

CYBERCRIME AND THE ELECTORAL SYSTEM

Oliver Friedrichs

This manuscript is a draft of a chapter that will appear in the forthcoming book “Crimeware” edited by Markus Jakobsson and Zulfikar Ramzan (to be published by Symantec Press and Addison-Wesley Professional).

While we first saw the Internet used extensively during the 2004 Presidential election, its use in future presidential elections will clearly overshadow it. It is important to understand the associated risks as political candidates increasingly turn to the Internet to more effectively communicate their positions, rally supporters, and seek to sway critics. These risks include among others the dissemination of misinformation, fraud, phishing, malicious code, and the invasion of privacy. Some of these attacks, including those involving the diversion of online campaign donations have the potential to threaten voters' faith in our electoral system.

Our analysis in this chapter focuses on the 2008 presidential election in order to demonstrate the risks involved, however our findings may just as well apply to any future election. We will show that many of the same risks that we have grown accustomed to on the Internet can also manifest themselves when applied to the election process.

It is not difficult for one to conceive numerous attacks that may present themselves which may, to varying degrees, impact the election process. One need only examine attack vectors that already affect consumers and enterprises today in order to apply them to this process. In this chapter we have chosen to analyze those attack vectors that would be most likely to have an immediate and material affect on an election, affecting voters, candidates, or campaign officials.

A number of past studies have discussed a broad spectrum of election fraud such as the casting of fraudulent votes [24] and the security, risks, and challenges of electronic voting [18]. There are many serious and important risks to consider related to the security of the voting process, and the new breed of electronic voting machines that have been documented by others [1]. Risks include the ability for attackers or insiders to either manipulate these machines or to alter and tamper with the end results. These concerns apply not only to electronic voting in the United States, but have also been raised by other countries, such as the United Kingdom, which is also investigating and raising similar concerns surrounding electronic voting [26]. Rather than revisit the subject of electronic voting, our discussion will focus exclusively on Internet-borne threats, and how they have the potential to impact the election process leading up to voting day.

In this chapter we will first discuss domain name abuse, including typo squatting and domain speculation as it relates to candidate Internet domains. Secondly, we will discuss the potential impact of Phishing on an election. Thirdly, we will discuss the impact of security risks and malicious code, and the potential for misinformation that may present itself using any of these vectors. Finally, we will also review how phishers may use spoofed

political emails (such as false campaign contribution requests) instead of spoofed emails appearing to come from financial institutions. The goal in such attacks might still be to collect payment credentials, in which case the political aspect is just a new guise. However, political phishing emails may also be used to sow fear among potential contributors and make them less willing to contribute online — whether to spoofed campaigns or real ones.

These set of risks cross technical, social, and psychological boundaries. While traditional forms of malicious code certainly play an important role, social engineering and deception provide equal potential and have a more ominous psychological impact on voters who are exercising their right to elect their next president, or cast their vote in any other type of election.

This chapter consists of a combination of active research conducted by the author as well as discussion on how current threats may be customized. In order to determine the impact of typo squatting and domain name speculation for example, we performed an analysis of 2008 presidential election candidate web sites and discovered numerous examples of abuse.

When examining the attacks that we discuss in this chapter, we believe and hope that candidates and their campaigns are unlikely to knowingly participate in or to support, these activities themselves. For one, it would not be acting in good faith, and secondly, their actions would in many cases be considered a breach of either existing computer crime or federal election law¹.

We conclude that perpetrators would likely fall into two categories; those with political motives and those seeking to profit from these attacks. In the end it may be difficult to identify from a given attack which one of these is the true motive.

10.1 Domain Name Abuse

In order to communicate with constituents and supporters, candidates have created and maintain web sites, identified by and navigated to via their registered domain names. All candidates for the 2008 federal election have registered, or already own, a unique domain name that is used in order to host their respective web site. In all cases this is a domain name that incorporates their own name in some capacity, and in some cases has been registered specifically in support of the 2008 campaign. Domain names play one of the most important roles in accessing a web site. They are the core

¹U.S. Code Title 18, Part I, Chapter 29. Available from: http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000594----000-.html

part of the URL that is recognized by the general population, and as such, their ownership dictates who can display content to users visiting web sites hosted on that domain name.

While users may well know the URL to their bank or favorite commerce site, voters may not readily know the URL to their political party, or their chosen candidate's web site. Legitimate sounding domain names may not be as they appear. The authors of this book for example, were able to freely register domain names such as `http://www.democratic-party.us` and `http://www.support-gop.org` that have for some time warned visitors about the risks presented by phishing. It would be easy to use a domain name of this type for the purposes of phishing or crimeware installation. Consider, for example, an email pointing to one of these domains, that contains text suggesting it came from the Democratic Party asking the recipient to contribute. If willing to do so, the recipient may be offered to choose a variety of payment methods, each one of which would allow the phisher to potentially capture the user's credentials as he enters these on the site (or on another, suitably named site hyperlinked from the donation page). The email may also offer the email recipient to download and access resources, such as campaign movies, which may then contain malware. An example of how existing movies can be modified to incorporate malware was given in [37]. This study also found that typical Internet users are very susceptible to attacks in which self-signed certificates are vouching for the security of executables as long as a person known to them has also indicated that the material is safe. In the case of [37] that known person was a friend, but in our hypothetical case, it may be a political party or a politician.

In today's online environment, individuals and businesses must consider a number of risks from individuals attempting to abuse the domain name system. These involve domain speculators, bulk domain name parkers, and typo squatters.

10.1.1 Background

Since the early days of Internet commerce, Internet Domain Names have held an intrinsic value, much as real-estate in the physical world has for centuries. In the early 1990's when relatively few .COM domain names existed it was highly probable that if one attempted to acquire the name of a well-known company, individual, or trademark that this name would be available to them. As a result, many early domain name speculators did, in fact, acquire such domain names, in many cases to sell them to the legitimate trademark holder for a profit. At that point in time, the legal precedence for domain

name disputes had not yet been set, and the speculator had a chance of profiting from this sale, in particular if it was to a well known and thus well-funded corporation.

It was only a matter of time before formal dispute guidelines were created in order to eliminate such infringement. A formal policy was created by ICANN in 1999 and is known as the Uniform Domain Name Dispute Resolution Policy [16]. Known in short as the UDRP, it is implemented in practice by the World Intellectual Property Organization's (WIPO) Arbitration and Mediation Center.

While this policy provides a framework for resolving infringement, it does not preclude the registration of an infringing domain name if that domain name is unregistered. What is in place is a policy and framework for the legitimate trademark owner to become the owner of the domain granted they first become aware of the infringing domain's existence. The policy is frequently used by legitimate business trademark holders in order to protect their names².

While used to protect trademarked proper names, the policy also applies to unregistered, or "common law" marks, including well known individual's proper names, even when a formal trademark does not exist. Julia Roberts, for example, was able to obtain ownership of the juliaroberts.com domain name, even in the absence of a registered trademark³. This is common when a domain name is specific enough and matches a full proper name. In other examples, such as the more general domain name sting.com, contested by the well known singer Sting, the transfer was not granted and the original registrant retained ownership⁴.

There appear to be very few cases in which either elected or hopeful political candidates have disputed the ownership of an infringing domain name. One example that does exist is for the domain name kennedytownsend.com and several variations thereof. Disputed by Kathleen Kennedy Townsend, Lieutenant Governor of the State of Maryland at the time, the transfer was not granted, based predominantly on what appears to be a technicality of how the dispute was submitted⁵. Central to the ruling in such dispute cases

²The Coca-Cola Company v. Spider Webs Ltd. <http://www.arb-forum.com/domains/decisions/102459.htm>.

³Julia Fiona Roberts v. Russell Boyd. <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html>.

⁴Gordon Sumner, p/k/a Sting v Michael Urvan. <http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0596.html>

⁵Kathleen Kennedy Townsend v. B.G. Birt. <http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0030.html>

is whether or not the trademark or name is used in order to conduct commercial activity, and thus whether the infringement negatively impacts the legitimate owner and as a result, consumers:

Here, the claim for the domain names is brought by the individual politician, and not by the political action committee actively engaged in the raising of funds and promotion of Complainant's possible campaign. Had the claim been brought in the name of the Friends of Kathleen Kennedy Townsend, the result might well have been different. But it was not. The Panel finds that the protection of an individual politician's name, no matter how famous, is outside the scope of the Policy since it is not connected with commercial exploitation as set out in the Second WIPO Report.

Within the United States, trademark owners and individuals are further protected by the Anticybersquatting Consumer Protection Act which took effect on November 29, 1999⁶. The ACPA provides a legal remedy in order for the legitimate trademark owner to seek monetary damages in addition to the domain name, whereas the UDRP only provides for recovery of the domain name itself.

Even today, the relatively low cost involved in registering a domain name (under \$10 per year) continues to provide an opportunity for an individual to profit by acquiring and selling domain names. The relative scarcity of simple, recognizable 'core' domain names has resulted in the creation of a significant after-market for those domain names, as well as the creation of a substantial amount of wealth for some speculators [36]. Today, a number of online sites and auctions exist explicitly to facilitate the resale of domain names.

