Securing the Campaign

Information security threats faced by modern political campaigns

by Ben Hagen ~ @benhagen

This article is an introduction to a talk I'll be giving at 29C3. The talk will cover threats faced modern political campaigns, relate practical advice for their mitigation, and stories from the 2012 US Presidential Campaign.

The importance of technology and online processes has exposed modern campaigns to an unprecedented number of information security threats. These security threats must be mitigated in order for a campaign to fully realize the potential of information technologies such as social media, online fundraising, and online organizing.

In the 2012 US Presidential Election the Obama campaign raised over $690 million dollars[1] from online fundraising. The Romney campaign hasn't released its fundraising totals, but their numbers are likely of a similar scale. Similarly, online organizing and communication played a major role. Both campaigns utilized such tools as online voter call tools, event management, organizing, communication, advertising, and Get-Out-The-Vote (GOTV) efforts.

This reliance on the digital world empowers campaigns to reach audiences it may not have had access to before and realise new efficiencies in communication, fundraising, and targeting. It also exposes campaigns to information security threats of a previously unknown scale. The impact of a major security attack aimed at derailing a campaign is incalculable, particularly if the attack is successful in affecting the availability or integrity of tools used during the final weeks of an election.

This article will describe both the major actors responsible for information security threats facing modern campaigns, and their targets.

Threat Actors

The main threat actors can be categorized into several broad categories:

- Organized crime
- Hacktivism
- Nation states

[1] http://www.businessweek.com/articles/2012-11-29/the-science-behind-those-obama-campaign-e-mails

- Political opponents
- Random Attacks of opportunity

Organized Crime

Modern political campaigns in the United States, and many parts of the world, generate and consume large amounts of money. An increasing amount of this money is raised via online fundraising activities and online store purchases. This volume of money, and the number of online transactions, make the campaign a target of “classic” criminal attempts at stealing monies or monetary proxies (such as credit card numbers). Organized crime is typically interested in compromising a site in order to exfiltrate financial information, or in the extortion of funds under threat of a Denial of Service. These are the same threats faced by any large eCommerce site on the web.

Hacktivism

Both the public image of political actors and the highly visible and popular web properties of political campaigns have become the target of “hacktivist” groups. The most well known hacktivist organization is the decentralized group called Anonymous. These groups typically try to deny access to a page (via DOS or DDOS attacks), deface a website with an embarrassing and/or political messages, or expose sensitive information from an organization in an attempt to discredit or embarrass the group. As with most online entities the reputation of a site’s security can impact the willingness of user’s to trust the website to protect sensitive information. Within the context of a campaign, this generally means their willingness to donate money, or use the site and its features to spread the message of the political contact.

Nation States

Political campaigns introduce an unknown quantity into foreign relations. This uncertainty makes them the target of nation state originated espionage attempts to either influence the election, or exfiltrate data from the political campaign. Nation states are interested in a variety of information regarding future economic and foreign policy decisions. During the 2008 US presidential race between Barack Obama and John McCain, both parties were reportedly infiltrated[2] by a foreign government interested in obtaining foreign policy documents. Attacks from nation states are sophisticated and hard to detect. They can generally be classified under the general “Advanced Persistent Threat” category describing sophisticated and targeted attacks which operate on a long-term scale. These attacks generally take the form of targeted phishing (spear phishing) campaign aiming to infect user machines with some sort of custom rootkit.

Political Opponents

Campaigns are contests between at least two participants. This competition inherently creates an atmosphere where biased parties may see each other as valid targets for cyber-sabotage or espionage. The impact, and subsequent publicity, of one of the major participants being discovered attacking their opponent is likely sufficient to discourage the

[2] http://www.wired.com/threatlevel/2008/11/obama-and-mccai/

major participants (political candidates and their organizations) from attempting any attack. There are, however, many political activists on both sides who will be eager to sabotage their rival whenever possible. These attacks are typically unsophisticated and will look to exploit one side's tools for the other's advantage. For example, a call-tool used to call constituents and ask for support for a candidate can be opposing activists' target for fraud. They may consume phone numbers programmatically to prevent legitimate contact, or contact numbers with a contrary message of support for the opposing candidate.

Random Attacks of Opportunity

Finally, the Internet is filled with the background noise of attacks of opportunity; where random attempts at exploiting websites or Internet addresses may unexpectedly reward someone with privileged access. These attacks are, in a general sense, blind attempts at exploiting existing vulnerabilities in widely used products, or identifying weakly configured credentials for remote access services. Once exploited, the attacker may not realise, or care, who owns the machine or what its purpose may be. They are simply interested in controlling a machine for use in a Denial of Service attack, or as a proxy for end-user exploitation. These attacks may not be directly targeted at campaign organizations, however they could impact the public's trust in a candidate and their online properties.

Threat Targets

The main threat targets of a campaign can be grouped into the following three general categories:

- Fundraising activities
- Public opinion
- Organizational, or logistical processes

Fundraising Activities

One of the most important roles of a political organization in a US election is to raise funds to support the campaign. These funds are used for a wide variety of purposes: advertising (both online and through traditional media), logistical expenses (travel, employees, etc.), field work (supporting regional and neighborhood offices), and infrastructure (online and traditional). A security event affecting a campaign's fundraising can have far reaching results both in the near and long term. A shortfall of funds can limit the reach of a campaign's ground-game or the scope with which they are able to spread a message. An example of a security event impacting online fundraising activities would be a Denial of Service of the campaigns donation website, particularly during a high-donation event or time period. This would directly impact how much money an organization receives, and hence the activities it is able to fund.

Public Opinion

The eventual goal of all campaigns is to sway public opinion in favor of a candidate. Any event resulting in a negative impact to public opinion can affect the final result of an election. The scope of US presidential elections is so large, that any security event, even a small

one, can have a negative impact on public opinion, furthermore the opportunities to subtly sway opinion through the theft and release of internal documents, or defacement of online properties and messages can have an even greater impact. An example of a security event impacting public opinion would be the defacement of a candidate's website with contrarian messaging. This would impact the trust with which constituents interacted with web properties and online fundraising.

Organizational or Logistical Processes

The political organization behind a campaign is ultimately what decides success. A security event impacting the organization's effectiveness or efficiency can have a real affect on its ability to quickly respond when needed and the efficiency with which it can utilize its resources (both in terms of manpower and money). An example of a security event impacting organizational efficiency would be a Denial of Service against an organization's email server. This would impact their ability to communicate internally and the speed with which dependant processes could operate.

Conclusion

Modern campaigns have a varied threat landscape. They are exposed to many of the threats common to online commerce organizations, but are always exposed to threats of a more political nature. Campaigns are hyper-sensitive to attacks which may impact public opinion, and require fundraising activities to operate without downtime. During key election milestones their focus shifts to organizational and logistical effectiveness. Each of these threat actors and targets must be taken into account when planning a campaigns information security strategy.