s.15(1) - Subv

s.24(1)

Dvorkin, Corey

From: Dvorkin, Corey
Sent: March-19-13 12:56 PM
To: Barr, Corri (Corri.Barr@tbs-sct.gc.ca)
Cc: [redacted]
PETER.ARCHAMBAULT@forces.gc.ca
Subject: why is it always Florida?!

s.19(1)

Cyberattack on Florida election is first reported case of cyberattack against election system: NBCNews

Hamilton, Sharon

From: Hamilton, Sharon
Sent: Monday, March 18, 2013 3:36 PM
To: Hamilton, Sharon
Subject: Cyberattack on Florida election is first known case in US, experts say

http://openchannel.nbcnews.com/_news/2013/03/18/17314818-cyberattack-on-florida-election-is-first-known-case-in-us-experts-say?lite

Cyberattack on Florida election is first known case in US, experts say
By Gil Aegerter Staff Writer, NBC News
March 18, 2013, 12:29 pm **NBCNews.com**

Tim Chapman / Miami Herald About 2,000 rejected absentee ballots at Miami-Dade Elections Department, mostly for lack of signatures or review of signatures from the last election.

An attempt to illegally obtain absentee ballots in Florida last year is the first known case in the U.S. of a cyberattack against an online election system, according to computer scientists and lawyers working to safeguard voting security.

The case involved more than 2,500 "phantom requests" for absentee ballots, apparently sent to the Miami-Dade County elections website using a computer program, according to a grand jury report on problems in the Aug. 14 primary election. It is not clear whether the bogus requests were an attempt to influence a specific race, test the system or simply interfere with the voting. Because of the enormous number of requests – and the fact that most were sent from a small number of computer IP addresses in Ireland, England, India and other overseas locations – software used by the county flagged them and elections workers rejected them.

Computer experts say the case exposes the danger of putting states' voting systems online – whether that's allowing voters to register or actually vote.

"It's the first documented attack I know of on an online U.S. election-related system that's not (involving) a mock election," said David Jefferson, a computer scientist at Lawrence Livermore National Laboratory

who is on the board of directors of the Verified Voting Foundation and the California Voter Foundation.

Other experts contacted by NBC News agreed that the attempt to obtain the ballots is the first known case of a cyberattack on voting, though they noted that there are so many local elections systems in use that it's possible that a similar attempt has gone unnoticed.

There have been allegations of election system hacking before in the U.S., but investigations of irregularities have found only software glitches, voting machine failures, voter error or inconclusive evidence. Where there has been evidence of a computer security breach -- such as a 2006 incident in Sarasota, Fla., in which a computer worm that had been around for years raised havoc with the county elections voter database -- it was unclear whether the worm's appearance was timed to interfere with the election.

In any case, experts say they've been warning about this sort of attack for years.

"This has been in the cards, it's been foreseeable," said law Professor Candice Hoke, founding director of the Center for Election Integrity at Cleveland State University.

The primary election in Miami-Dade County in August 2012 involved state and local races along with U.S. Senate and congressional contests (see a sample ballot here). The Miami Herald, which first reported the irregularities, said the fraudulent requests for ballots targeted Democratic voters in the 26th Congressional District and Republicans in Florida House districts 103 and 112. None of the races' outcomes could have been altered by that number of phantom ballots, the Herald said.

Overseas "anonymizers" -- proxy servers that make Internet activity untraceable -- kept the originating computers' location secret and prevented law enforcement from figuring out who was responsible, according to the grand jury report, issued in December. The state attorney's office closed the case in January without identifying a suspect.

Read the Miami-Dade County grand jury report (PDF)

Then came the Herald report, which said that three IP addresses in the United States had been identified among those sending the requests and that there had been a delay in getting that information to investigators, which a Miami-Dade elections official confirmed to NBC News. Terry Chavez, spokeswoman for the state attorney's office for Miami-Dade County, also confirmed to NBC News that the investigation was reopened to look into those IP addresses. Chavez said she could release no details on the investigation.

Rep. Joe Garcia won the Democratic primary in the 26th District and went on to win the general election. Jeff Garcia, his chief of staff and no relation, said last week that no state or federal investigators had contacted the congressman's office about the case.

State Rep. Jose Javier Rodriguez, a Democrat who won the District 112 seat, said Thursday that his office had not heard from investigators about the case either. A message left at the legislative office of state Rep. Manny Diaz Jr., the Republican who won the primary and the general election in District 103, was not immediately returned.

The Herald report said that as the requests began coming in, elections officials figured out that they were improper and started blocking the IP addresses. "I guess they finally gave up," the newspaper quoted Bob Vinock, an assistant deputy elections supervisor for information systems, as saying.

People who study election security say the fact that this attempt did not succeed should be of little comfort to election officials. They warn that attempts to attack voting systems are likely to increase.

"In this case the attack was not as sophisticated as it could have been, and it was easy for elections officials to spot and turn back," said J. Alex Halderman, an assistant professor of computer science and engineering at the University of Michigan who studies the security of electronic voting. "An attack somewhat more sophisticated than the one in Florida, completely within the norm for computer fraud these days, would likely be able to circumvent the checks."

Fraudulently obtaining absentee ballots is just one way elections might be subverted by digital means, experts say. Among the other methods and attack points:

- Malware. Rogue software infects millions of home computers across the country. Jefferson said hackers could use malware to change votes or prevent them from being cast in an online election.
- Denial of service attacks. Jefferson said that hackers could use botnets to prevent election-system servers from working for hours, or perhaps longer. In fact, during an election in June 2012, a DOS attack hit the San Diego County Registrar of Voters' website, preventing voters from tracking the results.
- "Spoofing" of election websites. For example, Hoke said, legitimate requests for absentee ballots could be misdirected to another site. The data then could be misused, or the requests could hit a dead end, and voters would be left wondering where their ballots were.
- Exploiting software flaws in digital voting machines, known as DREs. The flaws could allow insertion of viruses or alteration of programming code that would change votes or delete them. (Read one description of hacking a voting machine.)
- Tampering with email return of marked ballots. Experts say email return is troublesome because of the multiple points for attack along the ballots' electronic path. "The overwhelming consensus of the computer science community is don't do it, it's a bad idea," said Jeremy Epstein, a senior computer scientist at SRI International. But in about half the states, email absentee ballot return is an option for members of the military and their families, along with some other U.S. citizens living overseas.
- Wholesale hijacking of an online voting system. In 2010, the District of Columbia Board of Elections and Ethics tested an Internet-based voting system for a week, asking computer experts to probe it for flaws. It took only 48 hours for a team led by Halderman to break in and take control of the site – even altering it so that the University of Michigan fight song played after a vote was cast.

Read the University of Michigan researchers' report on the DC hack (PDF)

In terms of illegally getting access to absentee ballots, Epstein said, the attacker or attackers who failed in Florida might have had an easier time with Washington state and Maryland.

He said that last summer he demonstrated to the FBI a method of changing individual voters' addresses and other information online in those two states by predicting their driver's license numbers.