In addition to domain name speculation for the purpose of its future sale, many speculators also seek to benefit from advertising revenue that can be garnered during their ownership of the domain name. These individuals, and more recently for-profit companies such as iREIT⁷, may register, acquire and own hundreds of thousands to millions of domain names explicitly for this purpose. These domains display advertisements that are, in many cases, related to the domain name itself, and receive an appropriate share of the advertising revenue much like any web site participating in CPM, CPC, or CPA⁸ advertising campaigns.

⁶Anticybersquatting Consumer Protection Act. <http://thomas.loc.gov/cgi-bin/query/z?c106:S.1255.IS:=>

⁷Internet REIT. <http://www.ireit.com/>

⁸See chapter ?? for a description of the terms CPM, CPC, and CPA together with a

10.1.2 Domain Speculation and Typo Squatting in the 2008 Federal Election

Typo squatting seeks to benefit from a mistake made by the user when entering a URL directly into their web browser's address bar. An errant keystroke can easily result in the user entering a domain name that differs from the one that they intended. Typo squatters seek to benefit from these common mistakes by registering domain names that correspond to common typos. Whereas in the past, users making typos were most likely to receive an error indicating that the site could not be found, today they are likely to be directed to a different web site. In many cases this site may host advertisements; however the potential for more sinister behavior also presents itself.

In order to determine the current level of domain name speculation and typo squatting in the 2008 federal election we performed an analysis of well-known candidate domain names in order to seek out domain speculators and typo squatters.

To begin our analysis, we identified all candidates who had registered financial reports with the Federal Election Commission for the quarter ending March 31st, 2007⁹. This resulted in a total of 19 candidates who had submitted such filings. Next, we identified each candidate's primary campaign web site through the use of popular search engines and correlated our findings with additional online resources to confirm their accuracy. This in turn gave us the primary registered domain name upon which the candidate's web site is hosted.

In order to simplify our analysis, we removed domains that were not registered under the .COM top level domain. This resulted in the removal of two candidates who had domains registered under the .US top level domain. Our decision to focus on the .COM top level domain was driven by no other reason than our ability to access a complete database of .COM registrants at the time of our research. Our final list of candidate web sites, and their resulting domains appeared in table 10.1.

Once we had identified the set of candidate domain names, we conducted two tests in order to examine current domain name registration data. Firstly, we conducted a test in order to determine how widespread the behavior of typo squatting was on each candidate's domain. Secondly, we examined domain name registration data in order to identify cousin domain names [19].

discussion of Internet advertising.

⁹FEC Filing from Prospective 2008 Presidential Campaigns.
<http://query.nictusa.com/pres/2007/Q1>

Joe Biden (Democrat)	http://www.joebiden.com
Sam Brownback (Republican)	http://www.brownback.com
Hillary Clinton (Democrat)	http://www.hillaryclinton.com
John Cox (Republican)	http://www.cox2008.com
Christopher Dodd (Democrat)	http://www.chrisdodd.com
John Edwards (Democrat)	http://www.johnedwards.com
James Gilmore (Republican)	http://www.gilmoreforpresident.com
Rudy Giuliani (Republican)	http://www.joinrudy2008.com
Mike Huckabee (Republican)	http://www.mikehuckabee.com
Duncun Hunter (Republican)	http://www.gohunter08.com
John McCain (Republican)	http://www.johnmccain.com
Barack Obama (Democrat)	http://www.barackobama.com
Ron Paul (Republican)	http://www.ronpaul2008.com
Bill Richardson (Democrat)	http://www.richardsonforpresident.com
Mitt Romney (Republican)	http://www.mittromney.com
Tom Tancredo (Republican)	http://www.teamtancredo.com
Tommy Thompson (Republican)	http://www.tommy2008.com

Table 10.1. The final candidate web site list, together with the domain names.

For our search, we define a cousin domain name as one that contains the candidate domain name in its entirety, with additional words either prefixed or appended to, the candidate domain name. In this context we would consider domain names such as **presidentbarackobama.com** or **presidentmittromney.com** as a cousin domain name from the candidates' core domain names of **barackobama.com** and **mittromney.com** respectively. One can also define a cousin name more loosely as a name that semantically or psychologically aims at being confused with another domain name. In this sense, `www.thompson-for-president.com` should be considered a cousin name domain of `www.tommy2008.com`, in spite of the fact that they do not share the same core. For the sake of simplicity, we did not examine cousin domains that are not fully inclusive of the original core domain name.

In order to generate typo domain names we created two applications, `typo_gen` and `typo_lookup`. The `typo_gen` application allowed us to generate typo domain names based on five common mistakes that are made when entering a URL into the web browser address bar [41]. These include:

Missing the first '.' delimiter:	<code>wwwmittromney.com</code>
Missing a character in the name (t):	<code>www.mitromney.com</code>
Hitting a surrounding character (r):	<code>www.mitrrromney.com</code>
Adding an additional character (t):	<code>www.mittttromney.com</code>
Reversing two characters (im):	<code>www.imttromney.com</code>

As a result of these mistakes, the potential number of typos grows in proportion to the length of the domain name itself. The sheer number of typos for even a short domain name can be large. It is rare to find that an organization has registered all potential variations of their domain name in order to adequately protect itself. Typo squatters take advantage of this, in order to drive additional traffic to their own web properties.

Our second application, `typo_lookup`, accepts a list of domain names as input and then performs two queries in order to determine whether that domain name has been registered. First, a DNS look up is performed to determine whether the domain resolves via the Domain Name System. Secondly, a WHOIS look up is performed in order to identify the registered owner of the domain.

For the purposes of our analysis, we consider a domain to be typo squatted if it has been registered in bad faith by someone other than the legitimate owner of the primary source domain name. We have visited those web sites for which typos currently exist and confirmed that they were in fact registered in bad faith. We have filtered out those that directed the visitor to the

legitimate campaign web site as well as those owned by legitimate entities whose name happens to also match the typo domain.

Our second test involved the analysis of domain registration data to identify *cousin* domain names. In order to perform our analysis we obtained a snapshot of all registered domains in the .COM top level domain during the month of June, 2007. We performed a simple text search of this data set in order to cull out all matching domains.

There are additional techniques that could be used to generate related domain names that we have not examined during our research. This may include variations on a candidates name (*christopher* instead of *chris*), variations including only a candidate surname (*clinton2008.com*), and the introduction of hyphens into names (*mitt-romney.com*). In addition, a number of typos can be combined to create even more variations on a give domain name; although it is also less likely for an end-user to visit such a domain name as the number of mistakes increases. Nevertheless, such domain names can be very effective in phishing emails, since the delivery of the malicious information relies on spamming in these cases, and not on misspellings made by users.

Expanding our search criteria in the future may result in the discovery of an even larger number of related domains. It also has the side effect of increasing our False Positive rate, or the discovery of domains that appear related, but may in fact be legitimate web sites used for other purposes. In addition, the amount of manual analysis required in order to filter out such False Positives further forced us to limit our search. You will find our results in tables 10.2 and 10.3.

We can draw two clear conclusions from the results of our analysis. Firstly, we can see that a large number of both typo and cousin domain names have been registered by parties other than the candidate's own campaign. In analyzing our results, we find that many of the registered web sites, both in the typo squatting case as well as the cousin domain name case are registered for the purpose of driving traffic to advertising web sites.

Secondly, we see that candidates have not done a good job at protecting themselves by proactively registering typo domains to eliminate potential abuse. In fact, we were only able to find one single typo web site that had been registered by a candidate's campaign - <http://www.mittromny.com>. All other typo domains were owned by other third parties that appeared unrelated to the candidate's campaign.

One observation that we made is that many of the typo domains that display contextual advertisements, are in fact displaying advertisements that point back to a candidate's legitimate campaign web site. This is best

Domain Name	Registered Typo Domains	Example
barackobama.com	52 out of 160	narackobama.com
brownback.com	0 out of 134	
chrisdodd.com	14 out of 145	chrisdod.com
cox2008.com	3 out of 92	fox2008.com
gilmoreforpresident.com	0 out of 276	
gohunter08.com	1 out of 150	ohunter08.com
hillaryclinton.com	58 out of 191	hillaryclingon.com
joebiden.com	15 out of 125	jobiden.com
johnedwards.com	34 out of 170	hohnedwards.com
johnmccain.com	20 out of 137	jhmccain.com
joinrudy2008.com	9 out of 173	jionrudy2008.com
mikehuckabee.com	3 out of 167	mikehukabee.com
mittromney.com	18 out of 123	muttromney.com
richardsonforpresident.com	2 out of 340	richardsonforpresiden.com
ronpaul2008.com	11 out of 143	ronpaul20008.com
teamtancredo.com	1 out of 170	teamtrancredo.com
tommy2008.com	1 out of 107	tommyt2008.com

Table 10.2. Typo squatting analysis results. Many typo domain names were already registered and being used in bad faith. Campaigns have also not taken proactive measures in order to protect themselves which is evidenced by the number of available typo domain names. Note that all domains and examples are in the .COM top level domain.

