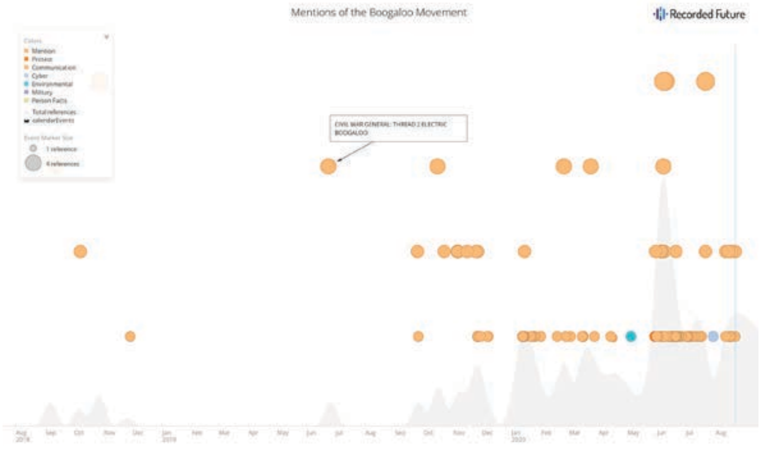
Boogaloo Movement

At a minimum, there is an established precedent for Russian influence operations working to co-opt ideologically motivated individuals as they used social media groups to encourage protests in New York City, New York, Houston, Texas, Florida and elsewhere, and during the 2016 U.S. presidential election. Given this precedent, the potential that Russian threat actors or activity groups could hijack existing activity, like that associated with the Boogaloo Movement remains a possible but highly dangerous threat.

The “Boogaloo” movement, which manifested itself on the online imageboard 4chan, later moving to wider social media platforms, is an “apocalyptic, anti-government group” which, among other stated goals, seeks to foment a second civil war in the U.S. According to The Atlantic, the movement began on a weapons-related 4chan board at least as early as 2018, and has gained significant traction in 2020. According to a report by investigative group Bellingcat, the movement later shifted to Facebook groups and posts, and alternately began referring to the movement as “The Big Igloo” and “The Big Luau”, encouraging adherents to dress in Hawaiian shirts; these shirts were later observed being worn by armed individuals appearing at “reopen” and BLM protests over the last several months.

Aside from being a largely online movement, as well as a physical presence at recent protests, several arrests and murders have taken place in recent months attributed to individuals associated with the Boogaloo movement:

- On April 11, 2020, a Texas man was apprehended by police for a Facebook Live video, in which he sought to murder police and professed to be a “Boogaloo Boy.”
- A May 29, 2020 murder of a federal officer in Oakland, who was protecting federal buildings during civil unrest protesting the death of George Floyd, as well as a murder of a deputy seeking to arrest the subject of the Oakland murder, have been attributed to an alleged adherent to the Boogaloo Movement.
- On June 3, 2020, three men were charged by Federal prosecutors in Las Vegas “alleging conspiracy to commit an act of terrorism, material support for committing an act of terrorism and multiple explosives violations.” The three men have been linked to the Boogaloo Movement.



Mentions of the Boogaloo movement in the last two years. (Source: Recorded Future)

Aside from the overt danger that the movement presents as a heavily armed group who has shown willingness to use violence in the name of their cause, given their alt-right penchant and built-in predilection to conspiracy, the Boogaloo movement would be an attractive target for foregin influence operations, or co-opting by a foreign threat group.

Outlook

U.S. officials or organizations have a greater awareness of and are more prepared for the potential of foreign interference to the November 2020 elections. Russian threat actors or activity groups are likely sensitive to measures the U.S. has taken to defend the 2020 elections and factoring that into their calculus. Based on these changes, it is likely any threat activity that may emerge from Russia against the 2020 U.S. presidential election will manifest differently from past efforts.

Russian threat activity groups who had conducted intrusions and operations against political parties and candidates in 2016 and 2018 have largely refrained from acting as of this writing. Although there has been no identified activity from Russian threat activity groups against elections-related entities yet, there has been activity by these groups in relation to malware development and intrusions against other entities in the U.S. Additionally, there have been attempts to spearphish entities abroad that have a nexus to the election, due to their association with Democratic presidential candidate Joe Biden. It is unclear at the time of writing if those efforts were successful. Recorded Future notes that, in a separate effort, some audio content has begun to be released that appears to relate to Biden, although this content has not been validated by third-parties as authentic or unaltered. Given that threat activity groups like APT28 have previously waited to release information they have obtained via targeted intrusions in order to maximize their impact, it is possible that a similar approach to delayed information release could occur in advance of the election.