First he used publicly available information to gain a voter's full name and address. Then, he predicted the individual's driver's license number – which is based on a combination of the person's name and numbers and letters -- and used the information to access their voter registration online. From there, he said, he could have changed their addresses and had absentee ballots sent out.

"Imagine if (attackers) changed the address for 2,500 votes. It could be completely automated, and they have the ballots sent to a post office box or whatever," Epstein said. "Then the registered voters would have no idea until they tried to vote."

In October, Halderman and other researchers sent letters warning elections officials in both states of the

danger of staking system security on driver's license numbers.

The letter to Washington officials (read it here in PDF) also said that other security features in the state's MyVote system would be only a speed bump to a dedicated hacker.

"Although the MyVote system uses a CAPTCHA, an image of distorted text intended to deter simple automated attacks, this provides only minimal defense," the letter says. "Attackers can use commercial services to defeat the CAPTCHA at a cost of less than $0.001 per voter."

Shane Hamlin, assistant director of elections in the Washington Secretary of State's Office, told NBC News that state election officials have acted on the recommendations in the October letter and will require additional information to register to vote or change registration online.

Maryland election officials did not immediately return a call from NBC News seeking comment, but the Washington Post reported last month that Ross K. Goldstein, deputy administrator of the Maryland State Board of Elections, acknowledged the security hole and said the online voter registration system was being updated to address the issue.

"I believe technology can solve problems, and there are steps that we definitely can, and plan to, take to mitigate the risks," the newspaper quoted him as saying.

While elections officials are attracted to the savings that online voting and registration systems promise, the cost of guarding online registration and voting systems is large, Hoke said. And that might negate the financial advantage of online balloting touted by some elections officials and vendors who want to sell electronic voting products.

"It's cheap, if you don't care whether elections are stolen," she said.

That possibility -- of an election being stolen through digital means -- haunts researchers. For Jefferson, it's a matter of national security.

"The legitimacy of government depends on it being impossible for single parties to change the results of elections," he said.

Sincerely,
Sharon Hamilton

Senior Strategist | Analyste principale
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité Publique Canada
340 Laurier Avenue West | 340, avenue Laurier Ouest
Ottawa, Ontario, K1A 0P8
T (613) 990-2735 | sharon.hamilton@ps-sp.gc.ca

Hamilton, Sharon

From: Hamilton, Sharon
Sent: Tuesday, February 05, 2013 11:07 AM
To: Hamilton, Sharon
Subject: The poster child for cybersecurity done right: How Estonia learnt from being under attack

The poster child for cybersecurity done right: How Estonia learnt from being under attack

Summary: In 2007, Estonia was the victim of a high profile campaign of state-sponsored online attacks. Now, years later, the country is promoting cybersecurity via a series of initiatives at home and abroad.

By Kalev Aasmae for Estonia Uncovered | February 5, 2013 -- 10:32 GMT (02:32 PST)

In 2007, Estonia became the first country in the world to be targeted by a large-scale co-ordinated international cyberattack. While the offensive, consisting of a series of smaller distributed denial-of-services (DDoS) attacks, did little damage, it did give the country's security industry valuable experience and information in dealing with such incidents.

Tallinn, home to the NATO Cooperative Cyber Defence Centre of Excellence. Image: Shutterstock

Since the 2007 attacks, Estonia's private and public sector, often working together, have heavily increased the security of the country's IT systems and built stronger authentication services, firewalls and back-up systems.

The country is now rated as being one of the most prepared against cyberattacks, according to a recent report by security vendor McAfee.

With so much of the country's government and public services available online — Estonians can even vote in national elections over the internet — cybersecurity is paramount for the country. Estonia's ID card, digital signatures and X-Road system all use 2048-bit encryption, for example, to keep citizens' data secure.

The beginnings of the online state

X-Road underpins Estonia's online government services, by enabling data to be securely exchanged between the state's information systems online. Along with public sector bodies, private sector organisations can also use X-Road to connect their own systems with the state's using X-Road – for example, in order to allow a user to query a company and a government database at the same time.

How do you solve an IT skills crisis before it happens? Estonia has the answer

- Read more

Estonians can also use their ID card to access government services online. The ID Card, now the primary identity document for Estonian citizens both in the real and digital world, was introduced in 2001. Ten years later, over 86 percent of citizens have ID cards. Holders can use the ID card to provide a digital signature that is as legally valid as a handwritten one in Estonia. Statistics from two years ago showed that approximately 40 percent of ID card owners had used digital ID to authenticate themselves or give a digital signature, and that percentage will only have grown.

With Estonia's adoption of the ID card and digital signature, preconditions for the country's first nationwide elections via the internet were created. In 2009, citizens were able to vote in elections for local government and the European parliament. In 2011, over 140,000 voters cast a ballot in the country's election, meaning that almost every fourth voter gave his or her vote via the internet.

The progress of Estonia as an online-savvy state started largely due to banking, EISA said. Today 99.6 percent of banking transactions are done electronically and the number of users of online banking in Estonia is 1.8 million clients, more than the country's population of 1.3 million.

Estonia's defence forces

With so much of its financial and state infrastructure now online, coupled with being the high-profile victim of online crime, Estonia clearly has an interest in making sure its cybersecurity is up to scratch.

Three years after the 2007 attacks, Estonia founded the Cyber Defence League — a volunteer organisation that operates under the Estonian Ministry of Defence. The body assisted the state during the cyberattacks and its members are mostly IT security specialists from different sectors. The Estonian Police and Border Guard also have their own Cyber Crimes Unit, which investigates and prosecutes online criminal activity.

Around a year later, in 2011, the Estonian Information Systems Authority (EISA) was founded. The body helps both private- and public-sector organisations to maintain the security of their information systems, and it is constantly monitoring cybersecurity threats regarding Estonia.

Estonia has also focused on the availability of education on cybersecurity, and for some years, the Tallinn Institute of Technology has been offering a master's degree programme in cybersecurity, providing opportunities for companies and organisations to gain highly educated workers.

At home and abroad

Estonia is also looking beyond its own borders in the fight against online threats: it has joined and heavily promoted different alliances and arrangements not only in the Baltic states and Nordic countries but also in EU and on a global scale.

And it's not gone unnoticed: in 2008, the Estonian capital Tallinn became the home of the NATO Cooperative Cyber Defence Centre of Excellence and in December last year, the EU's newly founded IT Agency also set up shop in the city.

Estonia's highest officials and representatives have also been championing the cyber-security agenda in Europe.

In November last year, it was announced that Estonia's president Toomas Hendrik Ilves was to chair the steering board of the European Cloud Partnership at the invitation of the European Commission; the function of the Committee is to promote the use of cross-border digital public services in European business and the public sector.

In the same month, European Parliament adopted a report by Tunne Kelam, an Estonian member of the European Parliament, calling for the development of a comprehensive cybersecurity and defence strategy on all levels in the EU.