Domain Name	Registered Cousin Domains	Example
barackobama.com	337	notbarackobama.com
brownback.com	152	runagainstbrownback.com
chrisdodd.com	21	chrisdoddforpresident.com
cox2008.com	50	johncox2008.com
gilmoreforpresident.com	20	jimgilmore2008.com
gohunter08.com	23	stopduncanhunter.com
hillaryclinton.com	566	blamehillaryclinton.com
joebiden.com	43	firejoebiden.com
johndwards.com	190	goawayjohndwards.com
johnmccain.com	173	nojohnmccain.com
joinrudy2008.com	123	dontjoinrudy2008.com
mikehuckabee.com	28	whymikehuckabee.com
mittromney.com	170	donttrustmittromney.com
richardsonforpresident.com	69	nobillrichardson.com
ronpaul2008.com	276	whynotronpaul.com
teamtancredo.com	16	whytomtancredo.com
tommy2008.com	30	nottommythompson.com

Table 10.3. Cousin domain name analysis results. A large number of cousin domain names were registered, both in support of a candidate, and in many cases, to detract from a candidate. Note that all domains and examples are in the .COM top level domain.



Figure 10.1. When we visited <http://www.barackobams.com>, a typo of Barack Obama's web site, <http://www.barackobama.com>, it contained advertisements pointing to the candidate's legitimate campaign site.

demonstrated in Figure 10.1. In cases such as this, a typo squatter has taken over the misspelling of a candidate's domain name and is able to profit from it. Worse, however, is that the candidate is paying to have their ads displayed on the typo squatter's web site! This is a result of the way in which ad syndication on the Internet works.

Ad syndicates display advertisements on a web site by indexing its content, and displaying advertisements that apply to that content. They may also look at the domain name itself, and display advertisements for matching keywords in the domain name. As a result, advertisements for the legitimate campaign may be displayed on a typo squatter's web site. When

a user mistypes the website name and browses to the typo domain, he is presented with an advertisement for the legitimate campaign's web site. If he clicks on this advertisement, the ad syndicate generates a profit, giving a portion to the typo squatter for generating the click-through, and charging the advertiser, who is in this case the legitimate campaign¹⁰.

Individuals who register cousin domain names may have similar motives to those of typo squatters, however they may also be speculating on the value of the domain name itself, with the intent to resell it at a later date. It is also possible that they intend to use the domain to defraud people, or to make people wary of emails purportedly from a given candidate.

In our analysis we can see that it is likely that the majority of the identified domains, both in the typo and the cousin case, have been acquired in bulk, for the explicit purpose of driving traffic to advertisements. As a result, many of these domains have been parked with companies that provide a framework for domain name owners to profit from the traffic that their web sites receive.

10.1.3 Domain Parking

Typo squatters and domain name speculators need not host the physical Web infrastructure required to display their own web content, or to host their advertisements. The domain name owners can rely on domain parking companies that will happily do this for them, for an appropriate share of the advertising revenue. Domain name parking companies will provide the required web site as well as leverage their pre-established relationships with advertising providers in order to make life as simple as possible for domain name owners. In order to leverage a domain name parker, the domain name owner need only configure his domain's primary and secondary DNS server to that of the domain parker. This makes the acquisition and profit from the ownership of a domain name even simpler, to the extent that an individual need only register a domain name and park it at the same time.

While registering a domain name and parking that domain name puts the core requirements and relationships in place for a revenue generation model; it does in and of itself not guarantee that the domain owner will in fact profit from this set up. In order to profit, an adequate amount of traffic and interest must be generated to draw Internet users to that domain name. As such, more emphasis is placed on domain names that are more likely to generate more interest. This is supported by our analysis in Table ??, which

¹⁰A more detailed discussion of how Internet advertising works can be found in chapter ??

clearly demonstrates that typo squatters and speculators have favored the domain names of leading candidates.

10.1.4 Malicious Intent

While advertising has been the primary motive behind the registration of typo and cousin name domains to date, the potential for more measurable damage using these techniques is highly probable. We have already observed a number of cases where a typo-squatted domain is forwarded to an alternate site with differing political views as seen in Figures 10.2, 10.3, and 10.4. This is problematic in the typo squatting case, since the end-user is unknowingly being redirected to a different web site. It is even more common when analyzing cousin domains. Since cousin domains can be registered by anyone, we can see from our analysis that the number of possible registrations can become near infinite. It is, however, much more difficult to drive visitors to those domains, without having some way in which to attract them. As such, owners of cousin domains use other techniques in order to attract visitors. This includes manipulating search engines in order to increase their ranking (Search Engine Optimization), or in some cases even taking out their own advertisements. It may also involve phishing-style spamming of large number of users.

One interesting side effect of ad syndication networks as they exist today is that we frequently encounter typo domains that are hosting advertisements for a candidate's competitor. It is interesting to see how search engine optimization and key word purchasing plays a role in attracting visitors. Many search engines allow the purchasing of advertisements that are displayed only when specific keywords are searched for. Google AdWords is a common example of such a program where particular key words can be purchased, and advertisements of the purchaser's choice will then be displayed. As shown in Figure 10.5, this may result in advertisements for one candidate being displayed when searching for a particular key word, or accidentally browsing to a typo squatted web site.

Advertising, misdirection, and detraction aside, the real potential for future abuse of typo and cousin domains may revolve around the distribution and installation of security risks and malicious code. This attack vector is by no means new, as web sites and banner advertisements are frequently used to attack visitors who happen to browse to a malicious web site [21]. Attackers who control such websites frequently leverage a software vulnerability in the web browser [22], or utilize social engineering and misleading tactics in order to trick the user into installing security risks [9] and malicious code. Even in



Figure 10.2. <http://www.hillaryclingon.com> is a typo version of Hillary Clinton's real web site, <http://www.hillaryclinton.com> (the g key is right below the t key), but it has another meaning as well.

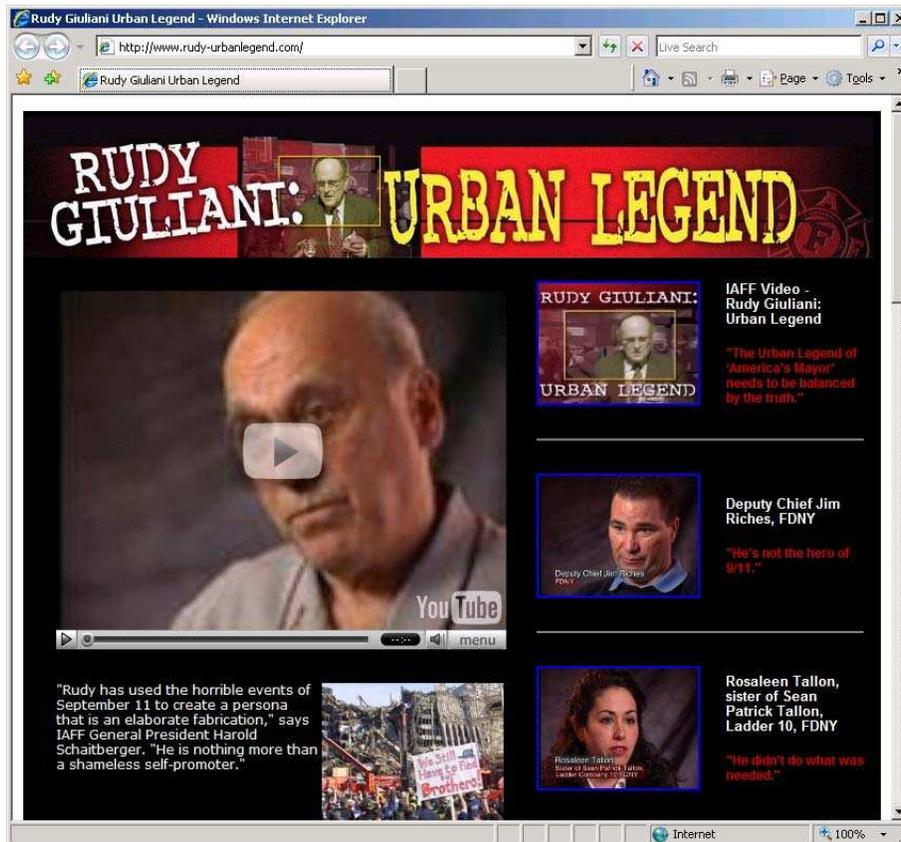


Figure 10.3. <http://www.joinrudy2008.com>, a typo of Rudy Giuliani's campaign web site, <http://www.joinrudy2008.com>, redirects to a detractor's web site at <http://rudy-urbanlegend.com>.

