

Business Browsing Insecurity

Mark Linton (CISSP, CISM, CGEIT, CISA, PCI-QSA)
Director - TripleCheck Consulting Inc.

Browsing Insecurity

- Business use of the Internet, really!
- The browser's risky lineage
- Threats, vulnerabilities, controls
- Ideas for improvement

Internet Reliance

- Web based interfaces are the standard
- Cloud computing is easy (no meteorology degree required)
- Social networking
- Wireless



1.966 Billion people (29% of people on earth) estimated to be using the Internet today. In just 10 years we've included 5x the the 360 million people that were using it in 2000.

We've commoditized and moved most common services to the "cloud" which is really just a fancy name for browser based services.

Social networking and Internet based connections are driving our marketing, advertising, and recruitment

The use of cell phones, smart phones, ipads, netbooks, etc is growing. People demand real-time anytime access to all their services – seen as convenience.

Browser Basics

- Originally built to interpret and display HTML 1.1 (1995)
- The browser is now the computer
- We've built a ton of disfunctionality on top of HTML (java/script - flash - acrobat)
- Cannot live without it!

Browser was invented in the early 90s as software to interpret and display the first internet language HyperTextMarkupLanguage. People probably remember Netscape and later Internet explorer as the popular choices.

Since then it has evolved to provide an entire computing environment in the browser with java, flash, pdf, and other technologies. Google's latest efforts include the ChromeOS which is a browser based operating system.

All of this extra functionality builds on the HTML language to enhance our experience with fancy interfaces, and interaction.

We are to the point now that our lives are completely dependent on the use of the browser, from reading news and email to complex supply-chain and business applications.

Reality - vulnerability

- Browser vulnerabilities are common across all major platforms*
- Microsoft Internet Explorer (51)
- Mozilla Firefox (95)
- Google Chrome (140)
- Apple Safari (113)
- Google paying (\$3133.7) for vulnerabilities

* Statistics from secunia.com/factsheets

Vulnerabilities are mostly problems with the way that browsers are programmed. They typically lead to the execution of unauthorized software on the vulnerable persons computer. Criminals use these vulnerabilities to gain access and control of the users computer.

New and variants of browser exploits and payloads are created non-stop and are very quickly integrated into the kits.

Most of the public research data released gives us data on vulnerabilities that are disclosed, we also know that there are many vulnerabilities for every platform that are not.

Vulnerability research is a profitable line of work, google is offering up to \$3133.7 for finding security bugs in the latest version of the Chrome browser. Even more attractive is that undisclosed critical browser vulnerabilities are often worth 10x times that amount.

Reality - the threat

- Motivation, means and opportunity
 - Criminal motivation driven by easy conversion of data to cash.
 - Browser hacking tools are easy to acquire.
 - Everyone browses the Internet, just a matter of getting them to www.clickhere.com
 - [click!](#)

Why has this become such a problem? You and your organization's information is valuable.

Credit card does anyone know how much credit card data (track 1 and cvv2) is worth in the carder networks? \$1.50 US card \$1.75 for Canadian cards.

Entrepreneur criminals creating reliable exploits and payloads are packaging them together in commercial exploit kits. Popular ones include "Eleonore, JustExploit, and Liberty" are popular ones. These kits are designed to be highly effective by including exploits and payloads for combinations of browsers and platforms.

The whole scheme is centered around getting access to your information.

What's the risk?

- Users expect unrestricted access to the Internet. CBC, online banking, facebook, twitter, NHL, etc.
- Our personal and work browsing habits are usually the same. We like to click!
- This results in a high infection-rate of users.
- Which group of staff have the highest infection rate?

We use the internet to access valuable information. Almost all Canadian banks have incentives for people to do electronic banking. We use these browser based services to book travel, communicate with our customers, and complete electronic transactions.

We also use these services to communicate and manage other sensitive data such as business plans, financial statements, merger and acquisition information.

At the same time we open a new tab and surf facebook, access web mail, and watch video and other content.

