High-Tech Campaigns Face New Security Risks

Adam Stone | June 29, 2012

How can cybersecurity issues bite a political campaign in the tail? Just ask Newt.

In late 2011, as the primaries picked up steam, a Democratic political action committee (PAC) bought the rights to newtgingrich.com and used it to send up a series of cutting spoofs. (The candidate's real site is newt.org.) The site redirected to high-end jewelry company Tiffany's (where Gingrich had a $500,000 line of credit), to mortgage lender Freddie Mac (where he had a lucrative consulting contract), and to a range of unflattering articles. The PAC, called American Bridge, even offered to sell the site to the highest bidder, saying it couldn't give it away for fear of its members being branded socialists.

How did this happen? The Gingrich team simply failed to renew the domain when its license expired, and the PAC snapped it up. The saga of newtgingrich.com highlights an emerging issue on the campaign trail. As candidates rely more on blogs, social

media and online campaign contributions, their IT teams are under mounting pressure to ensure that all cyberconnections are locked down.

To understand the digital threats to political campaigns, it first helps to understand what factors come together to make candidates — and their platforms and messages — such tempting targets.

First, there's the money. Campaigns have become adept at collecting contributions online, a practice that has grown considerably from just a few campaign cycles back. At the same time, IT managers have zealously built up databases of past donors who can potentially be tapped as future needs arise, along with their credit card information.

This combination of more online giving and rich databases full of donor names and financial information makes a tempting target for phishing or direct exploitation of stockpiled credit card data.

Even more enticing than money is power, said Ed Skoudis, SANS Institute senior instructor and cybersecurity expert. "This is how the electorate makes its decisions, how leaders are selected, so if you wanted to sway the electorate or public policy, one way to do that is by manipulating elections," he said. "I can take small actions to have big effects. I just have to type in a few key strokes. It's high profile, it has built-in publicity. There are all kinds of press. So if you want to make a splash, this is a great opportunity."

One more element? How about road rage? Some candidates speak out against hackers, propose new cybersafeguards, or question present practice in Internet usage. They want to change the rules of the road. "And some people don't want those rules of the road changed. They don't want any rules of the road," Skoudis said. Candidates who cross the hacker group Anonymous and similar organizations risk cyberwrath.

With these and other motivations looming, cyberattacks against candidates can come in many forms.

Pick Your Poison

At security provider McAfee, Vice President of Government Relations Tom Gann said the most dangerous attacks can be those that target players within the campaign itself. Called an "advanced persistent threat," this sort of highly strategic initiative opens a back channel into the inner workings of a campaign.

The attacker typically emails a campaign worker; launches an attack from within the email; and effectively sets up a pipe directly into the campaign through which to collect information on vulnerabilities, messaging and other key elements of the opposing team's strategy.

Denial of service (DOS) also is a significant peril. "Maybe all you need to do is just shut the systems down in those last days of the campaign," Gann said. DOS can cut off cash flow or squelch information at critical moments.

Denial of service (DOS) also is a significant peril. "Maybe all you need to do is just shut the systems down in those last days of the campaign," Gann said. DOS can cut off cash flow or squelch information at critical moments.

This sets campaign security apart from its corporate counterpart. “If an e-commerce site is offline for a few hours, they can recover, unless it’s right before Christmas,” said Jeremy Epstein, a computer security researcher at SRI International and technical adviser to nonprofit lobbying organization Common Cause. “ If a campaign site is offline at critical junctures — right before the election, right before contribution deadlines — the impact could be much worse,” he said.

While a DOS attack can interrupt the information flow, an equally dangerous exploit would be to radically deface information, by invading blogs, for instance, or by infiltrating a Web page.

“Campaigns face the threat of having false messages injected into the media by hackers,” said Lt. Gen. Harry Raduege Jr., chairman of the Deloitte Center for Cyber Innovation and a former director within the U.S. Defense Department. “Before the error is caught, significant damage can occur, which then escalates into valuable time being expended to supply correct messaging across multiple media sources and in trying to reverse negative impressions and perceptions.”

Such false messaging falls under the general heading of hacktivism, a broad term that refers to the use of illicit cyberstrategies to advance political ends. This is perhaps the most dangerous threat when it comes to political campaigns, because hacktivism doesn’t just disrupt money or messaging. It threatens the very system.

“To the degree that actors in a democracy start using cyberattacks to further political ends, it pollutes the kind of civil society we are supposed to be seeking,” said McAfee’s Gann.

Emerging Threats

Perilous as it may be, hacktivism also is the most visible among the evolving cyberthreats posed to political campaigns.

“Four years ago, we didn’t have nearly as much of this as we have seen in the last year,” Skoudis said. “Anonymous has shown that you can get a lot of press doing these things. You can achieve real goals here.”