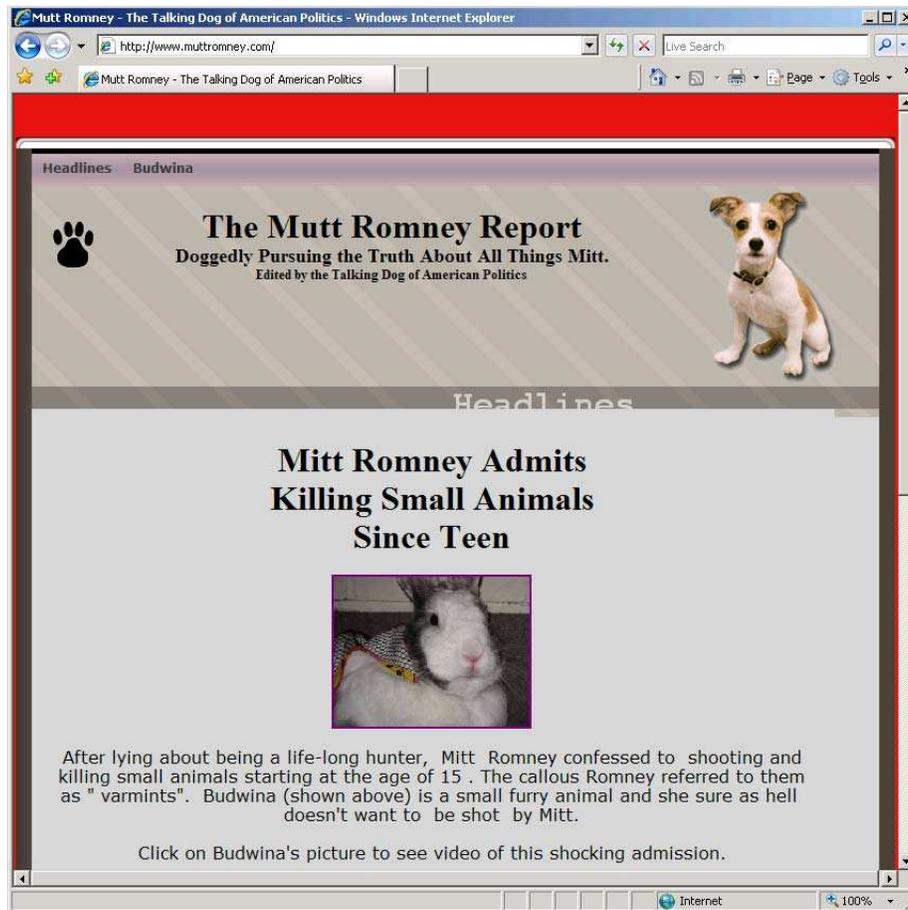


Figure 10.4. <http://www.muttromney.com> is a typo (since u is beside i) of Mitt Romney's web site, <http://www.mittromney.com> which redirects the user to a detractor's web site.

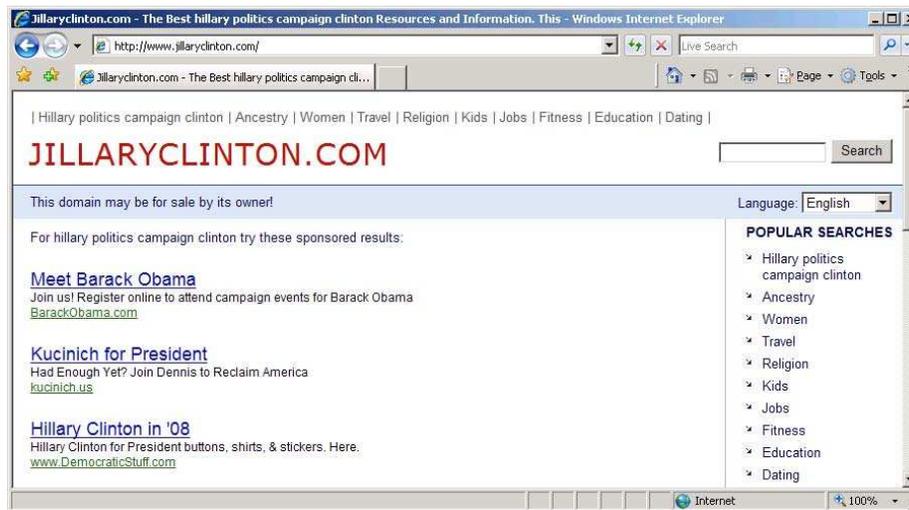


Figure 10.5. <http://www.jillaryclinton.com>, a typo of Hillary Clinton's web site, <http://www.hillaryclinton.com>, displays advertisements directing visitors to rival web sites.

the absence of a software vulnerability, we can conceive a number of convincing scenarios that one can construct in order to convince visitors to install such software. Consider that such a site could easily mirror Hillary Clinton's legitimate web site, however prominently offer for download a Hillary Clinton screen saver that was in fact Spyware or malicious code. Another site mirroring that of Rudy Giuliani could offer an application claiming to give instant access to his travels, speeches, and videos. Yet another site may claim that by downloading an application, the visitor can assist the candidate in fund raising, however that application is instead built to monitor and steal their own banking credentials. The impact of downloading such an application under false pretenses will be covered in more detail later in this chapter.

10.2 Campaign-Targeted Phishing

Phishing has without a doubt become one of the most widespread risks affecting Internet users today. As we look at Phishing, and the role that it may play in an election campaign, we find several incremental risks that present themselves beyond the traditional theft of confidential information.

10.2.1 Profit-Motivated Phishing

Profit-motivated event-based Phishing is certainly not new. It has been seen in the past on numerous occasions leading up to, and following significant events world-wide. It has been seen after natural disasters such as the Indian Ocean Tsunami [5] in 2004 and Hurricane Katrina [20], [23] in 2005. It has also been seen around sporting events, such as the 2006 and 2010 FIFA World Cup [27].

Election-related phishing has been observed in the past. During the 2004 federal election, phishers targeted the Kerry-Edwards campaign[35]; a campaign that was acknowledged as being at the forefront of leveraging the Internet for communications. At least two distinct types of phishing were observed during that campaign. In one case, phishers set up a fictitious web site in order to solicit online campaign contributions shortly after the Democratic National Convention, stealing the victim's credit card number, among other information. In the second case, phishers asked recipients to call a for-fee 1-900 number, whereby the victim would subsequently be charged \$1.99 per minute[40]. This is a prime example of how such attacks can cross technology boundaries in order to appear even more convincing. The perpetrators of these two attacks were never caught.

When considering the 2004 election as a whole, phishing presented only a marginal risk. At the time, Phishing itself was still in its infancy, and had yet to grow into the epidemic that can be observed today. When we revisit the potential risk of Phishing to the 2008 federal election, we find ourselves in a much different position. Candidates have flocked to the Internet in order to communicate with constituents, as well as to raise campaign contributions online.

We performed an analysis of campaign web sites in order to determine to what degree they allow contributions to be made online. We discovered that each and every candidate provided a mechanism by which supporters could make a contribution online. We noted that all web sites on which contributions could be made leveraged SSL in order to secure the transaction. We also noted the domain of each contribution site, and noticed that in numerous cases, would-be contributors were redirected to a third party site, sitting on a different primary domain. We show both the original domain, and the web site to which the user is redirected to in Table 10.4.

This redirection was the result of third party consulting, media, and online advocacy firms being used to assist in the running of the campaign, including the processing of online campaign contributions. This does not present a security risk in and of itself, nor is it an indication of phishing taking place; however the change in top level domain may add confusion to potential contributors who err on the side of caution. It also indicates that additional parties may be involved in the gathering and processing of personal information on behalf of a campaign, increasing the overall exposure of the credit cards numbers processed during fundraising.

It should also be noted that the redirection used here is not necessary, and that the contribution site can just as easily remain in the same top level domain, as a sub-domain hosted by the third party for processing. To do so simply requires the appropriate configuration of the primary domain's DNS records. It appears that this is what the majority of the remaining candidates have in fact chosen to do. Future research may also show whether or not those donation sites that do live under the campaign's domain name are in fact hosted on the same physical network as that of the campaign site, or on another, third party payment processor's network.

Figure 10.6 provides a sample of the information collected during an online contribution. We found that forms were fairly consistent in the type of information that was collected, while (not surprisingly) varying from a visual perspective.

The ability to process credit card transactions on an authentic campaign web site may provide an unexpected benefit to online identity thieves. One

Domain Name	Redirects To
barackobama.com	https://donate.barackobama.com
brownback.com	https://www.campaigncontribution.com
chrisdodd.com	https://salsa.wiredforchange.com
cox2008.com	https://www.completecampaigns.com
mikehuckabee.com	https://www.mikehuckabee.com
gilmoreforpresident.com	https://www.gilmoreforpresident.com
gohunter08.com	https://contribute.gohunter08.com
hillaryclinton.com	https://contribute.hillaryclinton.com
joebiden.com	https://secure.ga3.org
johnedwards.com	https://secure.actblue.com
johnmccain.com	https://www.johnmccain.com
joinrudy2008.com	https://www.joinrudy2008.com
mittromney.com	https://www.mittromney.com
richardsonforpresident.com	https://secure.richardsonforpresident.com
ronpaul2008.com	https://www.ronpaul2008.com
teamtancredo.com	https://www.campaigncontribution.com
tommy2008.com	https://secure.yourpatriot.com

Table 10.4. An analysis of 2008 federal candidate web sites and the site to which contributors are directed to. Note that the sites contributors are redirected to are legitimate, but the fact that they often are different from the original site increases the risk for confusion, and thereby, the risk that a phishing attack with a similar design would succeed.

MAKE AN ONLINE CONTRIBUTION

[Click here to contribute by mail](#)

CONTACT INFORMATION

First Name:
Last Name:
Address:
City:
State:
Zip:
Phone:
Email:

SELECT A TYPE AND AMOUNT

One-time contribution Recurring monthly *(what's this?)*

\$10 \$50 \$250 \$1000 \$4600
 \$25 \$100 \$500 \$2300 Other \$

CREDIT CARD INFORMATION

Card Number:   

Expiration:

Security Code: *(what's this?)*

EMPLOYMENT

To comply with Federal law, we must use best efforts to obtain, maintain, and submit the name, mailing address, occupation and name of employer of individuals whose contributions exceed \$200 in an election cycle.
If not employed, enter "none"

Employer:
Occupation:

CONFIRM YOUR ELIGIBILITY

By checking this box, I confirm that the following statements are true and accurate:

1. This contribution is made from my own funds, and not those of another.
2. This contribution is not made from the general treasury funds of a corporation, labor organization or national bank.
3. I am not a Federal government contractor.
4. I am not a foreign national who lacks permanent resident status in the United States.
5. I am at least 18 years of age.
6. This contribution is made on a personal credit or debit card for which I have the legal obligation to pay, and is made neither on a corporate or business entity card nor on the card of another.