Information operations are much more amenable to threat actor anonymity and very difficult to combat. Recorded Future observes that such operations remain an ongoing and real threat to the 2020 U.S. presidential election. Recorded Future has identified how the presence of Russian domestic and foreign operations conducted by the One Africa, One Success WhatsApp group, EBLA, and troll farms in Nigeria and Ghana reveal a shift away from more centralized and controlled operations to distributed and resilient information operations networks. Although many such efforts have been identified and taken down, there are still likely more remaining, operating unseen. While the fragmentation of such operations could point to the success of a U.S. operation to disrupt IRA influence efforts during the 2018 U.S. midterm elections, it is likely that they also reveal a degree of persistence and resilience of these operations, in the near term.

Russian threat actors or activity groups actively sought to use domestic American assets to bypass social media’s increasingly difficult advertising restrictions against foreign nationals, as well as to increase the difficulty in accurately detecting false personas or personas influenced by nefarious objectives. As social media platforms continue to limit the availability of advertisements and ability for foreign nationals to engage in U.S. political discourse, we continue to expect that engagement with Americans will remain a priority by Russian influence operations assets to bypass ad restrictions, establishing intelligence assets, and astroturf divisive content.

The expansion of conspiracy groups like QAnon or anti-government groups like the Boogaloo movement pose an additional threat to the election. These leaderless groups have the potential to be infiltrated and co-opted by a foreign threat actor seeking to disrupt the election. Adherents to the QAnon conspiracy have already displayed a willingness to engage in “information warfare” and several of their followers have committed criminal acts. In a similar fashion, several adherents to the Boogaloo Movement have committed murder or attempted murder and attempted domestic terrorism in the hopes of acting on their anti-government creed, to bring about a second U.S. civil war. The group has had a visible presence in recent “reopen” and BLM protests, appearing in body armor and heavily armed. This group presents itself both as a physical threat to election security, should the group choose to target election-related assets or polling places, as well as an online threat to spreading disinformation, which could eventually skew towards election related topics in an anti-government narrative.

Appendix A — Indicators of Compromise

2016 APT28 and APT29 Intrusion Activity Against the DNC

	Command and Control	
Threat Activity Group Name	**Indicator Description**	**IP Address**
APT28	X-Agent implant C2	185.86.148[.]227:443
APT28	X-Tunnel implant C2	45.32.129[.]185:443
APT28	X-Tunnel implant C2	23.227.196[.]217:443
APT29	SeaDaddy implant C2	185.100.84[.]134:443
APT29	SeaDaddy implant C2	58.49.58[.]58:443
APT29	Powershell implant C2	218.1.98[.]203:80
APT29	Powershell implant C2	187.33.33[.]8:80

	Malware	
Threat Activity Group Name	**Indicator Description**	**SHA 256**
APT28	X-Agent implant twain_64.dll	fd39d2837b30e7233bc54598ff51bdc2f8c418fa5b94dea2cadb24cf40f395e5
APT28	X-Tunnel implant VmUpgradeHelper.exe	4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976
APT28	X-Tunnel implant VmUpgradeHelper.exe	40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f
APT29	SeaDaddy implant pagemgr.exe	6c1bce76f4d2358656132b6b1d471571820688ccdbaca0d86d0ca082b9390536
APT29	SeaDaddy implant pagemgr.exe	b101cd29e18a515753409ae86ce68a4cedbe0d640d385eb24b9bbb69cf8186ae