Since the last election cycle, campaigns’ growing reliance on online donations has opened a new avenue for those seeking personal gain. Blogs and social media create new opportunities for attacking content, while sophisticated infiltration tools are making it possible for invaders to gain greater access to inside information culled from campaign servers.

As in the corporate world, campaigns also have come to rely more on mobile devices, thus opening up systems to a range of potential threats.

Before considering the options when it comes to prevention and remediation, it’s important to consider one further element that separates a campaign’s cyberneeds from those faced by users in the corporate world.

While no one in the world of IT would choose to dawdle in the face of a cyberbreach, speed is an even greater consideration in the realm of political campaigns. Campaigns happen in real time, unfolding not only in a matter of days but sometimes hours.

Think about candidates like Herman Cain or Rick Santorum, who came from nowhere to become leading candidates in the span of a week or so, Epstein said. “Suddenly their websites became high-profile targets — but without months and an appropriate budget to plan for it.”

Against this backdrop, careful planning and speedy remediation become critical elements of any cyberstrategy.

Building the Bulwarks

Campaign security begins at the level of policy, said Mark Patton, general manager of the security business unit at GFI Software.

Candidates and senior staff “need to set the tone for Web policies in the office and on the road to make it clear that IT and Web security are priorities of running a successful campaign,” Patton said. “Policies need to be created, socialized, approved and supported from the highest levels of the campaign. Make them official and discuss them often for them to hold weight, especially amongst an environment of nonpermanent staff.”

Such policies should address the fundamentals of security: acceptable use, Internet access, email and communications, and network security. Of special concern is the emerging realm of BYOD, or bring your own device, with risks including patching, operating system vulnerabilities and lack of local protection. “In many cases with personal devices, the employee or volunteer can walk out the door with it because it’s their device, and it may contain sensitive or proprietary information that is not adequately protected,” Patton said.

At Solera Networks Research Labs, Director of Threat Research Andrew Brandt takes this one step further. Beyond policies limiting or governing BYOD, he recommends that campaigns ban all forms of small removable media drives. “They are too easily lost, capable of holding large amounts of data, and the temptation to put sensitive information on them can be great at times,” he said.

Brandt also advises full-disk encryption on all campaign laptop hard drives, in addition to recommending that IT makes a secure, patched baseline image for all campaign computers, and then reimages those computers at least every couple of weeks. “It might be a hardship, especially because it will require campaigns to update the drive images frequently to account for software and operating system updates, but this is an easy way to prevent malware infections from persisting on a campaign computer,” he said. This rule is doubly necessary for the candidate and for his or her family’s personal laptops.

In an even more direct defensive action, Brandt said it makes sense to take campaign assets out of the most obvious line of fire. Most attacks today are directed at Windows systems, generally because of the ubiquity of these systems. To minimize the risk, put everyone on Linux or Mac. That’s one whole front shut down.

Candidates also can take a cue from the corporate world by protecting their online reputation through strategic domain acquisition. (Just ask Gingrich.) Beyond the dot-com, dot-org and dot-net options, it makes sense to snap up not just BobSmith but also BobSmithforPresident and related domains. And a little defense goes a long way. Consider disney-sucks.com, allstateinsurancesucks.com and oreilly-sucks.com. Bob Smith might do well to buy dot-suck pre-emptively.

When it comes to safeguarding critical campaign information in the cybersphere, the safest approach may be simply to keep it out of the cybersphere altogether. “There may be some documents you don’t want to put in digital format,” Gann said. “You might not want to put your most recent internal poll results in digital format, or maybe you have other key strategy documents. These are judgment calls, but that’s where being aware of the threat landscape becomes so important.”

In spite of safeguards, breaches will occur. When it comes to remediation, the expert consensus is clear: Come clean quickly and thoroughly.

“The first step if faced with some sort of cyberattack is to call in IT security pros to make sure that the hole is closed,” Patton said. “The second step should be to notify whoever has been breached — whether they be donors, agencies, supporters. Be apologetic and forthright, and explain how the issue is being remediated. Time and again, breached organizations wait too long to notify affected customers and stakeholders. Inform anyone who may be impacted immediately. It’s the right thing to do.”

Meanwhile, there’s former candidate Gingrich and his newtgingrich.com problem.

Gingrich had options. He could have filed a domain name complaint based on the Uniform Domain-Name Dispute Resolution Policy, but victory was by no means assured. He’d have had to prove that the PAC was using the name in bad faith, while the PAC could have claimed it was broadcasting legitimate political satire. All that would have taken time.

Instead, the candidate let things stand. As the campaign wound up, the website was still redirecting to shouldnewtgingrichdropout.com, which delivered a great big “Yes” midscreen along with Facebook, Twitter and email buttons for those wanting to share that sentiment.

Gingrich lost. Did the domain grab sway voters? There’s no easy way to tell. But it’s a fair bet the spoof did not help.

http://www.govtech.com/e-government/High-Tech-Campaigns-Face-New-Security-Risks.html