NEW PRIVACY SITES PROVIDE STEP-BY-STEP INFO FOR INTERNET USERS

Tue, 19 May 2015 14:34:15, newstips66, []

The Biggest New Web Security Tips Website:

http://www.privacytools.io

Also Check out:

https://krebsonsecurity.com/

and bookmark:

http://www.privacypage.me

Web Security 101 for The Average American:

How to protect yourself on the internet.

The most average, boring, "uninteresting" consumers are the ones that are the most targeted, the most "mood-manipulated", the most hacked and the most data-harvested!

Every single thing you write in an email or text, or click on, will, eventually be psychologically analyzed by governments, lawsuit adversaries, foreign interests, hackers and marketing companies in order to learn what you really think and how you think. They can ALL get ahold of all of that material going back at least ten years. Nothing is ever deleted off of a hard drive. Everything can be recovered using modern physics.

Here are a variety of recent news articles, from across the web, on how to take car of your personal web security:

Your most important link is: https://www.privacytools.io
This will tell you about all of the latest security tools you can use.

Basic Rules of Safety To Survive the Internet!

1. Never log in to anything without using a disposable email address. Never sign in to anything without using a disposable email address. Only use Apps and sites that do not use a login and keep you anonymous. Do not let the internet know that you are using the internet or you will instantly be targeted. EVERY government network has already been broken into at least a dozen times. Every retail network has been broken into nearly a hundred times. Otherwise: "Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"

2. Never send unencrypted email. Always use GPG, or other encryption, and change your password weekly.

3. Never backup or save files on "the cloud". When you put files out on the web on other services you quadruple the ease with which your files can be broken into and stolen. It is like leaving all of your notebook computers on the curb every night.

4. Don't buy any hardware unless it is open-source certified, globally, to be "back-door free". Many companies built spy door gates into their hardware but now all of the hackers have the keys to those doors. If you have un-certified servers, routers, wifi, etc. then the gates of hell are wide-open to any hacker these days.

5. Never buy anything online with an account that has more than $200.00 in it. Have one account only for buying things online and never connect it to any other account and never put more than $200.00 in it. Expect your accounts to be hacked and your money to be stolen.

6. Always remember you are 3 CLICKS FROM DISASTER any time you are connected to a network. These days, ANYBODY can take everything of yours off of ANY electronic device with just 3 clicks of most modern hacking software. BE CAREFUL!

7. Always use fake ID, Disinformation and a false name if you must log-in to a service like NETFLIX or other subscription service. You will be tracked, tagged and process manipulated if you don't.

8. Never post your picture online or you will be processed with imaging comparison software by third parties. Dating sites sell your image but hundreds of others run image comparison software on every image on the internet and abuse them for marketing too.

9. Never keep ANY files on your computer! Use an "air gap" where you never connect drives with actual documents to the live internet. Keep your Outlook .pst files, your photos, your documents, your movies and EVERYTHING you create, on an external encrypted hard drive. NEVER connect that hard drive to your computer unless your internet connection is physically unplugged and your wireless connection is removed or turned off in a way that you can check that it is turned off. If your mobile device is "always connected", ANY kid can take EVERYTHING off of it, with just two mouse-clicks, any time they want to. It IS OK to keep fake files on your computer to keep hackers on a wild-goose chase.

10. Tape over any camera on any device you own. ANY kid can secretly turn your camera on and watch you taking a shower, getting undressed, cheating on your partner, having sex or writing your secrets, with just two mouse-clicks, any time they want to.

11. Don't use the CONTACTS and CALENDER in OUTLOOK, ICAL or on your device. ANY kid can now download all of your contacts off of your phone and computer and watch them as well. A business competitor can download all of your calender appointments and bug your business meetings or get your business meetings cancelled. An ex lover and see who your new lover is and mess with that. Foreign countries can EASILY steal your technology Otherwise: "Over 42 different countries spy agencies, thousands of hackers and thousands of marketing manipulation services will be all over you and your ID, money and life will get stolen"

12. ALWAYS, ALWAYS pull the battery out of your device when you are not immediately using it. ANY kid can now download all of your contacts off of your phone and computer and watch them as well. A business competitor can download all of your calender appointments and bug your business meetings or get your business meetings cancelled. An ex lover and see who your new lover is and mess with that. Foreign countries can EASILY steal your technology. You device may appear to be turned off, you may have even seen it "turn off" but it is still on and pretending to be off.