"We need better co-ordination and more coherence. The EU is currently missing an exhaustive overview of the existing cybersecurity challenges and is also lacking common definitions, standards and a united approach to these threats. Politically motivated cyberattacks are targeting not only the information systems but also critical infrastructures of the member states," said Kelam at the time.

The report urges Europe's member states to press ahead with completing national cyber security and defence strategies and national contingency plans, and also to include cyber crisis management in crisis management plans and risk analyses.

Kelam underlined that cyber security and defence has become one of the core issues in transatlantic relations. The report encourages the EU and the US to deepen their mutual co-operation in countering the cyberattacks. "The 'cyber-dialogue' could be perceived as the new breath of fresh air in transatlantic relations," it concluded.

About Kalev Aasmae

Kalev Aasmäe is a technology and economics journalist, who also writes for the oldest and largest quality newspaper in Estonia, Postimees.

Sincerely,
Sharon Hamilton

Senior Strategist | Analyste principale
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité Publique Canada
340 Laurier Avenue West | 340, avenue Laurier Ouest
Ottawa, Ontario, K1A 0P8
T (613) 990-2735 | sharon.hamilton@ps-sp.gc.ca

Presidential Elections Followed with Malware Attacking Venezuelans

According to Kaspersky Labs the company offering digital security, one fresh PC-virus has been detected that attempts at capturing the Internet credentials of Venezuelans through one web-link, which pretends to provide details regarding the just concluded election for the country's president.

Head of the Research and Analysis Team Dmitry Bestuzhev at the Moscow-situated Kaspersky said in Latin America that perpetrators of the malicious program unleashed it following the presidential election on October 7, 2012 in Venezuela while disseminating it through e-mail. Businessweek.com published this dated October 12, 2012.

Bestuzhev also said that a minimum of 75 customers of Kaspersky as well as others became the malware's target.

According to him, the malware's filename had been called 'listas-fraude-electoral.pdf.exe' that in English meant 'electoral fraud lists.' Clearly, the nomenclature was likely to get a few citizens of Venezuela inquisitive enough following the re-electoral victory of President Hugo Chavez.

The Expert elaborated that potential victims got an e-mail having one web-link embedded. Suppose that web-link was clicked, it would divert the user onto one bogus site that posed as being from 'Globovision' a TV channel of Venezuela.

Interestingly, the malware recognized to be Trojan.Win32.Agent.uael has been created to target Venezuela government employees in addition to routine Internauts.

No sooner is the Trojan planted on a PC it deactivates the UAC (User Account Control) of the OS (operating system). Consequently, the cyber-crooks are facilitated with executing administrative commands devoid of any restriction whatsoever.

Thereafter, the Trojan remains quiet till the victim goes to one website from the total 5, each of a Venezuelan bank. And upon accessing that website, the victim gets led onto one malevolent host where theft occurs of his Internet banking credentials.

Eventually, Trojan.Win32.Agent.uael seizes the login details belonging to government employees after they log into the www.cadivi.gob.ve site which's of The Commission of Currency Administration. Since this Commission provides administering service for legitimate currency transactions inside Venezuela it isn't unnatural for the agency's employees getting attacked.

Conclusively according to Kaspersky, the malicious program getting utilized within the assault has presently been caught via 17 anti-virus engines of the total 44 of ViusTotal.

» SPAMfighter News - 25-10-2012

0 0 4 10

Press Releases - IT Security News

Provided by NewsDesk http://www.infomedia.gc.ca/ps-sp/ Fourni par InfoMédia

Published | Publié: 2012-05-10
Received | Reçu: 2012-05-10 4:14 AM

THE DAILY GLEANER

THE DAILY GLEANER (FREDERICTON)
MAIN, Page: A1

Private voter information accidentally released

Apology | Elections New Brunswick says it's asked parties to return CDs

SHAWN BERRY Legislature Bureau

A privacy expert says the personal information Elections New Brunswick accidentally sent to politicians in recent weeks about almost every eligible voter in the province had the kind of details used by identity thieves.

Elections officials confirmed Wednesday the office released confidential information on almost all of the province's 553,000 voters when it gave MLAs and political parties copies of voter lists in recent weeks.

The details inadvertently sent out included dates of birth, driver's licence numbers and even some telephone numbers. The list the office transmits to MLAs and political parties every spring is only supposed to include the name, address and gender of voters.

Elections New Brunswick said the Liberal and Conservative parties are co-operating with the office's efforts to recover all of the CDs it hand-delivered to the legislature containing the additional details.

The CDs are expected to be returned before the end of the week.

"The information that has apparently been disclosed as part of this supposed breach includes the type of information that could be used to commit **identity theft**, which is probably the No. 1 concern that people have when something like this happens," said David Fraser, a Halifax-based privacy lawyer who runs the Canadian Privacy Law Blog.

He said access to a name, home address, date of birth and your driver's licence number could be used by an impostor to open a bank account or a credit card account.

The good news, he said, is Elections New Brunswick knows who received the information.

"I don't think it's as big a deal in this case, principally because the information went to a relatively closed group of individuals who also probably have motivation to do the right thing," he said, noting no MLA or political party would want to be pegged as the one that didn't give the information back.

"There's no reason to believe it was anything other than an inadvertent error."

Chief electoral officer Michael Quinn said the incident amounted to a mistake his office hopes to resolve through a process that will take two people to approve release of the voters list.

"This is a regrettable situation. It's simply human error," he said.

Quinn said there was no evidence any of the information has been misused.

Ron Armitage, the voter information systems manager for Elections New Brunswick, took responsibility for the breach.

"I take the integrity of individual privacy very seriously and I deeply regret having made this error," Armitage told reporters at a news conference.

While Quinn said his office has been busy gearing up for municipal elections taking place provincewide Monday, he said it isn't the reason for the incident.

"We'll now take the extra precaution of having that procedure reviewed by a second official on future occasions," he said.

"It's fortunate that it went out to 55 responsible people who signed confidentiality agreements. They're in the process now of getting them back to me. I'll have most of them back shortly," he said.

"We'll be asking everyone to sign a declaration that this is the list they received and that if there were any copies made, that we get that copy as well."

Quinn said that under the Elections Act, Elections New Brunswick must provide every MLA the list of electors in their riding on March 31 of each year.

"It's for the purposes of the MLAs, to know who their constituents are, to call them to see if they have concerns and keep in communication with them," Quinn said.

A copy of the declaration MLAs have to sign upon receipt of the list notes it's for the purposes of "communicating with electors ... soliciting contributions and recruiting party members."

Politicians moved quickly Wednesday morning to shed light on the breach.

Premier David Alward said the issue was discovered Tuesday afternoon by an executive assistant to deputy premier Paul Robichaud, who noted the version he accessed contained additional information.

"We have been given something we shouldn't have ... so we will give it back," Alward said in a member's statement at the opening of the legislature.

He said he has full confidence all the MLAs will return the information.

Interim Liberal Leader Victor Boudreau followed suit.

"It's human error and it happens," he said.