Source: Crowdstrike

2018 APT28 Domain Registrations Spoofing Political and Elections-Related Entities

APT28 Domain Registrations		
Domain Registration	**Likely Mimics Legitimate Domain**	**Organization Associated with Legitimate Domain**
my-iri[.]org	iri[.]org	International Republican Institute - a Washington, DC non-profit
hudsonorg-my-share-point[.]com	hudson[.]org	Hudson Institute a non-profit American think tank based in Washington, D.C
senate[.]group	senate[.]gov	United States Senate
adfs-senate[.]services	N/A	Active Directory Federation Services (ADFS) is a Single Sign-On (SSO) solution created by Microsoft potentially similar to one used by the U.S. Senate
adfs-senate[.]email	N/A	Active Directory Federation Services (ADFS) is a Single Sign-On (SSO) solution created by Microsoft potentially similar to one used by the U.S. Senate
adfs.senate.gov[.]info	N/A	Active Directory Federation Services (ADFS) is a Single Sign-On (SSO) solution created by Microsoft potentially similar to one used by the U.S. Senate
office365-onedrive[.]com	N/A	Online Login Resources for Microsoft OneDrive

Source: Microsoft, Trend Micro

Indicators of Compromise Related to 2020 Activity

The following indicators of compromise (IoCs) relate to the attempted spearphishing of Burisma Holdings:

Target	Malicious Domain	Domain Registration Date	SPF Record	DKIM Record
KUB-Gas LLC	Kub-Gas[.]com	11/10/2019	“v=spf1 redirect=_spf. yandex.net”	“v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADC BiQKBgQDHmyzwHPXNRG0Q2mDIFPR8hfWSLh HMcEqndEbcxqef24gvt0HOFA+8YZC7VZnwH6Tz OofySR1MEh3ssau9iwXy+QVyIDNIQLwzZ8x8qWd HPP8NC/05R+VBDIpnx7bIIbPYpt7CIJ/sXLt2tvzLdJ bIn P4vABcjGoMYibZ5JGbrwIDAQAB”
KUB-Gas LLC	mail.kub-gas[.]com	11/10/2019	N/A	N/A
Esko-Pivnich	mail.esco-plvnlch[.]com	11/24/2019	“v=spf1 include:spf. privateemail.com ~all”	N/A
CUB Energy Inc	cubenergy-my-share-point[.]com	12/03/2019	“v=spf1 include:spf. privateemail.com ~all”	N/A

Source: Area 1

The following IoCs relate the Sandworm C2 associated with the Exim vulnerability:

IP Addresses
95.216.13[.]196
103.94.157[.]5
hostapp[.]be

Source: National Security Agency Cyber Security Advisory

The following IoCs are attributed by the NCSC as pertaining to the alleged APT29 attempt to gain information on COVID-19 vaccine research. Please reference the original report for additional YARA rules for detection.

WellMess Hashes
00654dd07721e7551641f90cba832e98c0acb030e2848e5efc0e1752c067ec07
0322c4c2d511f73ab55bf3f43b1b0f152188d7146cc67ff497ad275d9dd1c20f
03e9adae529155961f1f18212ff70181bde0e3da3d7f22961a6e2b1c9da2dd2e
0b8e6a11adaa3df120ec15846bb966d674724b6b92eae34d63b665e0698e0193
14e9b5e214572cb13ff87727d680633f5ee238259043357c94302654c546cad2
1fed2e1b077af08e73fb5ecffd2e5169d5289a825dcaf2d8742bb8030e487641
21129ad17800b11cdb36906ba7f6105e3bd1cf44575f77df58ba91640ba0cab9
2285a264ffab59ab5a1eb4e2b9bcab9baf26750b6c551ee3094af56a4442ac41
2daba469f50cd1b77481e605aeae0f28bf14cedfcd8e4369193e5e04c523bc38
49bfff6b91ee71bbf8fd94829391a36b844ffba104c145e01c92732ada52c8ba
4c8671411da91eb5967f408c2a6ff6baf25ff7c40c65ff45ee33b352a711bf9c
5ca4a9f6553fea64ad2c724bf71d0fac2b372f9e7ce2200814c98aac647172fb
797159c202ca41356bee18c5303d37e9d2a43ca43d0ce02e1fd9e7045b925d11
7c39841ba409bce4c2c35437ecf043f22910984325c70b9530edf15d826147ee
84b846a42d94431520d3d2d14262f3d3a5d96762e56b0ae471b853d1603ca403
8749c1495af4fd73ccfc84b32f56f5e78549d81feefb0c1d1c3475a74345f6a8
92a856a2216e107496ee086e1c8cfe14e15145e7a247539815fd37e5a18b84d9
93e9383ae8ad2371d457fc4c1035157d887a84bbfe66fbbb3769c5637de59c75
953b5fc9977e2d50f3f72c6ce85e89428937117830c0ed67d468e2d93aa7ec9a
a03a71765b1b0ea7de4fbcb557dcfa995ff9068e92db9b2dada9dd0841203145
a117b2a904c24df62581500176183fbc282a740e4f11976cdfc01fe664a02292
a3ca47e1083b93ea90ace1ca30d9ef71163e8a95ee00500cbd3fd021da0c18af
b75a5be703d9ba3721d046db80f62886e10009b455fa5cdfd73ce78f9f53ec5a
bec1981e422c1e01c14511d384a33c9bcc66456c1274bbbac073da825a3f537d
c1a0b73bad4ca30a5c18db56c1cba4f5db75f3d53daf62ddc598aae2933345f3
d7e7182f498440945fc8351f0e82ad2d5844530ebdba39051d2205b730400381
dd3da0c596fd699900cdd103f097fe6614ac69787edfa6fa84a8f471ecb836bb
e329607379a01483fc914a47c0062d5a3a8d8d65f777fbad2c5a841a90a0af09
e3d6057b4c2a7d8fa7250f0781ea6dab4a977551c13fe2f0a86f3519b2aaee7a
f3af394d9c3f68dff50b467340ca59a11a14a3d56361e6cffd1cf2312a7028ad
f622d031207d22c633ccec187a24c50980243cb4717d21fad6588dacbf9c29e9
fd3969d32398bbe3709e9da5f8326935dde664bbc36753bd41a0b111712c0950