Our expectation is that the Internet is open and accessible whenever and where ever we are. Airports, hotels, home, work, behind the wheel.

What's the Impact?

- Malware infection
 - Trojans and keyloggers - your computer is now under their control
 - Ransomware - encrypting files and demanding payment to decrypt
- Data compromise
 - Fake sites, stealing usernames and passwords

As the threats have changed so have the impacts. Data loss is obvious, and they are getting more efficient at getting it.

Once exploited the code enables the individuals full control over your computer. They can use it to infect others, participate in botnet denial of service or use it as a pivot to compromise other high value computers within your environment.

They're are also using browser vulnerabilities to extort people with ransomware that encrypts data that it can find and demands payment for the decryption key.

Targeted attack impacts are the lowest probability but have the highest impact, the Google incident in which the intruders were after source code have a very high impact on the businesses affected.

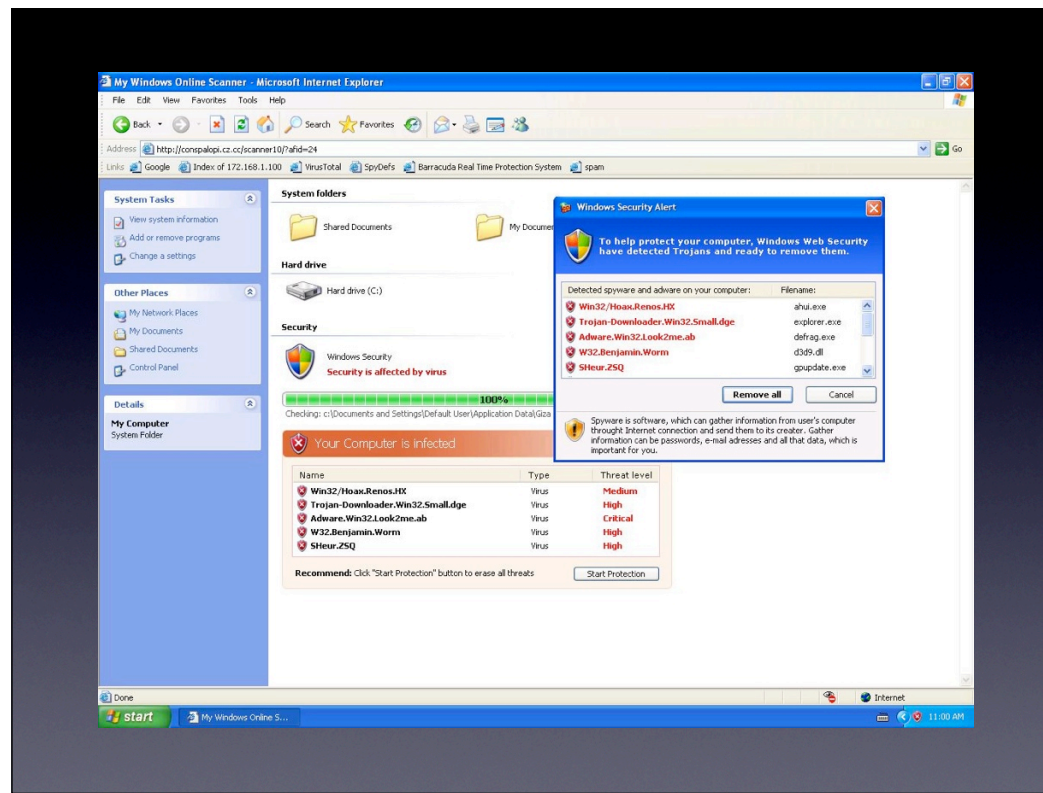
Our controls work, right?