"I gave a very clear directive to my caucus this morning and we communicated it to our staff that all copies of these discs are to be returned to the Opposition office and I want to return them to Elections New Brunswick in one bundle to make sure they are all accounted for."

Alward and Boudreau said they instructed MLAs and party staffers to delete any digital copies.

NDP Leader Dominic Cardy said his party didn't receive any voter information from Elections New Brunswick.

"It's serious. I'm glad that the government and the Opposition are taking it seriously, taking steps to return the information and I hope Elections New Brunswick will give us the full report," he said.

Privacy commissioner Anne Bertrand said her office is lending its assistance to Elections New Brunswick at Quinn's request.

"I am always concerned when there's a possible breach of personal information," she said.

"We don't know the full extent of the breach right now. I know they're looking into it."

But she said at first glance this isn't akin to cases where a computer hard drive with personal information goes missing.

The privacy commissioner said in evaluating the risk to the public Elections New Brunswick will need to determine how many of the CDs were actually accessed, who accessed them and whether any of the information was copied or passed on.

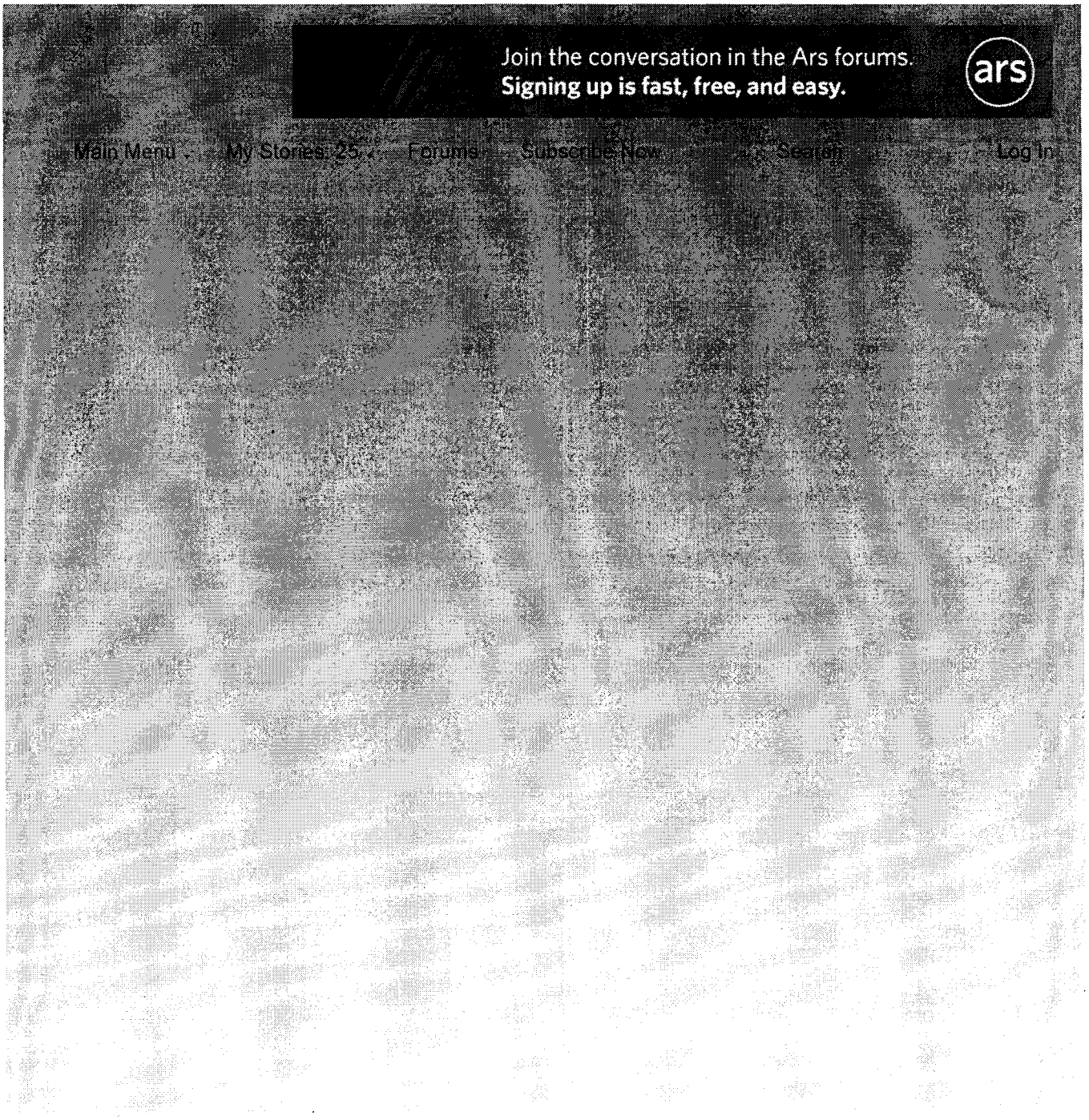
Hamilton, Sharon

From: Hamilton, Sharon
Sent: Thursday, October 25, 2012 5:17 PM
To: Hamilton, Sharon
Subject: The Michigan fight song and four other reasons to avoid Internet voting

The Michigan fight song and four other reasons to avoid Internet voting [...] Even more ambitious than the use of electronic voting machines in polling places would be to do away with the polling places altogether, conducting elections over the Internet. We didn't discuss this option in our previous piece because Internet voting has yet to catch on in the United States, but the topic crops up regularly in discussions (including in the Ars forums). So we thought it would be worthwhile to discuss five reasons it would be a big mistake to allow Americans to cast their votes online: Hacked servers, Client-side malware, Authentication, Coercion and bribery and Usability problems. Reference: http://arstechnica.com/tech-policy/2012/10/the-michigan-fight-song-and-four-other-reasons-to-avoid-internet-voting/

Sincerely,
Sharon Hamilton

Senior Strategist | Analyste principale
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité Publique Canada
340 Laurier Avenue West | 340, avenue Laurier Ouest
Ottawa, Ontario, K1A 0P8
T (613) 990-2735 | sharon.hamilton@ps-sp.gc.ca



LAW & DISORDER / CIVILIZATION & DISCONTENTS

The Michigan fight song and four other reasons to avoid Internet voting

Op-ed: Conducting elections online would be a security and privacy nightmare.

by Timothy B. Lee - Oct 24 2012, 7:35pm EDT

106

Pollypop

In a Monday article, we described the security and reliability problems that have undermined public confidence in electronic voting machines within the United States. We described how several states started scrapping paperless voting machines in favor of paper-based alternatives.

Even more ambitious than the use of electronic voting machines in polling places would be to do away with the polling places altogether, conducting elections over the Internet. We didn't discuss this option in our previous piece because Internet voting has yet to catch on in the United States, but the topic crops up regularly in discussions (including in the Ars forums). So we thought it would be worthwhile to discuss five reasons it would be a big mistake to allow Americans to cast their votes online.