WellMess IP Addresses
103.103.128[.]221
103.13.240[.]46
103.205.8[.]72
103.216.221[.]19
103.253.41[.]102
103.253.41[.]68
103.253.41[.]82
103.253.41[.]90
103.73.188[.]101
111.90.146[.]143
111.90.150[.]176
119.160.234[.]163
119.160.234[.]194
119.81.173[.]130
119.81.178[.]105
120.53.12[.]132
122.114.197[.]185
122.114.226[.]172
141.255.164[.]29
141.98.212[.]55
145.249.107[.]73
146.0.76[.]37
149.202.12[.]210
169.239.128[.]110
176.119.29[.]37
178.211.39[.]6
185.120.77[.]166
185.145.128[.]35
185.99.133[.]112
191.101.180[.]78
192.48.88[.]107
193.182.144[.]105
202.59.9[.]59
209.58.186[.]196
209.58.186[.]197

WellMess IP Addresses
209.58.186[.]240
220.158.216[.]130
27.102.130[.]115
31.170.107[.]186
31.7.63[.]141
45.120.156[.]69
45.123.190[.]167
45.123.190[.]168
45.152.84[.]57
46.19.143[.]69
5.199.174[.]164
66.70.247[.]215
79.141.168[.]109
81.17.17[.]213
85.93.2[.]116

WellMail Hashes
83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18(UPX)
0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494 (Unpacked)

WellMail IP Addresses (Malware)
103.216.221[.]19

WellMail IP Addresses (‘GlobalSign’ certificate, operated by APT29 but not necessarily used for WellMail malware communications))
119.81.184[.]11
185.225.226[.]16
188.241.68[.]137
45.129.229[.]48

SoreFang Hashes
58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2
65495d173e305625696051944a36a031ea94bb3a4f13034d8be740982bc4ab75
a4b790ddffb3d2e6691dcacae08fb0bfa1ae56b6c73d70688b097ffa831af064