SUBMIT

Figure 10.6. A sample form from one candidate's web site allowing visitors to make contributions online. This is a legitimate site. Since typical Internet users would not be well acquainted with the domains associated with political candidates, there is a risk that phishers would use a similarly designed website to collect credentials from unsuspecting victims.

tactic regularly employed by those peddling in stolen credit cards is to process a very small transaction in order to validate a credit card as legitimate[2]. Thieves began using this technique in early 2007 on online charity web sites, but it has been used on other types of online payment sites for some time now. Such a small transaction is unlikely to be noticed by the credit card holder, and unlikely to be flagged by the party processing the transaction.

All contributions are not helpful. Attackers may seek to disrupt a candidate's fundraising efforts by initiating illegitimate payments to cause confusion. If performed en masse, the widespread contribution of small, random amounts of money, from thousands or tens of thousands of stolen credit cards would certainly have a negative effect. While there is a slight chance such an attack may go unnoticed, it is more likely that it will be noticed, making it near impossible to differentiate legitimate contributions from those that are fraudulent. Thus, a significant burden would be placed on the affected candidates by diluting legitimate contributions with those that were not initiated by the credit card owners.

The increased collection of online campaign contributions also provides a ripe opportunity for phishers to target the unsuspecting public. Candidates and their parties regularly communicate with voters through e-mail, as demonstrated in Figure 10.7. Phishing involves the use of e-mail to lure a victim to a fictitious web site that attempts to steal confidential information from the victim [8]. While it is unreasonable to expect campaigns not to solicit contributions using email as a medium, they would be well advised to follow best practices that have been set by other online entities heavily prone to phishing. (A number of excellent resources are available through the Anti-Phishing Working Group [29] including a report funded by the U.S. Department of Homeland Security [14] that discusses the problem in-depth, and provides best-practices for organizations to communicate safely with their constituents.) However, whether the candidate uses email for contribution requests or not, a phisher may pose as a candidate and ask the recipients of his email for money. The typical goal would be to steal the credentials of his victims.

One of the more worrisome attacks may involve the diversion of donations intended for one candidate, to the web site of another. In such a scenario the attacker may set up a fictitious web site claiming to accept donations for one candidate, that by all intents and purposes looks legitimate. This attack may involve the registration of typo domains, or the use of phishing tactics in order to lure victims to this fictitious web site. When a donation is made however, this web site may in fact post the gathered transaction details to another candidate's web site. The contributor has now made a financial

From: "Howard Dean" <democraticparty@democrats.org>
Date: August 2, 2007 3:15:53 PM EDT
To:
Subject: They won't steal votes again
Reply-To: dnc-003m8004YD@mailier.democrats.org



Dear markus,

Last year, we put DNC staff on the ground all across the country to rebuild our party and stand up to the lies and failures of the Republican Party. The 50-State Strategy worked. Those organizers were key to our unprecedented victories up and down the ballot in 2006.

Our organizers are still on the ground in all 50 states, preparing for 2008 in every way possible. And starting this month, they are kicking off an unprecedented voter protection effort, of a scale never attempted by any organization.

While Democrats protect everyone's right to vote, Karl Rove and the Republican Party have a long history of threatening this right, working to make it harder for Americans to vote. We're going to stop them.

Protecting the right of every eligible American to vote is our party's top priority because we know that it's good for America and good for our democracy when everyone votes.

All Americans deserve to go to the polls confident that they won't be harassed or intimidated. That they won't wait hours for a ballot and that their vote will be counted fairly and accurately. Unfortunately, nearly forty-two years after the signing of the voting rights act, millions of American's are treated like criminals just for trying to vote.



Figure 10.7. The figure shows a portion of a legitimate fund-raising email, allowing the recipient to click on the hyperlinked “Contribute” button in order to support the campaign. This approach would be very easy for a phisher to mimic in order to make people submit their credentials to him, thinking they are contributing. Of course, phishers can use inflammatory texts (even more so than political candidates) as calls for action. The authors of this book were able to register the domain democratic-party.us, which would be suitable in such an attack, and found a wealth of other cousin name domains available for both parties. Thus, whereas financial institutions typically have registered cousin name domains to defend against abuse, political parties and candidates have not.

contribution to an entirely different candidate. This may be a candidate of the same political party or one from an opposing party. Such an attack may be difficult to trace, and at the time of this writing the author does not know what precautions (if any) candidates may be taking to avoid such an attack. The impact of such an attack is both monetary and psychological, undermining a contributor’s confidence in online donations altogether.

Phishers can increase their success rate by registering domain names that are typos or cousin domains of their target, a tactic which we have already discussed in some depth. For example, a phisher targeting John Edwards may elect to register **donatejohnedwards.com**. Additionally, phishers may simply create sub-domains for primary domains which they already own. A phisher who buys the domain **donatefor2008.com** may simply add DNS records for **johnedwards.donatefor2008.com** and **ron-paul.donatefor2008.com**, among others. These domain names are then referenced in the phishing e-mails that are sent to potential victims, that when clicked on, will drive the victim to the fictitious web site.

As we have observed, a significant number of typo domain names have already been registered, or are available to be registered, by parties who are acting in bad faith. Many of these domain names appear so similar to the legitimate domain name, that the unsuspecting eye of a potential victim would not notice if they were directed to one. Campaigns can take clear and immediate steps to purchase typo domains prior to them falling into the wrong hands, however, as of this writing, many have not done so.

More difficult, however, is the acquisition of cousin domain names. As discussed previously, a significant number of cousin domain names have been registered, for both speculative and advertising purposes. Given the near infinite number of possible cousin domain names, it is unlikely that a campaign can acquire all possibilities. This provides phishers the opportunity to register a domain name that may appear similar to the legitimate campaign's web site.

Yet another type of attack may use a spoofed email appearing to come from a political party or candidate to entice recipients to open attachments, and thereby infect their machines with malicious code. Again, this may be done either with the direct goal of spreading malicious code, or in order to deliver a blow under the belt to political candidates relying heavily on the Internet for their communication with constituents.

Even without the registration of a similar domain name, phishers will continue to succeed with e-mails and web sites that are obvious to detect by a trained eye, but perhaps not so obvious to those who continue to fall victim.

10.3 Malicious Code and Security Risks

Malicious code and security risks present one of the more sinister risks to the election process. As discussed in other chapters, malicious code, such as

threats that leverage rootkit capabilities¹¹ have the potential to gain complete and absolute control over a victim's computer system. In addition, security risks, such as Adware and Spyware also pose serious concern, both in terms of their invasiveness to a user's privacy, in the case of Spyware, and their ability to present users with unexpected, or undesired information and advertisements, in the case of Adware¹².

We can consider a number of scenarios where well-known classes of malicious code may be tailored specifically to target those participating in an election. Targets may range from candidates and campaign officials to voters themselves. In discussing these risks we begin with what we consider the less serious category of Security Risks, and then move into the more serious, insidious category of malicious code.

10.3.1 Adware

Adware, in its truest form, may not pose an immediate and dire risk to the end-user. However, once installed, its control over a user's Internet experience places it into a strategic position on the end user's computer. Adware has the potential to manipulate a user's Internet experience by displaying un-expected or unwanted advertisements. These advertisements may be displayed on the users desktop or shown to them through their web browser as they visit Internet web sites. These advertisements may appear as pop-up windows, or they may appear as content (Ads) that are either overlaid or inserted into existing web pages visited by the user. These techniques have been used frequently by such well known Adware applications as 180solution's Hotbar [13], The Gator Corporation's Gator [10], and WhenU's Save [11]. Adware may be installed by the end user as part of another third party application, or may be installed surreptitiously through the use of a software vulnerability in the user's web browser. Chapter ?? discusses adware in more detail.

There are a variety of ways in which Adware may be used in order to influence or manipulate users during the course of an election. In its most innocuous form, Adware may simply present the user with advertisements promoting a particular candidate, directing the user to the candidate's web site when clicked. Taking a more deceptive angle, Adware may be used to silently replace advertisements for one candidate with another. This may be done directly in the user's browser by manipulating the incoming HTML content before it is rendered or overlaying a new advertisement on top of an

¹¹A detailed discussion of rootkits can be found in chapter ??

¹²A more extensive discussion of adware can be found in chapter ??

existing one on the user's screen.

Until it is observed, it is difficult for us to predict the real-world impact that such an Adware application may have. It would be important for such an application to be silent, and unobtrusive, acting clandestinely in order to avoid annoying the end user; lest its objective backfire. In addition, such an effort may only help to sway those voters who have not already committed to a particular party or candidate, not those who have already made their decision.

10.3.2 Spyware

We have frequently seen Adware and Spyware traits combined into a single application that both delivers advertising as well as monitors a user's Internet habits. For the purposes of our discussion we chose to distinguish between the distinct behaviors of Adware and Spyware, discussing each separately. Spyware, with its ability to secretly profile and monitor user behavior, presents an entirely new opportunity for the widespread collection of election related trends and behavioral information.