Hacked servers

In 2010, election officials in Washington, DC, provided a good case study of the dangers in Internet voting. They unveiled a pilot project to let members of the military cast their votes online. During a test run, they invited security researchers to probe the system for vulnerabilities. The result: the election website was hacked to play the University of Michigan fight song after voters cast their ballots. Of course, the same tactics could be used to arbitrarily change the election results. In a follow-up report, Michigan Prof. Alex Halderman explained how his team found a "small error in file-extension handling" that "left the system open to exploitation."

Obviously, the specific vulnerability Halderman's team discovered can be fixed. But building a secure website is an inherently difficult problem. "If this particular problem had not existed, I'm confident that we would have found another way to attack the system," Halderman wrote. And that's a problem because there are many parties who might have a vested interest in compromising American elections. For example, foreign governments might be willing to spend significant sums of money to engineer the defeat of members of Congress who they saw as hostile to their interests.

This problem is exacerbated by the decentralized structure of America's electoral process. Decisions about voting technologies are made at the state, and often even the county, level. Even if the largest and most tech-savvy jurisdictions could build a hack-proof voting system—far from certainty—smaller jurisdictions lack the resources and expertise to do so.

Client-side malware

Even assuming election officials could properly lock down their servers, their security woes wouldn't be over. They would also have to worry about security on the millions of client machines that voters would use to cast their votes.

At any given time, hundreds of thousands, if not millions, of American PCs are members of botnets thanks to compromise by malware. Right now, hackers commandeer peoples' computers for nefarious activities like sending spam and participating in denial-of-service attacks.

In a world of widespread Internet voting, the same tactics could be used to compromise elections. Malware could silently monitor a user's Web browsing on Election Day, silently intercept the user's vote and invisibly switch it to the malware author's chosen candidate.

Authentication

Deterring in-person voter fraud is relatively easy. Voters who attempt to cast a vote in person place themselves at risk of prosecution if their fraud is discovered. Also, there's an inherent limit to the number of precincts any single person can visit to cast fraudulent votes on Election Day. In contrast, a single hacker who figures out how to impersonate other voters could potentially cast thousands or even millions of fraudulent votes. That means technical authentication mechanisms would bear a much bigger share of the security burden in an online election system.

America simply doesn't have the kind of authentication infrastructure necessary to support secure Internet voting. For example, driver's licenses are one of the most commonly-used methods for in-person identification. Some states allow voters to change their voter registration online using their driver's license number as an identifier. But security researchers have demonstrated that driver's license numbers are not a secure identifier, since they can be derived from other information about the voter (such as his name and date of birth).

Fortunately, these websites only handled voter registration, not voting itself. But a poorly-designed online voting scheme could be vulnerable to similar attacks, with devastating consequences.

Coercion and bribery

A key principle of modern voting systems is ballot secrecy. Polling places are designed to preserve the secrecy of any particular voter's ballot in order to prevent bribery and coercion of voters. If your boss threatens to fire you unless you vote for his preferred candidate, the secret ballot ensures that you can vote for whoever you want. If necessary, you can lie about it afterwards.

Online voting undermines ballot secrecy. Because voters can vote from anywhere, they can be coerced or bribed into voting with a third party looking over their shoulder.

Traditional paper voting techniques also keep voters' ballots secret from pollworkers themselves. This could be important in jurisdictions where voters might suspect, justifiably or otherwise, that election officials themselves are corrupt. It would be difficult to preserve this characteristic of verifiable anonymity in an online voting setting. Logging into an online voting site will necessarily require presenting credentials that could be tied back to a voter's real-world identity. And while election officials can claim they don't keep records of who cast which votes, it would be hard to design a voting system that allows the voter to verify that promise.

It's worth noting that paper absentee ballots expose voters to the same kinds of coercion risks. This is a key reason that many voting experts are critical of states such as Oregon and Washington that conduct their elections by mail, as well as other states that allow absentee voting on demand. For example, Miami-Dade police recently "arrested two boleteros, or ballot-brokers, on charges of altering ballots of elderly or disabled voters." The *Miami Herald* reports that "absentee-ballot fraud is nothing new, particularly in Miami-Dade, where two local elections were overturned in the 1990s because of phony and forged absentee ballots. In 1976, local elections officials tossed out piles of suspicious absentee ballots cast at Miami nursing homes."

Usability problems

We have no doubt most Ars readers would find Internet voting to be a straightforward and user-friendly process. But not all voters are so tech-savvy. Some elderly voters may have trouble finding the online voting site, may not know they have to click the "submit" button after clicking their choices, may get confused by error messages, and so forth. Traditional paper ballots have a comparatively straightforward user interface, and there are always pollworkers on hand to explain the process to voters if they get confused. Paper ballots certainly aren't perfect, but for many voters they're likely to be the least confusing option.

Of course, technological progress may eventually solve some of these problems, so it would be foolish to say that Internet voting will never be a good idea. But right now, we are nowhere close to being able

to conduct secure, reliable, private, or user-friendly elections over the Internet. Physically traveling to a polling place to fill out a paper ballot remains the safest, cutting-edge method for choosing our leaders.

READER COMMENTS 106

Timothy B. Lee | Timothy covers tech policy for Ars, with a particular focus on patent and copyright law, privacy, free speech, and open government. His writing has appeared in Slate, Reason, Wired, and the New York Times.
@binarybits

← OLDER STORY | NEWER STORY →

YOU MAY ALSO LIKE

Beaudoin, Luc

From: [redacted]
Sent: Tuesday, October 09, 2012 1:15 PM
To: CCIRC-CCRIC; [redacted]
Cc: [redacted]
Subject: RE: CCIRC CE-12-003695 [Halifax Internet Voting]

Good day . Electronic voting has been proceeding well since Saturday am. Just over 5% of eligible voters across HRM have cast their ballots with just under 10% casting their ballots by phone.

Most sincerely;

[redacted]

-----Original Message-----
From: CCIRC-CCRIC [mailto[redacted]
Sent: October-09-12 11:32 AM
To:[redacted]
Cc: [redacted]
Subject: CCIRC CE-12-003695 [Halifax Internet Voting]

Dear [redacted]

We appreciate your feedback. How was the vote on Saturday, October 6th, 2012?

Thank you,

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
www.publicsafety.gc.ca

par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

s.16(2)(c)
s.19(1)
s.20(1)(c)

-----Original Message-----
From:
Sent: October-05-12 11:07 AM
To: CCIRC-CCRIC
Cc:
Subject: Re: CCIRC CE-12-003695 [Halifax Internet Voting]

Dear Mr(s),

Find here under our feedback to your concerns about the overall security of our solution for the HRM Elections 2012.

[redacted]

In the event you need any further information, please don't hesitate to contact us again.