SoreFang IP Addresses (Malware)
103.216.221[.]19

Appendix B — Sample List of Domain Registrations Since January 2020

Joe Biden

Date Registered	Domain	Registration and/or Website Information	IP Address & Risk Scores
March 11, 2020	joesbiden[.]com	Domain redirects to a Medium.com story dated March 18, 2020 by Sean Moorhead titled “I’m a Bernie volunteer. Here’s how Joe Biden can win Bernie voters.” also redirects to DNC fundraising website	216.239.38[.]21 Suspicious - 64 216.239.34[.]21 Suspicious - 61 216.239.32[.]21 Suspicious - 55 216.239.36[.]21 Suspicious - 52
March 11, 2020	joebidenn[.]com	Google LLC; Appears to redirects to the DNC fundraising site ActBlue, and provides an error message as follows, *“You have attempted to make a contribution to a fundraising page that has no active recipients; either the page’s owner has remove all committees or organizations from the page, or we have included processing contributions for these committee or organizations”* with a link to contact the site owner.	216.239.36[.]21 Suspicious - 52 216.239.38[.]21] Suspicious - 64 216.239.32[.]21 Suspicious - 51 216.239.34[.]21 Suspicious - 57
June 3, 2020	jobebiden[.]com	ClaraNET LTD; N/A	195.22.26[.]248 Suspicious - 64
July 11, 2020	joebiden[.]tv	Chengdu West Dimension Digital Technology Co., Ltd.; Site offering products and styling itself as a news site focused on Joe Biden	63.250.43[.]2 Suspicious - 25
July 11, 2020	joebiden[.]in	GoDaddy.com, LLC; Website that styles itself after the official Joe Biden campaign website	43.255.154[.]37 Suspicious - 28
August 13, 2020	joebiden[.]design	Porkbun, LLC; Domain name offered for sale	52.58.78[.]16 Suspicious - 40
August 14, 2020	jooebiden[.]com	NameSilo, LLC; A website hosting links to external “Related Links” and other sites	199.59.242[.]153 Suspicious - 55
August 16, 2020	joebiden[.]tax	GoDaddy.com, LLC; Redirects to a website called the “American Herald” which styles itself as a media site that is critical of Joe Biden	184.168.131[.]241 Suspicious - 63
August 18, 2020	joebiden1[.]com	GoDaddy.com, LLC; Purports to be website allowing visitors submit their contact info to sign up for content from a stock related news bot	184.168.131[.]241 Suspicious - 63
August 19, 2020	joeebiden[.]com	GoDaddy.com, LLC; Purports to be website allowing visitors submit their contact info to sign up for content from a stock related news bot	184.168.131[.]241 Suspicious - 63

Donald Trump

Date Registered	Domain	Registration and/or Website Information	IP Address & Risk Scores
March 24, 2020	donaldrtrump[.]com	PLI-AS, CH; Page is blank and displays an error message "Too Many Requests"	63.143.32[.]94 Suspicious - 25
April 15, 2020	donaldjtromp[.]com	Namecheap-Net, US; Parked page, template page with external links in English	162.255.119[.]9 Suspicious - 31
April 16, 2020	donldjtrump[.]com	AMAZON-02, US; redirects to ww38.donldjtrump[.]com; Parked page	103.224.212[.]222 Suspicious - 49
May 19, 2020	dpnaldjtrump[.]com	GOOGLE, US; Parked page with text in German that appears to link to external sites	34.102.136[.]180 Suspicious - 46
May 24, 2020	donaldjtrump[.]com[.]au	Dreamscape Networks Limited, AU; Parked page domain purports to be registered by crazydomains[.]com[.]au	203.170.80[.]253 Suspicious - 27 203.170.80[.]250 Suspicious - 37
June 10, 2020	doñaldjtrump[.]com	Certificate registration for this domain; redirects to https://xn--doaldjtrump-2db.com/ containing a photo of Donald Trump, styled after his main page featuring the text "Black Lives Matter"	151.101.65[.]195 Suspicious -58 151.101.1[.]195 Suspicious - 50
June 16, 2020	ddonaldjtrump[.]com & donaldsjtrump[.]com	GoDaddy.com, LLC and BODIS-NJ, US (respectively); Parked page with links to external websites	199.59.242[.]153 Suspicious - 60
June 17, 2020	donaldntrump[.]com	Redirects to a YouTube video titled "I have killed the dog"	184.168.131[.]241 Suspicious - 63
June 20, 2020	donaldjttrump[.]com	BODIS-NJ, US; Parked page with links to external websites	199.59.242[.]153 Suspicious - 60
August 19, 2020	d0naldjtrump[.]com; donaldjtrmup[.]com; donaldtjrump[.]com	BODIS-NJ, US; Parked page with links to external websites	199.59.242[.]153 Suspicious - 60

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.