ERT Threat Advisory
Elections in France
April 21, 2017

Abstract
As the 2017 French presidential election approaches, many are becoming worried about the possibility of cyber interference in the election process. There is concern that a cyber-attack or social manipulation like those recently seen in the 2016 United States presidential election will occur in the time leading up to the April 23rd election date.

Following recent developments in France's internal politics and the European Union (Brexit), French officials are concerned that the election might be influenced by a foreign party or state in an attempt to promote a certain candidate, and might represent an attempt to destabilize the country and the European Union.

It is likely that over the next week France could experience various cyber-attacks, including hacked social media accounts, political parties' website defacements, denial of service attacks against government institutions, and data dumps containing personal information about the candidates.

Past Events
This would not the first time cyber-attacks have been leveraged to influence an election:

1) **United Kingdom:**
   A parliamentary committee - The Public Administration and Constitutional Affairs Committee (PACAC) - said they could not rule of the possibility of a DDoS attack on Gov.uk/register-to-vote. Hours before the deadline for registrations, the website experienced a service outage as it became flooded with requests that the PACAC said was unprecedented. As a result, the deadline for registration was postponed for two days.[i] Those extra two days could result in a shift in voter demographics via social manipulation.

2) **Turkey**:
   Before the presidential elections, both Germany and the Netherlands rejected requests from Turkish officials to hold assemblies with Turkish voters in their territories[ii]. The levels of tension resulted in cyber-attacks by pro-Erdogan hackers against Dutch targets. Several twitter accounts, including Forbes[iii], were hijacked and used to callout historical stereotypes of German and Holland and linked to a pro-Erdogan video.

3) **Latin America**
   Andrés Sepúlveda was arrested in Bogota, Colombia last year and charged with hacking elections in Nicaragua, Panama, Honduras, El Salvador, Colombia, Mexico, Costa Rica, Guatemala, and Venezuela.[iv] Sepúlveda and a group of hackers manipulated elections by phishing political targets and installing spyware on their devices. They data from candidates, politicians, friends and families, and used it to manipulate the media and social media channels to influence the masses with content.

4) **Philippines**
   Before the 2016 elections, hackers compromised the election commission and leaked a voter database containing the information of 55,000,000 voters.

5) **Australia**
   The Australian Bureau of Statistics stated that widespread outages on the 2016 census website were due to four "malicious" DDoS attacks on launch day[v].

More examples of Election-Related Cyber Assaults

Reasons for Concern

Manipulating elections is an emerging threat for nations and societies. Cyber-attacks have become a very powerful tools for governments, organizations, hacktivist groups and individual hackers for hire to influence voters via simple phishing and data collection campaigns in combination with social manipulation and propaganda via social media (tweet storms).

A recent example is the alleged Russian involvement in the 2016 United States presidential election. According to a joint U.S. intelligence review, “Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election” with the “goal to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton and harm her electability and potential presidency.”

Attack Vectors

HTTP/S Flood

An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are designed to consume a significant amount of the server’s resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack’s overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

Phishing

A digital attempt to obtain sensitive information from a victim by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent out to everyone in the company or designed to specifically target key associates. Once an associate falls victim to this attack, the hacker will then have the sensitive information required to gain access to certain systems.

SQL Injection

This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database and more.

Social Engineering

A process of psychological manipulation, more commonly known as human hacking. The goal is to have the targeted victim divulge confidential information or give you unauthorized access because you have played off their natural human emotion of wanting to help or provide them with something. Most of the time the attacker’s motives are to either gather information for a future attack, to commit fraud or to gain system access for malicious activity.

Prevention:

- **Politicians** leverage social media to communicate to the masses. It is critical that these accounts are secured. They should be aware of phishing attempts.
- **Media** outlets should ensure their social media accounts also remain secure to ensure the dissemination of accurate information.
- **Telecommunication** companies have to assure connectivity, which facilitates the visibility of both political parties and the public.
- **E-voting systems** and statistical websites must be able to withstand DDoS attempts to safeguard critical information.

Effective DDoS Protection Essentials:

- **Hybrid DDoS Protection** - (on-premise + cloud) – for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan** - that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerabilities 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

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

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

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.

---

[i] https://www.publications.parliament.uk/pa/cm201617/cmselect/cmpubadm/496/49607.htm#_idTextAnchor025
[ii] http://www.cnbc.com/2017/03/15/turkey-twitter-accounts-hacked-germany-netherlands-nazis-forbes.html
[iii] http://www.redstate.com/absentee/2017/03/15/forbes-twitter-page-appears-hacked-...-turkish/
[iv] https://www.bloomberg.com/features/2016-how-to-hack-an-election/
[v] https://www.cnet.com/au/news/the-census-wasnt-hacked-but-the-abs-still-has-a-problem/