Kind regards,

[redacted]

Senior Consultant

s.16(2)(c)

s.19(1)

s.20(1)(c)

[redacted]

On Thu, 10/04/2012 05:18 PM, "CCIRC-CCRIC" < [redacted] > wrote:

Greetings,

CCIRC would like to raise the following concerns with your organization:

[redacted]

[redacted]

Acknowledging that this is not the first time such system is used in Canada. Due to the Poll will be open on October 6th, 2012; we appreciate your taking the time to get back to us with a response.

s.16(2)(c)

Cyber Duty Officer
Public Safety Canada
CCIRC

[redacted]

http://www.publicsafety.gc.ca

[redacted]

NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

s.16(2)(c)

AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Reference:

[redacted]

s.16(2)(c)
s.19(1)
s.20(1)(c)

Beaudoin, Luc

From: [redacted]
Sent: Wednesday, October 03, 2012 11:40 AM
To: CCIRC-CCRIC
Cc: [redacted]
Subject: Fw: CCIRC CE-12-003695 [Halifax Internet Voting]

Attention Virvak Phlek,

As per our conversation this morning, please send any concerns regarding the Halifax Region Municipal election. Please copy all on this email, as they will be addressing the concerns.

Thank you,

[redacted]

From: Election, HRM
Sent: October 2, 2012 4:37 PM
To: [redacted]
Subject: FW: CCIRC CE-12-003695 [Halifax Internet Voting]

-----Original Message-----
From: CCIRC-CCRIC [mailto:[redacted]
Sent: October 2, 2012 4:37 PM
To: Election, HRM
Subject: CCIRC CE-12-003695 [Halifax Internet Voting]

Good Day,

The Canadian Cyber Incident Response Centre (CCIRC)* has received a report that raise some concerns regard to Internet Voting Campaign. Would it be possible for you to contact CCIRC to discuss those issues? Please provide this reference number CE12-003695 for any further correspondence relate to this matter.

Kind Regards,

s.16(2)(c)
s.19(1)
s.20(1)(c)

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
www.publicsafety.gc.ca

--

[redacted]

[redacted]

s.20(1)(c)

Beaudoin, Luc

From: Beaudoin, Luc
Sent: Tuesday, October 02, 2012 1:18 PM
To: Phlek, Vireak
Cc: CYBERDO
Subject: CE12-003695

I need you to take this on for me. See event number. There is a PDF attached. I need you to contact the vote system developer and walk them through this so they improve their implementation.

This is URGENT. Their election is 6 October !!!!!

ictsd@halifax.ca or (902) 490-4444

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>

PublicSafety.gc.ca | securitepublique.gc.ca

Government of Canada | Gouvernement du Canada

par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Beaudoin, Luc

From: [redacted]
Sent: Friday, September 28, 2012 2:46 PM
To: CYBERDO
Subject: See message
Attachments: CCIRC Halifax Election Concerns.pdf.pgp

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG/MacGPG2 v2.0.17 (Darwin)
Comment: GPGTools - http://gpgtools.org
Comment: Using GnuPG with Mozilla - http://www.enigmail.net/

hQIOA4v7Lo5QmG2hEAgA5Q5uLhnSm+vT8+xC6mcc7SGmn0X1zDtqk2ggpdTZMVCr
gugTo0dHGe1hw0v+ayyC5etItAc0/N9u0y1jgZISsSX2Jf5vknEKsooGg69mCzZn
gYZb4IMFvHyKwRNJN0Ngfd+WmSTRr4uwMqHyqe8tcZJNjE3MipSTXNZLNVLTN114
uO7x88lHjX1+NFxJOK335uTOktoU1+WnLmgUHDGF3UiHEsE58aK56SGUlhS1X2w1
AluX+tijdTIq/XYxFXzyP0TVft4puEj2IdAQzGvHYBH088TxZC/K9Zmx7vqdcsLw
4WbnhvXE5z2l5eV+sEQBPl9IycGRg14+BMo/+cpM4Qf/XviBDtYZQ1aEogWZnFF2
tEG2jStISu5V1SylQFn6QLKcwXIGn0jPuj1/+dXKanlUWxOIOkNbhfN+DgNSpyc/
sgvsmYexsrso7IB2xr9KANHBUJFe/GuQSZ9dU0bPRO8ksV9zt5tnW9EHWV6uJKhQ
gXT2bwSqVktV32t6OcGKDm7x8ECnh52XSFQs32vOkPxFBFaNQN2SOIu2IJSu8XER
3ZsF1xVef7v7y9QlXw9GUoQQefyGE5Bh6TR49eDeA2spF1ecfeMX7nWIF00t5n/F
x9uI+p0aaylevzqIaXHF5ohgLs8YK9GKCtI3fXz63YKISCBCuoHzVU+pN5SpVnBo
AIUCDANKI0yj5bX7NQEP/1zXDsBG3DmuMZ4a5cDejYcDNgNr5q6G7N90wYW4B7zz
P771QcUXqMBmOwKWikNUCIz1II9NjYScb+s5xPBJfSHOB2BnQKEJWEtI6cbJrdGn
IMDKIJPnGiM+gtsHdVIItA70LvZpJRAWadMJz+1ydyDJ7ZbrItSkAdyZ21CSSAOf
cQJ7zFVEDuPKJ/eCMk/nsxlgodooSsrLXQmmfXKUfe8azM97MTCLDXxRDGvr7aRz
h73tM1zAE9WIIszL10Jl2zhOKOu/EYln2QRoREXzLocT1x19oGGSLDfhBg/eyK2h
k021doZM8j8FveH7RxM9u5MZYjShpaG+jam+34zJlEFKkIvwwkv4ZkjDhrBsagaj
sLB/kKliet7vO+q1aW+ET6el0+Y31E/IMVdw2UEMXwgTphEso5L2rU6lvgvT+qog
WL5StPa3h7+20lhzn+fTd+zLSdkBuIAjpxJaeuz25fXdOW8gMtbKlYNxD+/dUcp9
choGVCF1DpIREYL2fLQcsd6TQncYK1Ia6oOiBWkQ3hp3bmWgcHLHTO10HX3ylplJ
Xnb879FsxXGXn47CP3LRfIOT89LSiHOLjiYZnOtGhE2ocVpM5Hx13KSKhF3FhmYj
4AZfJ3mcO0G9pY8OAC0Bj9W9ouGwHVN/GOidzDuAvCEvt+HUhGX1oiZMWSov0NYm
0oYBERQkSPiFV2Fi5k4CH6gev9puPihNVCFGwkjf5b3FdR2HGAPAqcB7KrNhPb0F
nOpkYe+1V4Piulvrrd2QD9sej/Ipav8s5koZJJAaV0+oIV1uex06YlocBJlxXiRW
33qaw5gO1W0YKId6DeC5LbPaUFK3v4uHxSbHi0rq+LHqrSSDRg2MUQ==
=Lr5P
-----END PGP MESSAGE-----

[redacted]

September 28, 2012

ATTN: Candian Cyber Incident Response Centre (CCIRC)
FROM: [redacted]

