Eli Boninger

December 14, 2016

Security Final Project

The Cybersecurity of Political Campaigns

Abstract

Political campaigns are large systems, with sensitive information about thousands of donors as well as important internal information including email exchanges between candidates, staff, and advisors. Yet because of campaigns' ephemeral nature, the security of these organizations often goes overlooked and under-regulated. Campaigns are created in a hurry and then gone as soon as the election is complete, and security is not generally the largest concern. This paper will examine the security of these organizations, as well as the policies that are currently in place to regulate and moderate this form of information sharing.

Introduction

If you were a Ted Cruz or Rand Paul supporter during the 2016 Republican Presidential Primaries, you may have been surprised when you started receiving emails from the Donald Trump campaign after your preferred candidate dropped out. You were not alone. In fact, most candidates in the 2016 primaries sold voter information to other candidates' campaigns. Losing candidates can make hundreds of thousands of dollars by renting out or selling voter lists to those still in the race.[1]

[1] Pagliery, Jose. "Here's How Presidential Candidates Sell Your Personal Information." July 7, 2016

Beyond the selling of donor and supporter information, internal campaign security is too often left out of the discussion when these organizations are being created. After the Obama administration officially accused Russia for interference in the United States presidential campaign, around 2,000 emails were released on WikiLeaks, all of which were hacked from the email of John Podesta, Hillary Clinton's campaign chairman.[2] Previously, we saw in the news how the hacking of the Democratic National Committee revealed embarrassing emails eventually leading to the resignation of the committee's chairwoman. While in this paper we will not discuss the morality of these disclosures of sensitive information, we will try to shed a light on what parts of the campaign process allow such events to take place.

To The Community

Information is currency, and political campaigns are rich. As good citizens, we find our ideal candidate and then share with them all kinds of sensitive information: our emails, our credit card numbers for donations, and our addresses, among other things. This is an important part of election seasons—we want to be informed and we want to support those candidates in which we believe. We are excited, motivated to take action, and often not considering the infrastructure of these rapidly created organizations.

How were the websites built? What security risks were taken into account? What happens with the information when the campaign is over? As we move forward into the digital age and campaigns employ more and more sophisticated tactics for information gathering and consumption, it is important that we begin to consider these issues.

---

[2] Nakashima, Ellen, "U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections," October 7, 2016.

Campaigns Are Like Massive Startups

We generally think of startups as a sector of the young-person dominated tech world, imagining new technologies and applications, building new apps fast enough to beat out all of the competition, growing their values at exponential rates, and either reaching great heights or tumbling back to Earth. Compared to the scaling necessary to grow a political campaign, though, cookie-cutter Silicon Valley startups are nothing. Campaigns aim to raise many millions, if not billions, of dollars over the course of about a year and a half. They hire hundreds of employees for this short period of time, and must have enough structure and organization to give every employee a direction and sense of purpose. These teams are built almost entirely from scratch, but within this short length of time they are expected to be functioning at a level that stereotypical startups may take years to achieve.[3]

This accelerated speed is a security risk for any startup, and definitely for political campaigns as well. A quote from Brian Burch of Symantec sums it up nicely: "Startups are incredibly vulnerable to cyber attacks in their first 18 months. If a business thinks that it's too small to matter to cybercriminals, then it's fooling itself with a false sense of security."[4] Campaigns, then, are almost more valuable targets to attackers than startups—their security measures are less developed yet their scale is that of a much larger company and the material they transmit is in some cases extremely valuable. Established companies have resources available to mitigate and defend against security breaches. Startups and campaigns don't necessarily have the time or the money to achieve similar ideals.

[3] Irwin, Neil, "Why a Presidential Campaign Is the Ultimate Start-Up," October 30, 2016.
[4] Cowan, David, "Security For Startups," January 22, 2015.

In addition, security is rarely the chief concern of a startup. These organizations are focused on raising money and winning elections, and sometimes will go to any means necessary to do so.

What Current Policies Are In Place?

According to Carrie Cordero, former Director of National Security Studies at Georgetown University, cybersecurity policies for political campaigns is a regulatory "no-man's land."[5] No part of government has devoted significant attention to campaign security restrictions. This is unfortunately no different from the rest of the tech world—the policies are far behind the technological advancements, with little sign of catching up any time soon.

The majority of states will let campaigns pay for a list of all registered voters, containing additional information such as voter history, party registration, and addresses. In some states, such as Minnesota, this list can cost as little as $46; in others it can cost as much as $2,000. There are policies in place that require campaigns to keep especially sensitive information, such as social security numbers, private.[6] However, requiring information be kept private is vastly different from actually keeping it private. Who is to say what in technology is actually considered private? Who will vet the security credentials of campaign staff, and who will perform penetration testing on their code to search for holes and weaknesses?

In the event that the security of a campaign is breached, the campaign is required to notify all parties involved.[7]

---

[5] Cordero, Carrie, "Political Campaigns and Cybersecurity Risk," July 27, 2016.
[6] Maass, Dave, "Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election," February 29, 2016.
[7] Ibid.

Often, Data Is Stored By Private Contractors

Private companies such as NGP VAN and NationBuilder are generally hired to stored data for political campaigns. However, the fact that multiple campaigns may use the same contractor allows for issues such as the NGP VAN debacle during the Democratic Presidential Primary.