When discussing the use of Spyware, we can conceive a number of behaviors that may be collected throughout the course of an election in order to provide insight into voter disposition. The most basic of these would be to monitor the browsing behavior of voters, and the party affiliation of Internet sites most frequently visited by the end user. Even without the installation of Spyware on an end user's computer, one web site may silently acquire a history of other web sites that the user has previously visited. This has been demonstrated by researchers in the past, and can be observed at <https://www.indiana.edu/~phishing/browser-recon>. This may also include the tracking of online news articles that are viewed and online campaign contributions made by determining whether a particular URL was visited.

With the addition of Spyware on the end user's computer, this can be taken a step further. E-mails sent and received by the user can be monitored. We found, for example, that all 19 candidates allow one to subscribe to their campaign mailing list, from which a user receives regular frequent updates on the campaign's progress. Knowing how many voters have subscribed to a particular candidate's mailing list may provide insight into overall support levels for that candidate.

It is important to consider that Internet and browsing behavior alone may not be an indicator of a voter's preference, since voters may be just as likely to visit a competing candidate's web sites and subscribe to a compet-

ing candidate's mailing list, in order to stay informed on that candidate's messaging. Unfortunately, we could find no prior research that examined a connection between user Internet behavior and a correlation to party or candidate affiliation. Regardless of this, Spyware does pose a new risk to the mass accumulation of election related statistics that may be used in order to track election trends.

It is important to note that the collection of voter disposition data is certainly not new, as groups such as The Gallup Organization [17] known for the Gallup Poll have been collecting and analyzing user behavior since 1935. What is different in this case is that Spyware has the ability to capture and record user behavior without consent, and without the voter's knowledge. Even when a Spyware application's behavior is described clearly in an End-User License Agreement (EULA) it is well known that few users read, nor understand these complex and lengthy agreements [12]. This changes the landscape dramatically when it comes to election-related data collection.

10.3.3 Malicious Code; Keyloggers and Crimeware

By far one of the most concerning attacks on voters, candidates, and campaign officials is that of malicious code infection. Malicious code that is targeted towards a broad spectrum of voters has the potential to cause widespread damage, confusion, and loss of confidence in the election process itself. When we consider all of the attacks mentioned in this chapter, malicious code, in the form of Key Loggers, Trojans and other forms of Crimeware has the potential to carry each of them out with unmatched efficiency. These include the monitoring of user behavior, the theft of user data, the redirection of user browsing, and the delivery of misinformation.

One additional angle on Crimeware is the notion of intimidation. Given a threat's presence on a voter's computer, that threat has the potential to collect personal, potentially sensitive information about that individual. This may include turning on the computer's microphone and recording private conversations. It may include turning on the computer's video camera and recording activities in the room. It may include retrieving pictures, browser history, documents or copyright files from a voter's computer. Perhaps you will be turned in to the RIAA if copyright music is found on your computer? The collection of such information creates the potential for an entirely new form of voter intimidation. The collection of such personally sensitive or legally questionable data gathered by a threat may allow an attacker to intimidate that one individual in this entirely new way. We would of course expect and hope that the number of voters who might be intimidated in

such a way would be relatively low, however only time will tell whether such speculation becomes reality.

Another form of threat that we have seen in the past is one which holds a victim's data hostage, until a fee is paid in order to release it. This was first discussed in [42]. An example of such a threat is Trojan.Gpcoder [31], which encrypts the user's data, erasing the original, until this fee is paid. Such a threat may present another new form of intimidation whereby the only way for a user to regain access to their personal data is to vote accordingly. Such an attack presents obvious logistical challenges, such as how is the attacker to know which way the victim voted? He may however take comfort in the belief that he has intimidated enough of the infected population to make a meaningful difference.

Just as the widespread infection of the populace poses a risk to voters, targeted calculated infection of specific individuals poses equal cause for concern. A carefully placed targeted key logger has the potential to cause material damage to a candidate during the election process. Such code may also be targeted towards campaign staff, family members, or others who may be deemed material to the candidate's efforts. Such an infection can result in the monitoring of all communications, including e-mail messages and web site access initiated on the infected computer. This monitoring would give the would-be attacker unparalleled insight into the progress, plans, and disposition of the candidate's campaign. This may include new messaging, speeches, and otherwise sensitive information critical to the outcome of the candidate's campaign.

10.4 Denial of Service Attacks

Denial of service attacks have become increasingly common on the Internet today. Denial of service attacks seek to make a computer network, in most cases a particular web site, unavailable and therefore unusable. Known commonly as distributed denial of service (DDoS) attacks, they are frequently launched by means of inundating a target with an overwhelming amount of network traffic. This traffic may be in the form of Internet protocol requests at the IP and TCP layers, or application level requests that target specific applications such as an organization's web server, e-mail server, or FTP server. Denial of service attacks are frequently perpetrated through the use of Bot networks, discussed in more detail in chapter ??.

A number of high profile wide scale DDoS attacks have demonstrated the effects that such an effort can have. One of the best known and largest attacks was launched against the country of Estonia in May of 2007 [7]. This

attack presented a prime example of one that was politically motivated as it was launched by Russian patriots in retaliation to the removal of a Soviet monument by the Estonian government. Attackers disabled numerous key government systems during a series of attacks that occurred over the course of several weeks.

In 2006, Joe Lieberman's web site also fell victim to a concentrated denial of service attack [38]. Forcing the site offline, the attack paralyzed the `joe2006.com` domain, preventing campaign officials from using their official campaign e-mail accounts and instead having to revert to their personal accounts.

The implications of such attacks are clear - they both prevent voters from reaching campaign web sites, and prevent campaign officials from communicating with voters.

10.5 Cognitive Election Hacking

Labeled by researchers as Cognitive Hacking [6], the potential for misinformation and subterfuge attacks using Internet-based technologies are as plenty as one's imagination. We have already discussed several techniques that may be used to surreptitiously lure users to locations other than a legitimate campaign's web site. These same techniques can be used to spread misleading, inaccurate and outright false information.

We have discussed *typo* and *cousin* domain names that users may visit accidentally when attempting to browse to a legitimate web site. We've also discussed phishing and spam, and the potential to lure users to web sites impersonating a legitimate candidate's web site. Finally, we discussed malicious code, and the role that it may play in manipulating a user's desktop experience before they even reach their intended destination.

The security of a campaign's web site plays another vital role in the election process. The breach of a legitimate candidate's web site would allow an attacker to have direct control over all content viewed by visitors to that web site. This may allow for the posting of misinformation, or worse, the deployment of malicious code to unsecured visitors.

Examples of misinformation about a specific candidate include the decision by a candidate to drop-out of the race, a fake scandal, and legal or health issues. It may also include subtle information that could be portrayed as legitimate, such as a change in a candidate's position on a particular subject, resulting in the loss of voters who feel strongly about that issue.

Attempts to deceive voters through the spread of misinformation are not new. In fact, numerous documented cases exist for past elections using

traditional forms of communication [33]. These include campaigns aimed at intimidating minorities, those with criminal records, attempts to announce erroneous voting dates, and many other tactics resulting in voter confusion.

During the 2006 election, 14,000 Latino voters in Orange County received misleading letters warning them that it is illegal for immigrants to vote in the election, and that doing so may result in incarceration and deportation. In his testimony¹³, John Trasviña, President and General Counsel of the Mexican American Legal Defense and Educational Fund (MALDEF), discusses this use of misinformation as an example of voter suppression:

“First, the Orange County letter falsely advised prospective voters that immigrants who vote in federal elections are committing a crime that can result in incarceration and possible deportation. This is a false and deceptive statement: naturalized immigrants who are otherwise eligible to vote are free to vote in federal elections without fear of penalties (including but not limited to incarceration and/or deportation). Second, the letter stated that “the U.S. government is installing a new computerized system to verify names of all newly registered voters who participate in the elections in October and November. Organizations against emigration will be able to request information from this new computerized system.” Again, the letter adopts an intimidating tone based upon false information in an apparent attempt to undermine voter confidence within the targeted group of voters. Finally, the letter stated that “[n]ot like in Mexico, here there is no benefit to voting.” This letter, representing a coordinated and extensive effort to suppress the Latino vote in the days leading up to a congressional election, has been traced to a candidate running for the congressional seat in the district in which the affected voters live.”

Another case of deception was targeted at college students in Pittsburgh in 2004 [32]. Canvassers, posing as petitioners for such topics as medical marijuana and auto insurance rates, gathered signatures from students that, unknown to them, resulted in a change to their party affiliation and polling location.

Push polling is one technique that lends itself extremely well to Internet based technologies. In push polling, an individual or organization attempts

¹³United States Senate Committee on the Judiciary Prevention of Deceptive Practices and Voter Intimidation in Federal Elections: S. 453 Testimony of John Trasviña. Available from http://judiciary.senate.gov/testimony.cfm?id=2798&wit_id=6514

to influence or alter the views of voters under the guise of conducting a poll. The poll, in many cases, poses a question by stating inaccurate or false information as part of the question. One well known push poll occurred in the 2000 Republican Party primary¹⁴. Voters in South Carolina were asked "Would you be more likely or less likely to vote for John McCain for president if you knew he had fathered an illegitimate black child?". In this case, the poll's allegation had no substance, but was heard by thousands of primary voters. McCain and his wife had in fact adopted a Bangladeshi girl.