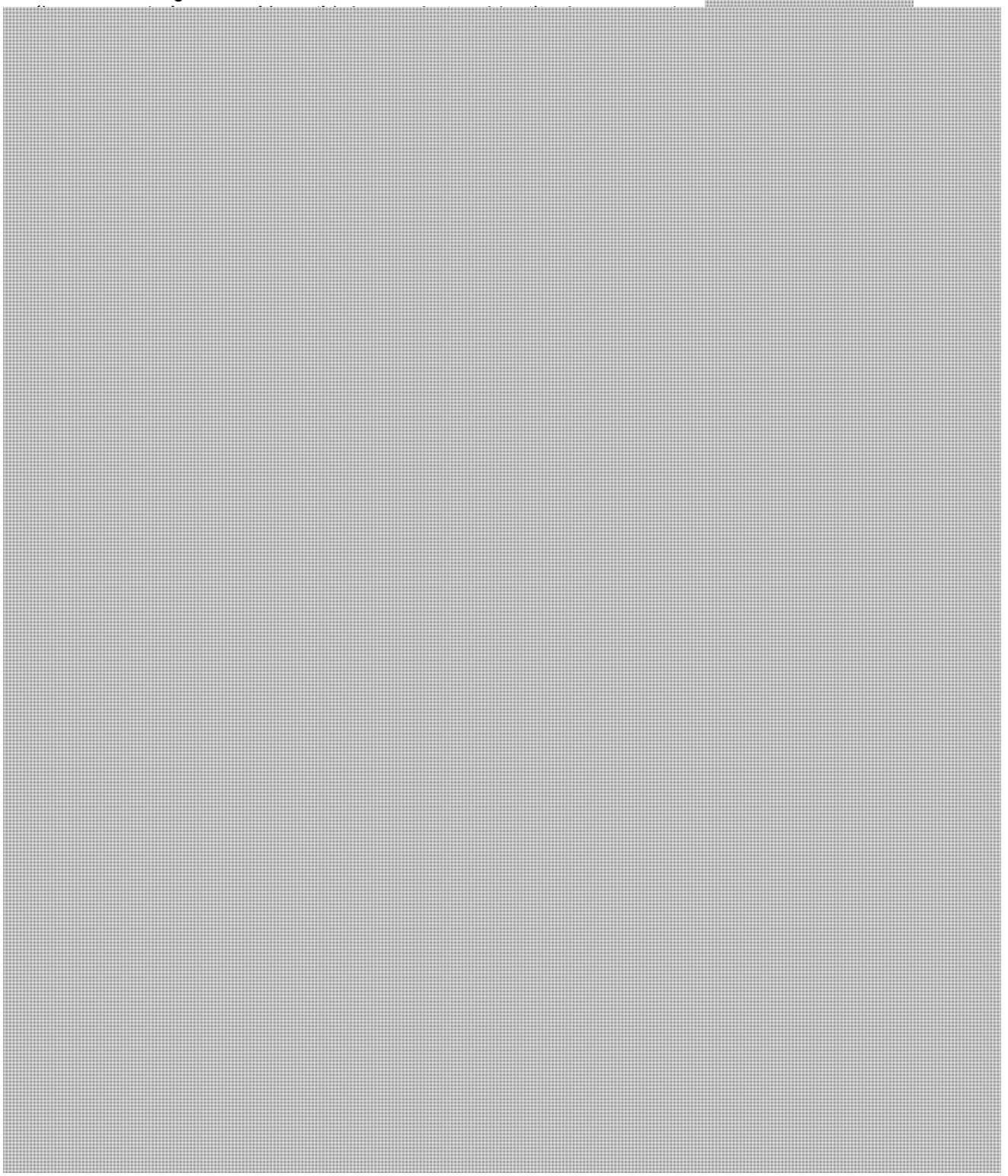
[redacted]

[redacted] Before election day voters are provided a card directing them to visit "vote.halixfax.ca". The voting card example found at http://www.halifax.ca/election/evoting12.html does not contain instructions to use a HTTPS url or instructions on how to verify the polling site identity presented to the voter. All major browsers will interpret a voter input of 'vote.halifax.ca' to mean http://vote.halifax.ca.

[redacted]

[redacted]

As of 10 Sep 2012, the Halifax election site presents the login link as a third-party domain, with voters being directed from the vote.halifax.ca site to securevote.ca.



Page 33

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Beaudoin, Luc

From: [redacted]
Sent: Thursday, September 27, 2012 6:03 PM
To: Beaudoin, Luc
Subject: Updated CCIRC contact

Hey Luc,

Are you still in this role? May have some vulnerability info for you affecting the Halifax online election coming up.

--

[redacted]

Beaudoin, Luc

From: [redacted]
Sent: Tuesday, September 04, 2012 4:40 PM
To: [redacted]
Cc: Beaudoin, Luc
Subject: RE: Under attack - N1-U1

Hi [redacted]

Any significant anomalies in traffic get picked up by netflow monitoring, and go to the NOC for action. Good luck!

[redacted]

From: [redacted]
Sent: September 4, 2012 02:37 PM
To: [redacted]
Cc: [redacted].uc.Beaudoin@ps-sp.gc.ca
Subject: RE: Under attack - N1-U1

Hi [redacted]

Just came out of a meeting on this. They have installed an IPS in rush over the weekend to add a layer of protection. They should be OK.
At this point, not sure I could (they couldn't) be specific on what to look for except for anything that seems to be triggered to news agencies in the province of Quebec. That's too large for a request but if any of you happens to see anything.. [redacted] will be on a proactive bridge with them to this subject tonight and keep us posted should anything occur.

Thanks again,

[redacted]

Devez-vous imprimer ce courriel ?

s.16(2)(c)
s.19(1)
s.20(1)(c)

[redacted]

2012-09-04 12:20

A

[redacted] "Luc.Beaudoin@ps-sp.gc.ca" <Luc.Beaudoin@ps-sp.gc.ca>

cc

Objet

RE: Under attack - N1-U1

Hi [redacted]

I'll see what I can dig up in flow records w/ PfSP.

Do you recommend/request us to watch for traffic like tonight?

[redacted]

From: [redacted]
Sent: September 1, 2012 01:23 PM
To: [redacted] Luc.Beaudoin@ps-sp.gc.ca
Subject: Under attack - N1-U1

Hi all.

N1 - U1

s under attack since yesterday 20h00. Might be a UDP bomb on port 80. One of the attacking address seems to be
The attacked addresses are
The fear is that it might be a practice for next Tuesday's election night
Have you seen anything throu your monitoring tools or other means ?

s.16(2)(c)
s.19(1)
s.20(1)(c)

Thanks

Devez-vous imprimer ce courriel ?