- User awareness
 - We are trained and conditioned to make poor decisions regarding clicking “Ok”.
 - Passwords are hard to remember so we create one and reuse it everywhere.
 - Security is confusing

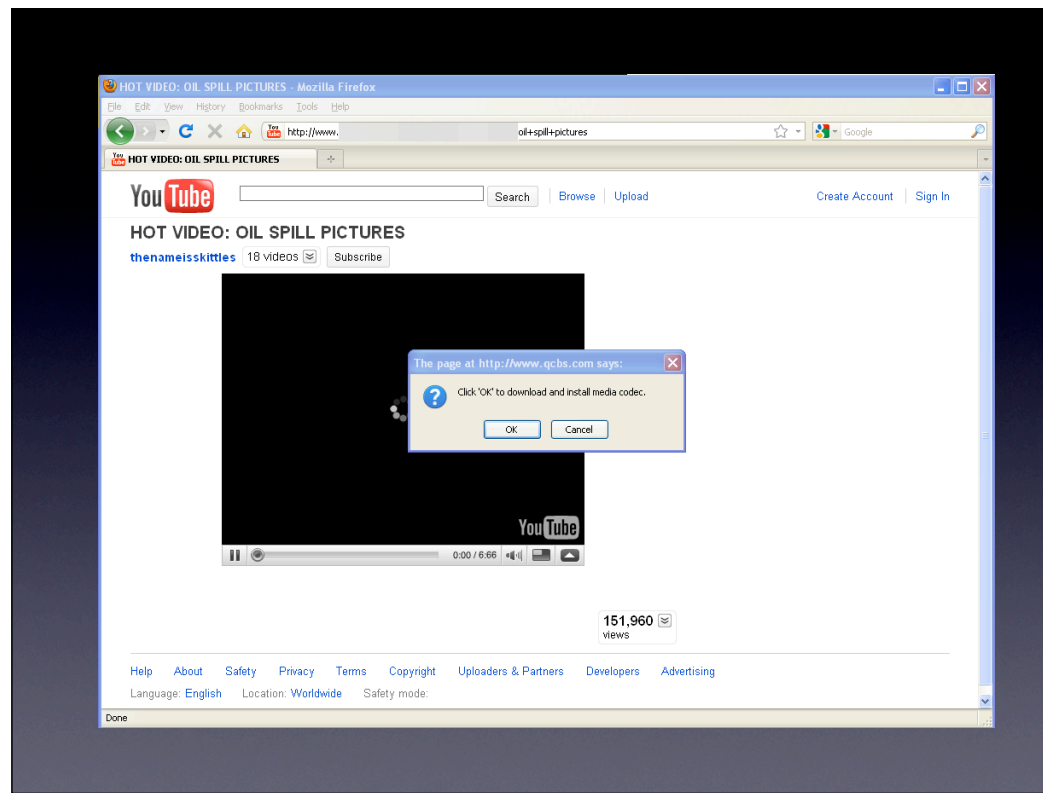
As users we are used to the process of having to install software to get things to work. I've seen many software test scripts which include installation of additional Java components, clicking OK to browser security prompts, and following redirections.

Passwords, this is my favorite. Too many examples here to mention, but almost everyone is guilty of reusing passwords across sites and never changing them.

Each new version of our browser comes with some new security feature, now the icon has a lock, now its green, now there is a message when a site tries to redirect you, now you get alerted when content is coming from different domains. Its hard to keep up with as a security professional, how do we expect average users to understand?



This is an example of a fake-av page. The user was browsing a trusted site, and got redirected. They get a prompt the alerts them they are infected and offered an opportunity to “clean” their computer. But by clicking remove all they are installing malicious code that allows a bot-net to take control of their computer.