A bill known as the Deceptive Practices and Voter Intimidation Prevention Act of 2007¹⁵ seeks to make these attacks illegal. Currently waiting to be heard in the Senate, it is possible that this bill would be in place for the 2008 federal election, making deceptive tactics such as these illegal, and introducing a maximum penalty of up to 5 years in prison for offenders. This bill is likely to apply to deceptive practices whether they are performed using traditional communication mechanisms, or through modern Internet-based technologies.

While the introduction of such policies are important, and provide a well defined guideline to prosecute offenders, only time will tell to what extent they will succeed in controlling these acts. As we have seen in some areas such as the policies developed in order to outlaw the transmission of spam e-mail, regulations have only a marginal affect in reducing the problem. Even today, over 50% of all email sent on the Internet is purported to consist of spam [39]. There is absolutely no reason to doubt that the type of deception and intimidation discussed will be equally successful on the Internet.

The challenge with Internet-based technologies is the ease by which such an attack may be perpetrated. Whereas traditional communication mediums may have required an organized effort in order to commit an attack, the Internet provides a single attacker the benefit of automation and scale that previously did not exist. As such, one person has the potential to cause widespread disruption, with comparably little effort.

Historically, some of the most successful misinformation attacks on the Internet have also been motivated by profit. Pump and dump schemes [34], have become an extremely common form of spam. These schemes involve the promotion of a company's stock, through the issuance of false and misleading statements. After the stock rises due to renewed interest from the message's recipients, the perpetrators sell their own stock for a substantial profit.

¹⁴SourceWatch. http://www.sourcewatch.org/index.php?title=Push_poll

¹⁵Deceptive Practices and Voter Intimidation Prevention Act of 2007. <http://www.govtrack.us/congress/billtext.xpd?bill=h110-1281>

One significant surge of pump and dump emails that was observed in 2006 was attributed to a Bot network, operated by Russian fraudsters [25]. In this attack, 70,000 infected computers, spread across 166 countries were organized into a bot network that was used to send out unsolicited stock-promoting spam. It should be noted that such a network can be directed to send any form of email, including disinformation and fallacies related to a candidate, voters, and the election itself. Chapter ?? discusses botnets and their applications in more detail.

10.6 Public Voter Information Sources - FEC Databases

The Federal Election Commission [3] was created in order to both track campaign contributions, and enforce federal regulations that surround them.

In 1975, Congress created the Federal Election Commission (FEC) to administer and enforce the Federal Election Campaign Act (FECA) - the statute that governs the financing of federal elections. The duties of the FEC, which is an independent regulatory agency, are to disclose campaign finance information, to enforce the provisions of the law such as the limits and prohibitions on contributions, and to oversee the public funding of Presidential elections.

In order to provide a public record of campaign contributions, the FEC must maintain, and provide to the public, a full record of all campaign contributions. Many web sites that allow online contributions clearly indicate their requirement to report those contributions to the Federal Election Commission. The following text, taken from an unnamed candidate's web site exemplifies this:

We are required by federal law to collect and report to the Federal Election Commission the name, mailing address, occupation and employer of individuals whose contributions exceed \$200 in an election cycle. These records are available to the public. However, they cannot be used by other organizations for fundraising. We also make a note of your telephone number and email address, which helps us to contact you quickly if follow-up on your contribution is necessary under Federal election law. For additional information, visit the FEC website at <http://www.fec.gov>.

The FEC's role is to make this data available to the public, and thus it is available as both raw data files, via FTP, and viewable through online web interfaces on the FEC web site.

Numerous third party web sites, such as <http://www.opensecrets.org>, also consume this data in order to provide regular high level reports on candidate funding. Consumers of the data are restricted by a policy that regulates how the data can be used [4]. The policy is however surprisingly lenient, primarily intended to prevent the use of contributors names for commercial purposes or further solicitation of contributions.

The information provided in this database consists of the contributors full name, city, zip code, and particulars of the contribution, such as the receiving candidate or party, the amount, and the date of the contribution. While limited, this information does allow one to build a history of political contributions for any U.S. citizen contained herein.

In addition, contributors of record may be more likely to become victims of other attacks already discussed in this chapter. Appearing in this database may expose high net worth contributors to targeted phishing (spear phishing) or malicious code attacks if that individual's name can be connected to their email address (no longer a difficult feat).

10.7 Intercepting Voice Communications

While we have focused primarily on Internet based risks, we would be remiss if we did not discuss at least one additional risk given a recent particularly noteworthy and sophisticated attack against a foreign nation's communication infrastructure. Labeled as *The Athens Affair* by authors Vassilis Prevelakis and Diomidis Spinellis [30], this well coordinated attack accentuates the increased role that common technologies play in all forms of our daily communications. In their paper, the authors retrace the alarming events related to the interception of cell phone communications from high ranking Greek government officials:

On 9 March 2005, a 38-year-old Greek electrical engineer named Costas Tsalikidis was found hanged in his Athens loft apartment, an apparent suicide. It would prove to be merely the first public news of a scandal that would roil Greece for months.

The next day, the prime minister of Greece was told that his cell-phone was being bugged, as were those of the mayor of Athens and at least 100 other high-ranking dignitaries, including an employee of the U.S. embassy.

The victims were customers of Athens-based Vodafone-Panafon, generally known as Vodafone Greece, the country's largest cellular service provider; Tsalikidis was in charge of network planning at the company. A connection seemed obvious. Given the list of people and their positions at the time of the tapping, we can only imagine the sensitive political and diplomatic discussions, high-stakes business deals, or even marital indiscretions that may have been routinely overheard and, quite possibly, recorded.

Even before Tsalikidis's death, investigators had found rogue software installed on the Vodafone Greece phone network by parties unknown. Some extraordinarily knowledgeable people either penetrated the network from outside or subverted it from within, aided by an agent or mole. In either case, the software at the heart of the phone system, investigators later discovered, was reprogrammed with a finesse and sophistication rarely seen before or since.

In this attack, perpetrators used rootkit techniques, like those discussed in chapter ?? on the cellular provider's phone switch in order to remain hidden. Over the past two decades the basic communications systems that we rely on for both our traditional land-line telephones as well as our cellular phone communications have increasingly moved to commodity-based hardware and software [15]. In the past, would-be attackers were forced to learn complex and proprietary embedded systems, making the introduction of malicious code on these systems difficult if not impossible. Today's commoditization simplifies this effort, as witnessed by the attack discussed here, and greatly increases the potential for an attacker to gain a similar foothold on communications systems in the future.

Central switching networks are not the only target. Mobile devices themselves remain the more likely candidate for interception of communications. Today's mobile devices, an increasing number of which can now be considered Smartphones, provide a ripe avenue for the introduction of malicious code. While traditional threats, such as viruses, worms and Trojans have yet to gain widespread prominence on mobile devices (although they do exist), the potential for targeted customized mobile threats has existed for some time.

One particular application, known as FlexiSpy, sold by Bangkok, Thailand software vendor Vervata, allows listening to a remote phone's surroundings while it is not in use. It also allows retrieval of the phone's personal data, and monitoring of all email and SMS messages sent by the phone.

This page helps you understand what all the spyphone features mean				
	PRO	LIGHT	ALERT	BUG
Application Features				
 Remote Listening				
Make a spy call to the target phone running FlexiSPY and listen in to the phones surroundings. This does not allow you to listen to the phone conversation in progress. Call Tapping will be available very shortly. Please sign up to our mailing list of you are interested in this feature				
 Control Phone By SMS				
Send secret SMS to the target phone to control all functions. No need to physically access the phone for any feature not related to installation				
 SMS and Email Logging				
All SMS and EMAIL contents are sent to your FlexiSPY web account. Support all languages				
 Call History Logging				
The time, duration and number of all voice calls are sent to your web account. If the phone number is in the phones address book, then the name will be available also				
 Location Tracking				
See the CELL ID and CELL name that the mobile is physically located in. Read more about mobile location tracking by cell id				
 Private Data Deleting				
Delete your videos, pictures, SMS, and application with one SMS				

Figure 10.8. FlexiSpy, developed and sold by Bangkok, Thailand's Vervata allows for monitoring and tapping of cell phone communications. It is supported on Windows Mobile, Symbian OS and Blackberry devices. Today installation requires physical access to the device, however much like desktop operating systems, future versions have the potential to be installed through software vulnerabilities or messaging applications.

The software itself is available in "Pro", "Light", "Alert" and "Bug" versions. The vendor prides itself by its software's ability to remain hidden and unnoticeable on an infected device.

The infection of a candidate, campaign staff, or candidate's family's cell phone with such a freely available application could have dire consequences. Now all back-room and hallway conversations partaken by the candidate can be monitored at all times and intercepted by the attacker. Worse, opinions, perhaps not shared with the public or outsiders are recorded, and available

for later playback introducing the potential for widespread exposure and damage.

We have already seen examples of unexpected recordings accidentally made public for other political figures, including California Governor Arnold Schwarzenegger [28] in 2006 and 2007. In that case, the recordings were unintentionally exposed through the Governor's web site and resulted in criticism on a comment made about Hispanic Americans that was made without the intent of it becoming public.

