Radware Cybersecurity Alert

Election-Interfering Cyberattacks

September 22, 2020

AN ASSESMENT OF DDOS ATTACKS RELATING TO ELECTION PROCESSES AROUND THE GLOBE

DDoS Attacks Impact the Election Process

Election interference is defined as an attempt by a government to influence an election in another country for political gain. Via covert and overt operations, both **nation states** and **individuals** have been able to accomplish regime change. The only thing that has changed in terms of foreign electoral intervention is the way current operations are conducted in a digital age.

The digital evolution has had a positive and a negative impact on election processes around the world. While information and news travel at a faster rate, the powers that be have leveraged this exposure for political gain and exploitation. The digital evolution of the election process has created a larger threat landscape than most anticipated.

Election Interference

Today, there are a few fundamental ways an adversary could digitally interfere with an election process. A malicious actor could interfere with an election through disinformation campaigns, information-based campaigns or disruptive attacks.

Disinformation campaigns can leverage social network bots to spam the world with misinformation to influence an array of people. Targeted disinformation campaigns make use of information and **intelligence gathered from big data leaks and paid ad campaigns on social media platforms that target specific people and groups**.

Information campaigns typically involve spear phishing and malware-based attacks designed to gain access to critical systems to either alter, leak or destroy the data. Normally, the malicious actors look to steal campaign strategies and sensitive information to manipulate, overstimulate and emotionally-compromise social media users. This is accomplished by targeting the personal/professional emails or social media accounts of election officials, campaign staff or volunteers **so they can discredit and smear a targeted campaign at strategic moments**. By compromising digital users with information, a threat actor can influence an election.

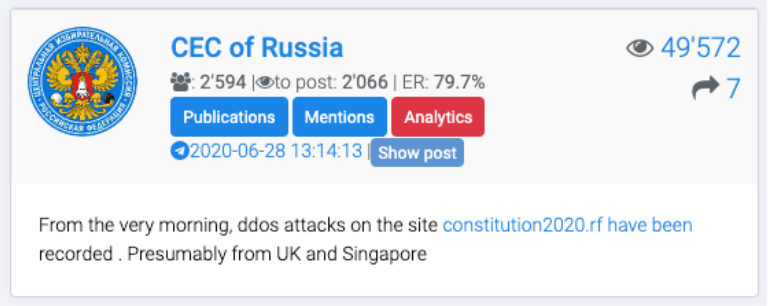
The other form of election interference comes in the form of disruption that can sometimes be caused by the majority party to silence their opposition. Attacks can range from **disruptive calls and messages designed to flood campaign resources** to malicious acts such as **denial-of-service attacks on election-related website** and **reporting systems**. Additionally, outages designed to impact power, water, internet, telephone and transportation services are used to cause chaos, project national instability and influence voters at critical moments.

Around the Globe in 2020

Throughout 2020, several countries have experienced services degradation caused by denial-of-service attacks during election processes. Typically, voting machines are not directly targeted during disruption-based attacks. Malicious actors will more likely target election infrastructure, reporting websites or the internet. These attacks are designed to delay information such as polling results or to project political instability at critical moments. Nations have also been known to disrupt their own election process to silence the opposition.

RUSSIA

Throughout the year, Russia has experienced a number of disruptions to their election process. In May 2020, during the preliminary voting for **United Russia**, the largest political party in Russia, a **denial-of-service attack was launched against their online voting platform** preventing votes from accumulating. In June, the Russian **Central Election Commission (CEC) faced a DDoS attack** that peaked at 240,000 requests per second. The website Constitution2020.rf was the target on the first day of voting for amendments to the Russian constitution. The website contained information related to the amendments and on Russian votes. The CEC reported that the two DDoS attacks were for the purpose "**external interference**" aimed at increasing the load of the server and disrupting the flow of information during an election. Allegedly the **DDoS attacks came from the USA, United Kingdom and Ukraine**.