Inside the shadowy world of data brokers

From CIO Magazine. From: http://www.cio.com

By Matt Kapko

Most consumers would not recognize the names of the large data brokers that constantly collect detailed information on their finances, health and other personal information. It's safe to say most people probably have no idea this is happening at all. Those who are aware should be shocked by the extent to which their online and offline behaviors are being sifted through for profit. Call it panning for gold in the digital age.

The World Wide Web has always been a vehicle for advertising, but as the Internet permeates every facet of society from our apps to our appliances its role is expanding in kind. While surfing the Web or updating social apps on our smartphones, we blindly share valuable information about ourselves often without considering the ramifications - or, in some cases, even knowing we are sharing it. Despite these growing privacy concerns, without advertising the Internet would deliver very few of the experiences many of us enjoy today. Companies need to be profitable to survive, and for most that path to revenue is advertising. While companies like Facebook and Google capture most of their data through consumer-facing products and services they offer for free, outside firms are collecting and organizing virtually all activity elsewhere.

As 2013 came to a close, Sen. Jay Rockefeller (D-W.Va.) issued a scathing report about the role and unchecked power of data brokers. Following a year-long investigation by the Senate commerce committee into the collection, use and sale of consumer data for marketing purposes, he called these companies and their practices "the dark underside of American life."

"Your smartphones are basically mini tracking devices that supply the kind of information that really talks about who you are on a day-to-day basis." --Federal Trade Commissioner Julie Brill

"In 2012, the data broker industry generated $150 billion in revenue. That's twice the size of the entire intelligence budget of the United States government -- all generated by the effort to detail and sell information about our private lives," Rockefeller adds.

Privacy concerns have ebbed and flowed with the rise of the Internet for decades now, but the backlash against data collection has grown more recently as consumers wake up to the reality that their personal information is being bought and sold as a commodity. Former NSA contractor Edward Snowden's revelations about the wide and almost unfathomable reach of the federal government's surveillance apparatus has only stoked these flames of discontent.

Recent reports from the likes of CBS' news magazine "60 Minutes" are shining fresh light on data brokers as well. During that featured report, Federal Trade Commissioner Julie Brill says "your smartphones are basically mini tracking devices" that supply "the kind of information that really talks about who you are on a day-to-day basis."

That data may include information like when someone comes home or leaves, the places or establishments they frequent and when and where they swipe their credit cards to make purchases.

"I think most people have no idea that it's being collected and sold and that it's personally identifiable about them, and that the information is basically a profile of them," Brill says. "Consumers don't know who the data brokers are. They don't know the names of these companies."

By flying under the radar, data brokers have largely been able to keep consumers at bay. The sheer volume of them, which easily number in the thousands, confuses consumers and matters of privacy all the more.
"When you're collecting across billions of data points, regardless of its accuracy, there's going to be groups of individuals behaving the same way."

The largest of these companies -- Acxiom, Datalogix, Epsilon and Experian -- are bridging together data from the online and offline worlds and selling it to the likes of Facebook, Twitter and others to enhance their respective ad products. The general approach is to group and categorize consumers for marketers' online ad targeting efforts. Programmatic ads are then sold and targeted based on these profiles, which the industry insists are anonymous and not personally identifiable.

Regulators and legislators across the political spectrum are making it a top priority to investigate these data brokers and enact laws that could curtail their way of business. But as more troubling details about the operation and seemingly unrestricted reach of these data brokers come to the surface, it's unclear what can or will be done to rein in their most damning practices.

Daniel Kaufman, deputy director for the FTC's Bureau of Consumer Protection, says the agency is currently studying nine data brokers. "They collect an enormous amount of data and they are not consumer-facing," he said at last week's GigaOm Structure Data conference in New York City.

