Cyber-attacks against the 2020 US elections - A first analysis

Threat Memo - Date: 04/11/2020 - Version: 1.0

TLP:WHITE

	Category	Type	Domain(s)	Sector(s)	Confidence
FOR INFORMATION	Cyberwar, Cyberespionage, Cybercrime, Hacktivism	Targeted intrusions, hack and leak, influence operation, ransomware, botnet	[World]	Elections, Political affairs	A1

Key Points

- According to US authorities and security companies, several actors attempted to influence or disrupt the US 2020 presidential elections.
- Four categories of attacks have been identified: influence operations, cyberespionage, cybercrime, and hacktivism.

- US authorities took measures such as dismantling attackers' infrastructure, charging or sanctioning individuals or organisations, and sharing technical alerts.
- Public reports allow to draw a first synthetic analysis on the *state of the art* for election interference risk mitigation.

Summary

In the last few weeks preceding the 2020 US presidential election, there have been several public reports, many of them originating from reputed sources, or official press releases related to cyberattacks aiming at disrupting or influence these elections. This mass of information makes it possible to draw, based on *real-life incidents*, a realistic landscape of today's threats to a democratic election process.

The table below indicates some of the identified actors that have, according to US authorities or companies, attempted to interfere with the US presidential election.

Identified threat actors	Country	Tactic	Response
* Internet Research Agency * Strategic Culture Foundation * DCLeaks	Russia	Influence operations on social networks (Facebook) and other media	* Removing accounts on social media * Naming and shaming * Sanctions
* Islamic Revolutionary Guard Corps and affiliated organisations	Iran	Influence operations on social networks (Facebook) and other media	* Seizing domains * Removing accounts on social media * Naming and shaming * Sanctions
* Ransomware operators (Ryuk, others)		* Botnet * Big game hunting	* Disrupting botnet
* APT28	Russia	* Targeted intrusions * Stealing sensitive information	* Sharing indicators of compromise and TTP information
* APT31	China	* Targeted intrusions * Stealing sensitive information	* Sharing indicators of compromise and TTP information
* APT35	Iran	* Targeted intrusions * Stealing sensitive information	* Sharing indicators of compromise and TTP information

Influence operations

In the months preceding the elections, US authorities and US firms uncovered and revealed several information operations aiming at "**sowing discord** among the voting populace by **spreading disinformation** online and executing malign influence operations aimed at **misleading US voters**."[1][2]

According to reports, tactics used by attackers included the following:

- Disguising as news organisations or media outlets,
- Posing as editors and journalists,
- Managing networks of social media accounts to promote sites frequented by right-wing,
- Paying real Americans to write about politically sensitive issues,
- Denigrating US President Donald Trump by highlighting issues of racial tension, criticizing the US foreign policy, and condemning the response to the COVID-19 outbreak.

US authorities[1] and think tanks[3] have attributed these influence operations mainly to two countries:

- Iran, especially organisations tied to the Islamic Revolutionary Guard Corps (IRGC),
- Russia, in particular organisations specialised in influence operations such as the Internet Research Agency and the Strategic Culture Foundation.

In reaction to these operations, measures taken by US authorities or companies consisted of:

- Releasing public alerts detailing ongoing operations,
- Sanctioning of individuals or organisations accused of being behind the operations[1],
- Seizing infrastructure[4],
- Removing organised networks of social media accounts[5].

Cyberespionage

US authorities and US security firms warned on the risk of cyberespionage operations aiming at stealing sensitive political information that could be used in post-exploitation operations ("**hack and leak**"). Russian actors had indeed used this tactic against the US Democratic candidate during the 2016 election. In early September, Microsoft released a report[6] in which they identified three active threat actors targeting the US political scene.

- APT28 (Strontium), operating from Russia, has attacked more than 200 organisations, including political campaigns, advocacy groups, parties, and political consultants.
- APT31 (Zirconium), operating from China, has attacked high profile individuals associated with the election, including people associated with the Joe Biden for President campaign as well as prominent leaders in international affairs.
- APT35 (Phosphorus), operating from Iran, has continued to attack the personal accounts of people associated with the Donald J. Trump for President campaign.

As of the time of writing, however, no significant public exposure of information that might have been stolen in these operations has been detected.

Cybercrime

Three principal categories of cybercrime attacks have been observed targeting the election process: ransomware disruption, selling voter data, lures for malware distribution.

- **Ransomware disruption and leaks**. In a global context where ransomware has become the most significant cybercrime threat, across countries and sectors, the US authorities warned[7] of ransomware attacks disrupting the election process. In summary, however, it does not appear that this threat has materialised in a significant manner. In a single event, at a Georgia county, cybercriminals disabled a database used to verify voter signatures of absentee ballots. The ransomware attackers also leaked voter information.

To fight the ransomware threat, the US tried[8] to disrupt one of the most important infection vectors, the Trickbot botnet. A coalition of public and private entities joined their forces to that end. There was some success in disrupting the botnet, but only for a limited duration. The cybercriminals behind TrickBot have continued to develop new functionality and tools, increasing the ease, speed, and profitability of victimization. They have learned and they re-built a more resilient botnet.