From the very morning, ddos attacks on the site constitution2020.rf have been recorded . Presumably from UK and Singapore

Figure 1: CEC Announcement

UKRAINE

Throughout the year, **Ukraine has also suffered from dozens of DDoS attacks aimed at election officials**. CERT-UA and other officials have registered monthly DDoS attacks that were mostly aimed at the Office of the President of Ukraine, the State Security Services and State Service for Special Communication. While it is unknown who can be attributed to the attacks, the growth and majority of DDoS attacks can likely be categorized as an attempt to project political instability in the region.

MACEDONIA

In Macedonia, **the Ministry of Interior stated that a DDoS attack was launched against the website for the State Election Commission (SEC)**. This attack was designed to prevent the publication of the results for Macedonia's preliminary election. In addition to the attack on the SEC, **DDoS attacks were also**

launched against media outlets Time.mk. The founder of Time.mk posted on Twitter that his website was targeted by 35 million IP addresses generating thousands of clicks per second.

BELARUS

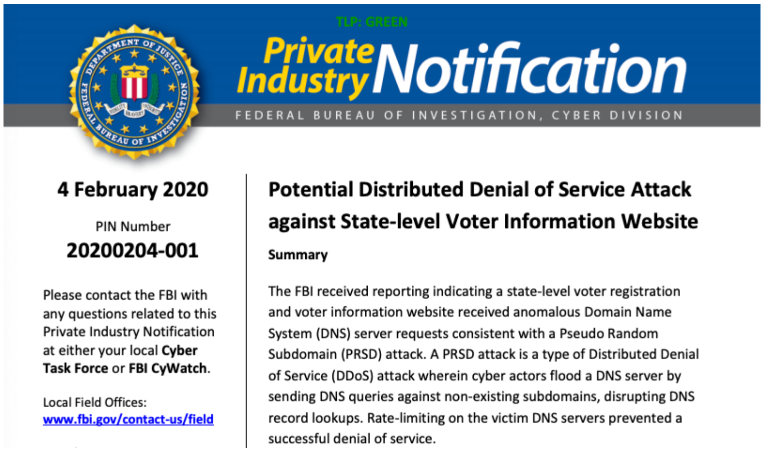
Belarus has seen political instability that lead to several country-wide outages, some attributed to denial-of-service attacks. Internet disruptions started in the evening of August 8 when the government of Belarus requested a communications lockdown per a reported source from Solon Cellular. It was also reported that a similar request was made earlier on July 19th during a campaign rally for presidential candidate, Svetlana Tikhanovskaya.

While this shutdown was labelled as a politically-motivated restriction to influence an election, the Belarus CERT explained the shutdown as a preventive measure to counter incoming DDoS attacks. These statements were ultimately confirmed by CERT.BY in August when CERT.BY reported they recorded a large wave of DDoS attacks on BY-NET, the host of the State Security Committee of the Republic of Belarus and the Ministry of Internal Affairs of the Republic of Belarus. The reported DDoS attack consisted of one-hour waves peaking at 203Gbps with attack vectors including UDP Floods, UDP Frag, ICMP, and DNS and NTP flooding.

As the polls closed in Belarus, NetBlocks reported that multiple ISPs lost routing for a duration of 61 hours. The outage impacted fixed phone lines, cellular communications and online platforms, including most of the popular social media, search engines and news sites. According to NetBlocks, the application-layer outages were due to deep packet inspection (DPI) keyword filtering, a rarely-used facility provided by network filtering devices to block internet domain names matching a predefined list of keywords. NetBlocks further reported several additional outages that coincided with rally's in support of the political opposition.

FBI PIN 20200204-001

In February, the FBI reported a potential risk for DDoS attacks against state-level voter information websites. This Private Industry Notification came after an undisclosed attack was observed. The threat specifically covers state-level voter registration and voter information websites. These websites experienced a denial-of-service attack known as a DNS Recursive Flood or Pseudo Random Subdomain Attack (PRSD). The attacks have been persistent, lasting up to a month, with attacks in two-hour intervals peaking at 200,000 DNS requests during a time span that normally would see 15,000 requests.