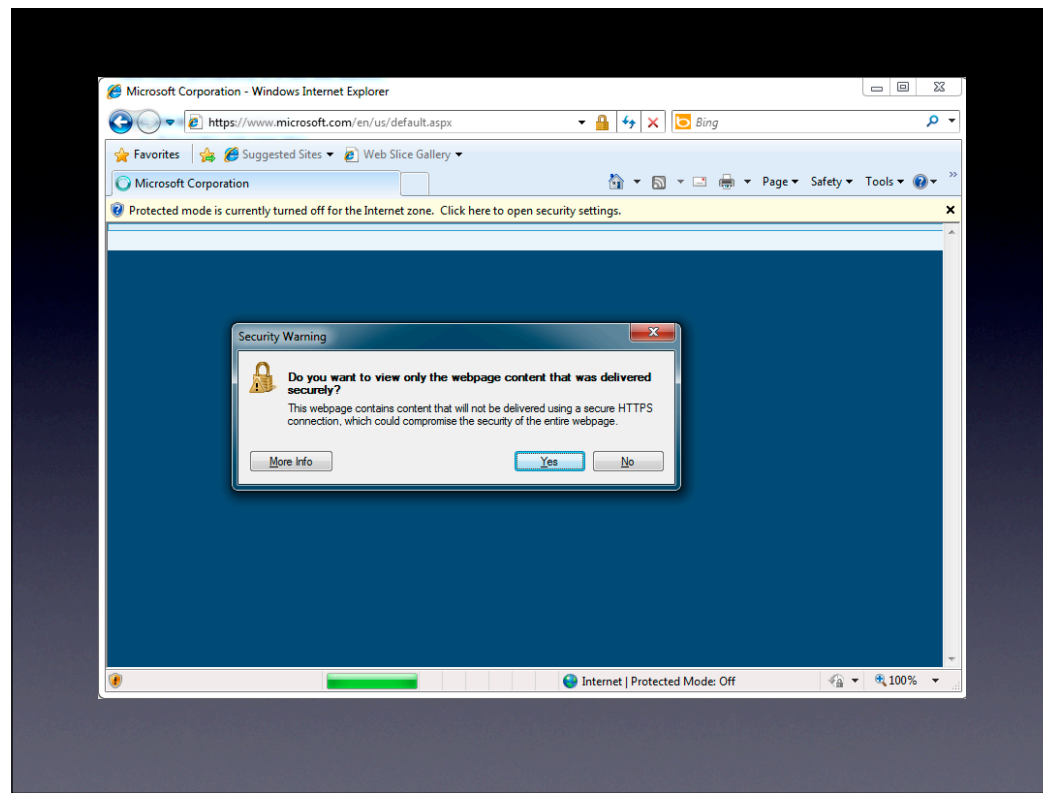
Another good example of this. I just got sent an email link to some popular video on youtube. Of course I have to install a new plugin for my browser to view the video which I've had to do for other services, seems reasonable?

Our controls work, right?

- Which of the following do you use to judge the security of a site?
 - Uniform Resource Locator (URL)
 - includes HTTPS? color? X'd out
 - what is the FQDN?
 - Lock icon? title/status bars?
 - Security pop-ups and warnings?

A little bit confusing right? They have built a ton of features into browsers to help users make good decisions. Here are a few.

One of the problems is that different browsers and successive releases of browsers have different features and behaviours. Not to mention all of the extra plugins like flash and java that have their own security features on top of these.



This is the latest version (8.0) of Microsoft's Internet Explorer, running on the latest version of the Windows 7 operating system. I simply typed <https://www.microsoft.com/> into the URL and hit enter.

URL bar, seems ok I've got a lock icon on the far right that is yellow, but now I also have a security status bar that indicates that protected mode is turned off for the Internet zone, and a Security Warning prompt that's asking me if I want to only view the content that was delivered securely, but that it might compromise the security of the entire webpage.

I also have a small orange shield with an exclamation mark in it down here, and something else regarding protected mode: off on the bottom.

But as a responsible user I'm going to give the service desk a call and find out what the safest thing to do would be.

Our controls work, right?

- Anti-virus (1980s) - 2009 - \$7B*
 - Often relied upon as a panacea for security
 - Signature based, only good at finding known issues
- Browser Patching
 - Patch Tuesday = Malware Wednesday

* Statistics from Computer Magazine

So the browser is vulnerable and its trivial to get users to click and ignore security warnings, that's why we've got other controls.

Anti-virus, first known use of software to clean an infected computer was in the mid-80s. Original design was to identify virus code and remove it. The size of the AV market is not measured very well, but a conservative estimate in 2009 was about 7 billion dollars a year industry.