Beaudoin, Luc

From: Murphy, Gregg
Sent: Tuesday, March 27, 2012 11:38 AM
To: *[redacted]
Subject: NDP voting company calls disruption attack deliberate

Of interest: ... Scytl, has identified more than 10,000 IP addresses, mostly in Canada

"An attack on the online voting system used to select Thomas Mulcair as the leader of the NDP on the weekend needed a level of organization that points to a deliberate effort to disrupt the leadership race, according to the company that created the electronic ballots.
The company, Scytl, has identified more than 10,000 IP addresses, mostly in Canada, that could help identify the people behind the attack, which slowed down voting and denied party members access to the website used for voting.
Scytl says in a news release that "the required organization and the demonstrated orchestration of the attack indicates that this was a deliberate effort to disrupt or negate the election by a knowledgeable person or group.""
Reference: http://www.cbc.ca/news/politics/story/2012/03/27/pol-ndp-voting-disruption-deliberate.html

Gregg Murphy
Incident Handler | Agent chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

Beaudoin, Luc

From: Dick, Robert
Sent: Sunday, March 25, 2012 12:08 AM
To: Beaudoin, Luc; Anderson, Windy; CYBERDO
Cc: Bendelier, Kenneth; Clow, Patrick; Champoux, Martin
Subject: Re: Ddos against NDP

s.16(2)(c)
s.20(1)(c)

Merci, Luc.

----- Original Message -----
From: Beaudoin, Luc
Sent: Saturday, March 24, 2012 11:19 PM
To: Anderson, Windy; CYBERDO
Cc: Bendelier, Kenneth; Clow, Patrick; Champoux, Martin; Dick, Robert
Subject: Re: Ddos against NDP

Correction on the source IP(s). Still looking at actual source location.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: Beaudoin, Luc
Sent: Saturday, March 24, 2012 11:15 PM
To: Anderson, Windy; CYBERDO
Cc: Bendelier, Kenneth; Clow, Patrick; Champoux, Martin; Dick, Robert
Subject: Ddos against NDP

Report of cyber attack against NDP convention in the news.

The reports of DDOS against NDP website refers to 2 IP addresses as attacking sources.

CCIRC was informed through trusted channels of one possible IP, located

Information obtained by CCIRC indicates DDOS was active EST.

NDP convention leveraged on-line voting.

NDP.ca is hosted by

NDP convention apparently unfolded without major impact. NDP authorities were reportedly aware of the attack as it occurred earlier this afternoon.

No additional information is available at this time.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

Beaudoin, Luc

From: Loyer, Jean-Francois <Jean-Francois.Loyer@elections.ca>
Sent: Friday, January 07, 2011 2:20 PM
To: Carter, Eric; Williston, Sandra
Cc: Bazinet, Denis; Beauregard, Danielle
Subject: Re: Cyber Event CE11-4379 Shadowserver DRONE Report HTTP Bot.msg

Thanks Eric.

JF

----- Message d'origine -----
De : Carter, Eric
Envoyé : Friday, January 07, 2011 02:17 PM À : 'sandra.williston@ps-sp.gc.ca' <sandra.williston@ps-sp.gc.ca> Cc : Bazinet, Denis; Beauregard, Danielle; Loyer, Jean-Francois Objet : RE: Cyber Event CE11-4379 Shadowserver DRONE Report HTTP Bot.msg

Good Afternoon,

Thank you for your assistance is this matter. The offending machine has been found and the problem addressed. Additionally, we will be examining both our technical controls and Training & Awareness preparations to avoid re-occurrence.

Eric

Eric Carter

IT Security
Tel: (613) 949-3707
E-Mail: Eric.Carter@Elections.ca

-----Original Message-----
From: Williston, Sandra [mailto:sandra.williston@ps-sp.gc.ca] On Behalf Of CYBERDO
Sent: January 5, 2011 10:49 AM
To: Cousineau, Stéphane; Beauregard, Danielle; Loyer, Jean-Francois; Kreis, Rocky; EC-Cyberdo; Lalonde, Anne-Marie; Bazinet, Denis
Cc: CYBERDO
Subject: Cyber Event CE11-4379 Shadowserver DRONE Report HTTP Bot.msg

Good Day;

CCIRC has received a report from the Shadowserver Foundation listing host(s) in your IP space associated with potentially malicious network behaviour.

The following listed IP was reported to be generating BOT activity traffic. Shadowserer describes how they determine "BOT" activity. Shadowserver collects a list of all the infected machines, drones, and zombies that they are

able to capture from the monitoring of IRC Command and Controls and capturing IP connections to HTTP botnets. Timestamp the IP was seen in UTC+0.

timestamp,ip,port,asn,geo,region,city,hostname,type,infection,url,agent,cc,cc_port,cc_asn,cc_geo,cc_dns,count,proxy,application,p0f_genre,p0f_detail
04/01/2011

[redacted]

CCIRC recommends that your security team investigate hosts associated with the provided IP(s) for this timestamp.

Additional info: Shadowserver's Permanent Sinkhole IP address is [redacted] If you observe any internal host attempting connection outbound to this IP should be investigated.

s.15(1) - Subv
s.16(2)(c)
s.20(1)(c)

[redacted]

Thank you. If you have any questions, please contact CCIRC.

Cyber Duty Officer
Public Safety Canada
CCIRC
[redacted]
www.publicsafety.gc.ca

Beaudoin, Luc

From: Williston, Sandra on behalf of CYBERDO
Sent: Wednesday, January 05, 2011 2:56 PM
To: CYBERDO; 'Stephane.cousineau@elections.ca'; 'Danielle.Beauregard@elections.ca'; 'jean-francois.loyer@elections.ca'; 'rocky.kreis@elections.ca'; 'EC-Cyberdo@elections.ca'; 'anne-marie.lalonde@elections.ca'; 'denis.bazinet@elections.ca'
Subject: RE: Cyber Event CE11-4379 Shadowserver DRONE Report HTTP Bot.msg

Follow Up Flag: Follow up
Flag Status: Completed

Good Afternoon;

Further to our email below. A second Shadowserver report provides further information which may assist in locating the affected system(s):

COLUMN_HEADERS
timestamp,ip,asn,geo,url,type,http_agent,tor,src_port,p0f_genre,p0f_detail,hostname,dst_port,http_host,http_referer,
http_referer_asn,http_referer_geo,dst_ip,dst_asn,dst_geo

DATA

Hope this helps.

Cyber Duty Officer
Public Safety Canada
CCIRC
www.publicsafety.gc.ca

-----Original Message-----
From: Williston, Sandra On Behalf Of CYBERDO
Sent: January 5, 2011 10:49 AM
To: 'Stephane.cousineau@elections.ca'; 'Danielle.Beauregard@elections.ca'; 'jean-francois.loyer@elections.ca'; 'rocky.kreis@elections.ca'; 'EC-Cyberdo@elections.ca'; 'anne-marie.lalonde@elections.ca'; 'denis.bazinet@elections.ca'
Cc: CYBERDO
Subject: Cyber Event CE11-4379 Shadowserver DRONE Report HTTP Bot.msg

Good Day;

CCIRC has received a report from the Shadowserver Foundation listing host(s) in your IP space associated with potentially malicious network behaviour.

The following listed IP was reported to be generating BOT activity traffic. Shadowserer describes how they determine "BOT" activity. Shadowserver collects a list of all the infected machines, drones, and zombies that they are

Page 44

is a duplicate

est un duplicata