- **Malware distribution**. Cybercriminals behind Emotet leveraged[9] the US 2020 Presidential election with a spam campaign pretending to be from the Democratic National Convention's Team Blue initiative.

- **Selling voter data**. Hackers have reportedly[10] been selling personal and voter registration data for some 186 million American voters, on the dark web. Information compromised and being sold includes victims' full names, email addresses, phone numbers, and voter registration records.

Hacktivism

Based on available reports, the threat by political hacktivists, who typically use tactics like **leaks**, **defacements**, or **denial of service attacks**, has not been identified as significant. One incident was however noted: on October 27, the website of the US President Donald Trump's campaign was defaced[11] for roughly thirty minutes before being fully restored. The defacement message —written in grammatically incorrect English— claimed the perpetrator had compromised several devices and obtained "strictly classified information" but offered no evidence to support the assertion.

Comments

The US response to risks of disruption in the 2020 presidential election, was provided by public authorities and security firms. On the public side, the US Federal Bureau of Investigation (FBI) and the US Cybersecurity and Infrastructure Security Agency (CISA) have released warnings, alerts and have shared actionable information; the US Cyber Command and the NSA have run offensive operations against the infrastructure of threat actors; the US

Department of Justice and US Department of Treasury have respectively charged or sanctioned individuals or organisations.

In some cases, measures taken were intended to have an immediate operational effect: seizing domains, disrupting a botnet, removing social media accounts, sharing indicators of compromise to detect intrusions. In other cases, they aimed at a deterrence effect or to publicly show that authorities were addressing threats: naming and shaming, charging[12] individuals or entities assessed to be behind past operations.

Annex - Recent cybersecurity-related events in the US election process.

Date	Category	Type	Political attribution	Summary	Details
2-Nov	Cyberwar	Electoral interference	Iran	Spreading disinformation	Gen. Paul Nakasone, who leads both the NSA and the US Cyber Command, revealed that these two entities have taken recent actions to ensure that foreign actors do not interfere in the 2020 election, including an operation in the last two weeks of October against Iran. The NSA had been watching the Iranians for a while, had a “very good understanding on what a number of actors were trying to do, (…) provided early warning and followed [them very closely], (…) and weren’t surprised by their actions.”

Date	Category	Type	Political attribution	Summary	Details
30-Oct	Cyberwar	Influence operation	Iran	Steal voter data	The US CISA and FBI jointly issued an alert describing Iranian state-sponsored cyber activities conducted against several state and election-related websites. Attackers successfully obtained voter data from an unidentified US state's website. The CISA advisory associates the activity to the actor responsible for sending voter intimidation emails masquerading as the Proud Boys.
30-Oct	Cyberespionage	Targeted intrusion	Russia	Target the email accounts of Democratic state parties	According to an article from Reuters, the Russia-based APT28 threat actor targeted the email accounts of Democratic state parties in California and Indiana, and influential think tanks in Washington and New York.

Date	Category	Type	Political attribution	Summary	Details
27-Oct	Hacktivism	Defacement		Defacement of Trump’s campaign website	US President Donald Trump’s campaign website was defaced for roughly thirty minutes before being fully restored. The defacement message —written in grammatically incorrect English— claimed the perpetrator had compromised several devices and obtained “strictly classified information” but offered no evidence to support the assertion.
23-Oct	Unknown	Targeted intrusion		Cyberattacks aimed at small government offices	The Louisiana National Guard was called in to stop a series of cyberattacks aimed at small government offices across the state in recent weeks, according to two people with knowledge of the events, highlighting the cyber threat facing local governments in the run-up to the 2020 US presidential election.

Date	Category	Type	Political attribution	Summary	Details
22-Oct	Cyberwar	Influence operation	Iran	Spreading disinformation	On October 22, the US Department of Treasury sanctioned 5 Iranian entities - tied to the Islamic Revolutionary Guard Corps (IRGC) - for attempting to influence elections in the US. They are accused of targeting the US's electoral process with brazen attempts to sow discord among the voting populace by spreading disinformation online and executing malign influence operations aimed at misleading US voters. They have reportedly disguised themselves as news organisations or media outlets.
21-Oct	Cybercrime	Selling voter registration data		Selling voter registration data	Hackers have reportedly been selling personal and voter registration data for some 186 million American voters on the dark web. Information compromised and being sold includes victims' full names, email addresses, phone numbers, and voter registration records.

Date	Category	Type	Political attribution	Summary	Details
20-Oct	Cyberwar	Influence operation	Iran	Intimidation emails	Voters registered as Democrats in Florida and Alaska received voter intimidation emails. These emails use the subject “Vote for Trump or Else” and warn Democrat votes that they must change their party to Republican and vote for President Trump, or the Proud Boys (far-right group) will come after them. The US government confirmed that some voter registration information has been obtained by Iran (and separately by Russia) and that Iran is behind the threatening emails.
9-Oct	Cybercrime	Botnet, ransomware	Trickbot	Disrupt botnet used to spread ransomware	The US Cyber Command has mounted an operation to temporarily disrupt the Trickbot botnet. With more than 2 million infected hosts, Trickbot is currently one of the largest botnets. The goal of the Cyber Command is to prevent the botnet from disrupting the presidential elections with ransomware attacks. See details in TM-20-129.