The other control that helps compensate for browser insecurity is patching. Microsoft uses a monthly release cycle to release fixed security issues, every second tuesday patches for Internet Explorer are released. As you might expect, criminals wait until the day after to start using the newly discovered vulnerabilities. To their credit Microsoft has started releasing interim/OOB patches for serious issues.

Our controls work, right?

- Incident Response
 - We often treat the symptoms, cleaning systems, locking down sites, etc.
 - Root cause analysis takes effort to determine and often we don't collect the data to support it.

So lastly, if the user clicks, the browser breaks, and the AV doesn't catch it, what do we do?

Most organizations have some form of incident response to try to isolate and contain the damage, but we still see many issues. We tend to treat the symptom and not the problem, focused on cleaning/rebuilding compromised computers, and not the issue of hazardous clicks on email and web links.

Root cause analysis takes real effort and understanding, we don't always have the staff to do it, outsourcing can make this harder.

We also don't always collect the data necessary to understand what happened. When did this happen? Who was the user? what link did they click? what site did they visit? what software was run? what data might have been compromised? Without the capability to search this data, its not possible to determine the root cause.

Our role in improving

1. Prevention - Safe-browsing (train and test users resistance to clicking “OK”)
2. Bring the pain, IT staff don't need to browse youtube from the domain controller
3. Stay current with new control designs
 - Monitor and control the network
 - Prevent browser infections (sandboxing)

As a security professional I believe our role is to educate ourselves in how these threats operate, and ensure we employ controls which are as effective as possible in preventing, detecting, containing and responding to browser based attacks.

Educating our users is important – they should be trained on how to spot common weaknesses and respond to vulnerabilities – test their knowledge with real scenarios, send phishing emails, what percentage of people click it? if they do, send them to page that reinforces their understanding of the risks.

Restrict Internet access – system administrators, finance staff, on-line banking. Use specifically hardened and isolated computers to perform these sensitive tasks. Train these users on specific browser security features that they need to pay attention to.

Stay current with new preventative controls. Prevent connections to known-bad destinations. There are lists of these bad domains that can be subscribed to, and methods of not allowing their resolution. Some AV vendors have these features, but they are not enabled by default! Other new technologies include browser enhancements

Our role in improving

4. Prevent communications with known bad sites - do we really have suppliers/customers in latvia?
5. Promote and maintain good password habits.
6. Improve incident response. Start by logging.

Many of the sites that are serving compromised web pages are located in areas that have lax laws and ability to crack down on criminals. There are lists of these compromised sites and domains and tools which allow you to prevent connections to them.

Passwords, use strong unique passwords for different services.

My personal favourite is logging, we can enhance our ability to respond and understand issues by simply turning on logging of which sites are visited, what software is installed, and which users are responsible. Focus on the outcome of understanding the risk and not punishing the user. Use the data to educate management and staff, and prioritize other controls.

Our role in improving

- IT Audit and management need to understand these risks and adjust their audit approach (don't just check if AV signatures are updated)
- Reporting, containing and investigating incident root cause is key to ongoing effectiveness.

For those auditors in the room, it's our job to also raise awareness of this risk, and measure the effectiveness of our controls. I've seen too many audit reports with a checkbox for updated antivirus signature files, which promotes a false sense of security.

Audit procedures and results should be focused at root-causes and impacts not just on control existence.

Are you infected now?

If you monitored your network today, would you find infections?

Difficult question - Would the risk they pose be acceptable?

What methods would you use to improve?



A few final thoughts and questions to leave you with.

If you were able to identify infected computers in your environment how many would you find?

Would the risk they pose to your organization be acceptable?

How would you improve?

Questions / Discussion?

- Copy of the presentation is available, email me, visit the site:

mark.linton@triplecheck.ca / www.triplecheck.ca

- Some useful links:

<http://www.shadowserver.org> - Malware threat research

<http://bothunter.net> - Bot command and control monitoring

<http://blade-defender.org> - Client browser process isolation

<http://nsslabs.com/browser-security> - General browser security research

<http://www.malwaredomains.com> - DNS Blackholing