TLP: GREEN

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 February 2020

PIN Number

20200204-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices: www.fbi.gov/contact-us/field

Potential Distributed Denial of Service Attack against State-level Voter Information Website

Summary

The FBI received reporting indicating a state-level voter registration and voter information website received anomalous Domain Name System (DNS) server requests consistent with a Pseudo Random Subdomain (PRSD) attack. A PRSD attack is a type of Distributed Denial of Service (DDoS) attack wherein cyber actors flood a DNS server by sending DNS queries against non-existing subdomains, disrupting DNS record lookups. Rate-limiting on the victim DNS servers prevented a successful denial of service.

Figure 2: FBI PIN 20200204-001

A PRSD, also know as DNS Water Torture attack, is a sophisticated DNS Flood in which the attacker generates a distributed request flood towards DNS servers in an attempt to overload them with false requests (see Figure 2). The flood consists of randomly generated subdomains part of the target domain(s). The attacker sends crafted DNS queries to DNS recursive servers that contain a random string prepended to the victim's domain (for example, idueyai.VictimDomain.com). The recursive DNS servers will attempt to get an answer from the authoritative DNS server. Sending a continuous flood or randomly generated subdomains through several recursive DNS servers will overload the authoritative DNS server with a flood of false requests. When the authoritative DNS server is unable to respond, the recursive servers will start to retry to requests pushing the authoritative DNS server further down in an amplified flood of false requests.

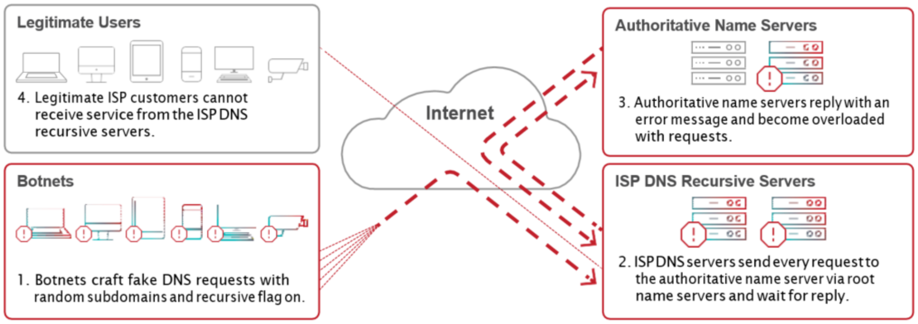

Legitimate Users
4. Legitimate ISP customers cannot receive service from the ISP DNS recursive servers.
Botnets
1. Botnets craft fake DNS requests with random subdomains and recursive flag on.
Internet
Authoritative Name Servers
3. Authoritative name servers reply with an error message and become overloaded with requests.
ISP DNS Recursive Servers
2. ISP DNS servers send every request to the authoritative name server via root name servers and wait for reply.

Figure 3: DNS recursive random-subdomain attack

Besides the authoritative server, the recursive servers are also impacted by the flood of false requests and the delay or missing responses from the authoritative server, causing the complete chain to suffer from the attack.

Radware Cybersecurity Alert

Election-Interfering Cyberattacks

September 22, 2020

The Upcoming US Election

THE UNITED STATES ELECTION

The threat landscape for the United States election has been quiet given the recent shifts in processes due to COVID-19. Recently **Microsoft disclosed attempts by Russia, China and Iran** to breach email accounts associated with the Biden and Trump campaigns. As election day approaches, tactics to influence shift from information campaigns to one of disruption and chaos. With the changes to the election process this year, it is expected that denial-of-service attacks will likely be used to disrupt polling results as the US will likely not converge in an instant and uncontested result.

REVOLUTIONS REQUIRE COMMUNICATION WHILE DDOS CAN BE THE SILENCERS

Disruptive attacks on the election process can have just as much impact on society as an disinformation campaign. The two are quite different but have the same result. In one, the actor floods users with (false) information hoping to manipulate and control the masses while the other limits or prevents information from being shared with the masses, resulting in panic and chaos. From elections to revolutions, availability of information and the ability to communicate are critical elements, and inhibitors at the same time, of political society. Those looking to silence or limit the flow of information during an election process are often the same who are attempting to interfere with the election process.

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit **DDoSWarriors.com**. Created by Radware's **Emergency Response Team (ERT),** it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.