Date	Category	Type	Political attribution	Summary	Details
7-Oct	Cyberwar	Influence operation	Iran	Spreading disinformation	The US Department of Justice seized 92 domains used in Iranian global disinformation. The campaign was focusing on denigrating US President Donald Trump, highlighting issues of racial tension, and criticizing US foreign policy and its response to the COVID-19 outbreak. The IRGC, who is accused by the US to be behind the disinformation campaign, also has ties with cyberespionage groups. See details in TM-20-130.
7-Oct	Cybercrime	Ransomware		Disable voter verification system	Georgia county voter information leaked by ransomware gang. The Georgia Hall County government suffered a ransomware attack that disabled a database used to verify voter signatures when authenticating absentee ballots, which could ultimately disrupt voting systems and raise public doubts about the validity of the vote outcome.

Date	Category	Type	Political attribution	Summary	Details
2-Oct	Cybercrime	Malware	Emotet	Malware infection	Emotet is now taking part in the US 2020 Presidential election with a new spam campaign pretending to be from the Democratic National Convention’s Team Blue initiative.
2-Oct	Cyberwar	Influence operation	Iran	Spreading disinformation	After being alerted by the FBI about suspicious account behaviour, Twitter announced on Wednesday it has removed some 130 Iranian accounts that were created to sow disinformation and disrupt the first 2020 US presidential debate.

Date	Category	Type	Political attribution	Summary	Details
2-Oct	Cyberwar	Influence operation	Russia	Spreading disinformation	A Russia-based operation is posing as an independent news agency called the Newsroom for American and European Based Citizens (NAEBC) in order to spread disinformation and influence voters on both sides of the political aisle ahead of the 2020 US presidential election. According to reports, the NAEBC website largely focused on US current events, paid real Americans to write about politically sensitive issues, and republished articles from conservative media, all of which was then promoted on social media sites frequented by right-wing users by a network of accounts posing as editors and journalists.

Date	Category	Type	Political attribution	Summary	Details
28-Sep	Cyberwar	Influence operation		Spreading disinformation	The FBI and the CISA today issued a joint public service announcement about the threat of disinformation campaigns targeting the 2020 US election season. Threat actors actively spreading false information about successfully compromised voting systems and voter registration databases “to manipulate public opinion, sow discord, discredit the electoral process,” and to weaken the public’s trust in US institutions according to the two agencies.
24-Sep	Cyberwar	Influence operation	Russia	Hack and leak	Facebook removed 3 Russian networks engaged in foreign and government interference. Behind these networks, Facebook found individuals associated with 2 entities specialised in influence operation: the Internet Research Agency and the Strategic Culture Foundation. Facebook also found individuals associated with an entity specialised in the “leak” side of “hack and leak” operations, DCleaks.

Date	Category	Type	Political attribution	Summary	Details
10-Sep	Cyberespionage	Targeted intrusion	Russia, China, Iran	Target political parties, political campaigns	Microsoft report on cyberattacks targeting US elections: - APT28 (Strontium), operating from Russia, has attacked more than 200 organisations including political campaigns, advocacy groups, parties and political consultants - APT31 (Zirconium), operating from China, has attacked high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community - APT35 (Phosphorus), operating from Iran, has continued to attack the personal accounts of people associated with the Donald J. Trump for President campaign

Date	Category	Type	Political attribution	Summary	Details
10-Sep	Cyberwar	Electoral interference	Russia	Steal US identities	The US Department of Justice (DoJ) announced a criminal complaint filed against Russian national Artem Mikhaylovich Lifshits. In a statement, the DoJ detailed his alleged use of stolen US identities to open fraudulent accounts at banks and cryptocurrency exchanges in support of electoral interference on behalf of Russia, as well as for personal enrichment. The complaint indicates members of Project Lakhta, a Russian interference effort stretching from mid-2014 to present, purchased the means of identification of US persons, which they then used to open bank accounts, PayPal accounts, and cryptocurrency accounts.

References

1. https://home.treasury.gov/news/press-releases/sm1158
2. https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia/
3. https://medium.com/dfrlab/facebook-takes-down-assets-linked-to-russian-disinformation-outlet-acab0164e3d4
4. https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps

https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia/
5.
6. [https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/]https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/)
7. https://www.reuters.com/article/us-usa-cyber-election-exclusive/exclusive-u-s-officials-fear-ransomware-attack-against-2020-election-idUSKCN1VG222
8. https://krebsonsecurity.com/2020/10/report-u-s-cyber-command-behind-trickbot-tricks/
9. https://www.bleepingcomputer.com/news/security/emotet-malware-takes-part-in-the-2020-us-elections/
10. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/massive-us-voters-and-consumers-databases-circulate-among-hackers/
11. https://www.cbsnews.com/news/trump-campaign-website-defaced/
12. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and