10.8 Conclusion

As campaigns increasingly look to the online medium in order to gather support, it is important to consider the inherent risks that will follow. In this chapter we have discussed a number of risks that may present themselves in any election campaign; however it is important to consider that there are many that remain which we have not discussed.

It is apparent from both past events, and from our findings that candidates and their campaigns are only beginning to understand the risks of online advocacy and have yet to take the necessary precautions in order to protect themselves. Our fear is that a true appreciation of the required countermeasures will not be realized until these attacks do in fact manifest themselves.

It is important to consider that many of these individual risks, when combined, result in increasingly sophisticated attacks. While we have discussed many of these risks independently, the combination of these threats create complex new variations that are already seen in the wild today in other areas such as online banking and ecommerce.

Our goal in writing this chapter was certainly not to seed the minds of would-be attackers, nor to spread fear, uncertainty and doubt, but rather to discuss real-world risks that already exist today. None of the attacks which we have discussed are new or novel, however we have applied them to a specific recurring event; the election process. Our hope is to raise awareness of the potential risks before they are able to manifest themselves in both the upcoming 2008 federal election, and any election to follow.

One thing is clear, it is impossible for us to predict how successful any one of these attacks may be in making a material impact to the election process. Given previous widespread Internet-borne risks, we certainly do have an appreciation and respect for the potential that they present, and while that is not to be discounted; only time will tell.

In addition, if a successful widespread attack were to occur (one which

was recognized to have swayed the vote), what recourse is there? What if intimidation, misinformation, and infectious election-targeted malicious code became the norm?

10.9 Acknowledgements

The author wishes to thank Markus Jakobsson for providing a political fundraising email sample, for pointing out additional political-sounding URLs that he had registered, and for his helpful discussions, feedback, and contributions on earlier drafts. In addition, the author would like to thank Zulfikar Ramzan for his advice, feedback, and recommendations during the writing of this chapter, and Kevin Haley for his recommendation on the addition of push polling.

BIBLIOGRAPHY

- [1] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller. Source Code Review of the Diebold Voting System. http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf.
- [2] Jim Carr. Not-so-sweet charity: Credit card fraud takes a charitable twist. SC Magazine, July 6, 2006. <http://scmagazine.com/us/news/article/669553/not-so-sweet-charity-credit-card-fraud-takes-charitable-twist/>.
- [3] Federal Election Commission. About the FEC. <http://www.fec.gov/about.shtml>.
- [4] Federal Election Commission. Sale and use of campaign information. http://www.fec.gov/pages/brochures/sale_and_use_brochure.pdf.
- [5] ConsumersUnion.org. Tsunami Scams Underscore Need for Caution When Giving to Charities Online. Press Release, Tuesday, January 11, 2005. http://www.consumersunion.org/pub/core_financial_services/001781.html.
- [6] George Cybenko, Annarita Giani, Carey Heckman, and Paul Thompson. Cognitive Hacking: Technological and Legal Issues. Proceedings of Law and Technology, 2002. <http://www.ists.dartmouth.edu/library/cht1102.pdf>.
- [7] Joshua Davis. Hackers Take Down the Most Wired Country in Europe. Wired Magazine, Issue 15.09. http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

-
- [8] Christine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz. Anatomy of a Phishing Email. Conference on Email and Anti-Spam, 2004. <http://www.ceas.cc/papers-2004/114.pdf>.
- [9] Benjamin Edelman. Claria's Misleading Installation Methods - Ezone.com. <http://www.benedelman.org/spyware/installations/ezone-claria/>.
- [10] Benjamin Edelman. Documentation of Gator Advertisements and Targeting. <http://cyber.law.harvard.edu/people/edelman/ads/gator/>.
- [11] Benjamin Edelman. "Spyware": Research, Testing, Legislation, and Suits. <http://www.benedelman.org/spyware/>.
- [12] Benjamin Edelman. WhenU License Agreement is Forty Five Pages Long. <http://www.benedelman.org/spyware/whenu-license/>.
- [13] Benjamin Edelman. Hotbar Advertising - Screenshots, May 2005. <http://www.benedelman.org/spyware/installations/kidzpage-hotbar/details-ads.html>.
- [14] Aaron Emigh. Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. ITTC Report on Online Identity Theft Technology and Countermeasures. <http://www.antiphishing.org/Phishing-dhs-report.pdf>.
- [15] Ericsson. Ericsson and Compaq form strategic partnership to build next generation switches based on AlphaServers. Press Release, October 10, 2000. <http://www.ericsson.com/ericsson/press/releases/old/archive/2000Q4/20001010-0060.html>.
- [16] The Internet Corporation for Assigned Names and Numbers. Uniform Domain-Name Dispute-Resolution Policy. <http://www.icann.org/udrp/udrp.htm>.
- [17] Gallup Poll Web Site. <http://www.galluppoll.com/>.
- [18] Randolph C. Hite. Electronic Voting offers Opportunities and Presents Challenges. Testimony Prepared for the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives. Available from: <http://www.gao.gov/new.items/d04766t.pdf>.

- [19] Markus Jakobsson. The Human Factor in Phishing. Privacy & Security of Consumer Information '07. <http://www.informatics.indiana.edu/markus/papers/aci.pdf>.
- [20] Brian Krebs. Katrina Phishing Scams Begin. Washington Post Security Fix, August 31, 2005. http://blog.washingtonpost.com/securityfix/2005/08/katrina_phishing_scams_begin_1.html.
- [21] Robert Lemos. Attackers strike using Web ads. CNET News.com, November 2004. http://news.com.com/Attackers+strike+using+Web+ads/2100-7349_3-5463323.html.
- [22] Robert Lemos. More security hiccups for ie. CNET News.com, November 2004. http://news.com.com/More+security+hiccups+for+IE/2100-1002_3-5457105.html.
- [23] Robert McMillan. Man charged in Hurricane Katrina phishing scams. IDG News Service, August 2006. http://www.infoworld.com/article/06/08/18/HNkatrinaphishing_1.html.
- [24] Lori Minnite and David Callahan. Secure the Vote: An Analysis of Election fraud. http://www.demos.org/pubs/EDR_-_Securing_the_Vote.pdf.
- [25] Ryan Naraine. 'Pump-and-Dump' Spam Surge Linked to Russian Bot Herders. eWeek, November 16, 2006. <http://www.eweek.com/article2/0,1895,2060235,00.asp>.
- [26] BBC News. Halt e-voting, says election body, August 2007. http://news.bbc.co.uk/2/hi/uk_news/politics/6926625.stm.
- [27] OUT-LAW News. FIFA warns football fans of phishing scam, September 2005. <http://www.out-law.com/page-6171>.
- [28] Rich Pedroncelli. Recordings reveal Schwarzenegger annoyed by Democrats, GOP alike. USA Today, February 5, 2007. http://www.usatoday.com/news/nation/2007-02-05-schwarzenegger-recordings_x.htm.
- [29] Anti Phishing Working Group Resources. <http://www.apwg.org/resources.html#advice>.
- [30] Vassilis Prevelakis and Diomidis Spinellis. The Athens Affair: How some extremely smart hackers pulled off the most audacious cell-network

- break-in ever. IEEE Spectrum Online. <http://www.spectrum.ieee.org/jul07/5280>.
- [31] Symantec Security Response. Trojan.Gpcoder. http://www.symantec.com/security_response/writeup.jsp?docid=2005-052215-5723-99.
- [32] Dennis B. Roddy. Rendell vows action on voter scams; Pitt students tricked. Pittsburgh Post-Gazette, October 27, 2004. <http://www.post-gazette.com/pg/04301/402432.stm>.
- [33] Laura Rozen. New NAACP report on GOP voter suppression efforts against minority voters in america, November 2004. <http://www.warandpiece.com/blogdirs/001293.html>.
- [34] Securities and Exchange Commission. Pump and Dump schemes. <http://www.sec.gov/answers/pumpedump.htm>.
- [35] Larry Seltzer. Spotting Phish and Phighting Back. eWeek.com, August 2004. <http://www.eweek.com/article2/0,1759,1630161,00.asp>.
- [36] Paul Sloan. The man who owns the Internet. Business 2.0 Magazine. http://money.cnn.com/magazines/business2/business2_archive/2007/06/01/100050989/index.htm.
- [37] Sid Stamm, Markus Jakobsson, and Mona Gandhi. verybigad.com: A study in socially transmitted malware. <http://www.indiana.edu/~phishing/verybigad/>.
- [38] Bob Sullivan. Lieberman campaign site, e-mail hacked. MSNBC, Aug 8, 2006.
- [39] Symantec. Symantec Internet Security Threat Report, Edition XII. <http://www.symantec.com/threatreport/>.
- [40] Tech Web Technology News. New Phishing Scam Takes Advantage of Election Hype, October 2004. <http://www.techweb.com/wire/security/49400811>.
- [41] Yi-Min Wang, Doug Beck, Jeffrey Wang, Chad Verbowski, and Brad Daniels. Strider Typo-Patrol: Discovery and Analysis of Systematic Typo-Squatting. Microsoft Research Technical Report MSR-TR-2006-40. <http://research.microsoft.com/Typo-Patrol/>.

- [42] Adam Young and Moti Yung. *Malicious Cryptography: Exposing Cryptovirology*. John Wiley and Sons, 2004.