Because NGP VAN ran a software patch that unintendedly allowed clients to access data from other campaigns, the Bernie Sanders campaign was given the ability to view critical voter information from Clinton's databases. After the Sanders campaign's actions were revealed, the Democratic National Committee was then able to temporarily bar the Sanders campaign from accessing its own information stores.[8]

This incident reveals multiple flaws in the system. First of all, when multiple campaigns use the same private contractor, all that is required to betray large amounts of information is one glitch in the system. Better to force campaigns to spread out their information than risk one bug causing a larger meltdown.

In addition, there are three parties involved in this story: the Sanders campaign, the Clinton campaign, and the Democratic Party, and it seems as though every single party involved had access to these databases. The issue in this case was the structure of the storage.

During elections, the DNC owns and maintains a large vat of voter data that each campaign can update and extend.[9] Because the DNC was chief owner of the database, they were able to completely block the Sanders campaign from all of its information, including its own additions and insights. However, if a campaign is generating data on its own, it should be the

[8] Arnsdorf, Isaac, and Darren Samuelsohn, "Data Breach Exposes Democrats' Vulnerability," December 18, 2015.
[9] Ibid.

only campaign with admin access to those tables. The rule of "least privilege" is one way to look at this handling this issue. Give each party involved the lowest possible access rights that still allow them to do what they need to do.

All of this being said, it certainly seems safer for campaigns to hire contractors that specialize in data storage than to hurriedly roll their own database modules in a limited amount of time.

Action Items

A campaign can be trusted about as much as a startup can be trusted, which is to say, it isn't a great idea to give them information you really care about.

If you want to give money, see if the website will let you use an external service such as PayPal. Never let a campaign store your credit card information.

If you don't want to start getting emails from other candidates once yours drops out, it's better not to give your email in the first place. Ted Cruz's last email sent to his subscribers had the headline, "What I really think about Donald." The content of the email, as you can imagine, was not flattering, calling Donald Trump a "pathological liar."[10] Fifteen days after this email was sent, Cruz donors got an email from the Trump campaign. This is something all email subscribers should expect to experience when signing on to a campaign's mailing list.

Ultimately, the best thing we can do as voters is to be careful and to stay informed.

[10] Pagliery.

Conclusion

Some progress has already been made on the campaign security front. Donna Brazile, the new DNC chairwoman, suggests changes are on their way, saying, "[The DNC] has brought in the best cyber security team in this country."[11] If there is a positive to take from the DNC hack, it is that it has brought light to the issue and has allowed the new chairwoman to address it directly.

NGP VAN was able to isolate and correct the bug in their system. They released a blog post concerning their steps moving forward: "…we are adding to our safeguards around these issues. We have thousands of automated tests and extensive code review and release procedures in place to prevent these types of issues…"[12] This statement, if anything, shows the imperfect nature of software development. Even with thousands of automated tests and various forms of code review in place, buggy code can still be rolled into production.

Campaigns will always be structured similar to startups—any organization built in such a small period of time is bound to have flaws. In my opinion, the best way to combat these inherent flaws is to do as much contracting as possible. Let the experts handle what they can, and use tools that have been designed and updated with security in mind.

Too often, it seems, issues of security are ignored until some event or another "brings that issue to the light." If I can preach one thing other than mindfulness, it would be activity. Do your best to make others aware. As more and more fields of work are beginning to have technological fronts, it becomes more and more important that the general public is informed. We must do our best to spread this knowledge.

---

[11] Scott, Eugene, "Brazile to Trump: 'Call Me' over Russia Hack," September 27, 2016.
[12] Trevelyan, Stu, "Data Security and Privacy," December 18, 2015.

Works Cited

Arnsdorf, Isaac, and Darren Samuelsohn. "Data Breach Exposes Democrats' Vulnerability." *POLITICO*. Politico LLC, 18 Dec. 2015. Web. 30 Oct. 2016.

Cordero, Carrie. "Political Campaigns and Cybersecurity Risk." *Lawfare*. The Lawfare Institute, 27 July 2016. Web. 10 Dec. 2016.

Cowan, David. "Security For Startups." *TechCrunch*. AOL Inc., 22 Jan. 2015. Web. 10 Dec. 2016.

Irwin, Neil. "Why a Presidential Campaign Is the Ultimate Start-Up." *The New York Times*. The New York Times, 4 June 2015. Web. 30 Oct. 2016.

Maass, Dave. "Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election." *Electronic Frontier Foundation*. N.p., 29 Feb. 2016. Web. 30 Oct. 2016.

Nakashima, Ellen. "U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections." *The Washington Post*. WP Company, 7 Oct. 2016. Web. 10 Dec. 2016.

Pagliery, Jose. "Here's How Presidential Candidates Sell Your Personal Information." *CNNMoney*. Cable News Network, 7 July 2016. Web. 30 Oct. 2016.

Scott, Eugene. "Brazile to Trump: 'Call Me' over Russia Hack." *CNN*. Cable News Network, 27 Sept. 2016. Web. 12 Dec. 2016.

Trevelyan, Stu. "Data Security and Privacy." *NGP VAN*. NGP VAN, 18 Dec. 2015. Web. 12 Dec. 2016.