"How are they getting their data? How do they make sure it's accurate? Who are they sharing it with?" Kaufman says. The FTC takes law-enforcement actions, and it doesn't create regulations. However, he adds that "the commission has been supportive of legislation that would support or improve the transparency of data brokers."

The how, when and where of data collection may be perceived by many as nefarious, but the real debate begins over why. "Quite simply, in the digital age, data-driven marketing has become the fuel on which America's free market engine runs," the Digital Marketing Association wrote to members of Congress in 2012. That generally sums up the view of almost marketer today, and the sentiment is even more on point and agreed upon in the world of real-time marketing on social media.

"It's become an essential part of the marketing mix," says Adam Kleinberg, CEO of Traction, an advertising and interactive agency in San Francisco. Data brokers are "becoming increasingly important because the way digital media is being purchased is moving toward the robots. Programmatic advertising and programmatic media buying is using tools that automate the process," he says. "You enhance the targeting efficiency by leveraging that data. It's just gotten to the point in the past few years where 30 to 40 percent of media is purchased that way."

These profiles are directional and optimized behaviorally, Kleinberg says. The cookies that follow us around the Internet are being used to index us based on behaviors such as what we search, visit, click on or buy. "If you actually saw your data you'd think 'wow, these people don't know me at all,'" he says.

"The power of the data in certain circumstances is in the massive quantity and patterning that is possible. When you're collecting across billions of data points, regardless of its accuracy, there's going to be groups of individuals behaving the same way," Kleinberg adds.

"There is sensitive data that is collected and sold on you... What's new is this big data that is being collected and cross referenced with those things," he says. "The reality is that most of this big data is simply being used anonymously to better target you with an ad."

While he freely admits "the ability to look at that individual data is a little scary," he adds that "anyone who's buying digital media today is buying data."

From that the debate usually pivots around the promise of self-regulation versus the need for legal protections and regulations. Industry groups like the Internet Advertising Bureau and the Network Advertising Initiative have already developed standards and best practices which member companies must adhere to, but it appears unlikely that will remain their exclusive responsibility. Regulatory agencies and elected officials aren't subscribing to simple notion that the ends justify the means. Legislation could be on the horizon as they aim for a middle ground.

Sharing the view of the industry at large, Kleinberg says he thinks the responsibility should come from within because regulators don't have a deep understanding. "I think that the industry organizations are actually taking it very seriously and putting together standards that accommodate reasonable privacy restrictions like allowing people to opt out," he says.

"I think consumers care less than we think in the moment. They care in the abstract sense," Kleinberg says. "I can't tell you of an example where data has been abused."

To embolden the case for self-regulation, the industry needs to do more to explain what data means, Kleinberg adds. "The terms data and big data get lumped together as this big sinister beast and a lot of it is not innocuous ... it's anonymized by obscurity," he says. "We should not rush to judge all of it without understanding that nuance."

How your enemies, competitors and corporate theives can have you attacked and robbed on "data-mining" services?

Every time you touch a keyboard, you hand your opposition the tools of your own destruction!

There are a group of BIG DATA Data Mining, privacy harvesting companies that can: find your kids for any stalker, kill off any chance you have of ever getting a job, destroy your credit, destroy your chances of getting a home, anticipate what you might do tomorrow, make you buy things you would not have otherwise bought, tell spammers and junk phone callers where and when to find you, tell everyone what your political affiliations are, and millions of other things that you never thought you were actually showing to the internet.

They grab every mouse move, hand twitch, the direction of your mouse travel, every word, password, page and link that you engage in. They know how long you looked at something, when you back-spaced, how many stories about sex you looked at and in what order. Are you a politician? This is the way your opponents wipe you out in elections.

OR... do YOU have an opinion that conflicts with certain politicians? BANG! Push a button and you are TOAST via a "data burn"! You saw what happened to Micheal on the "BURN NOTICE" tv series, Right?

If someone does not like you, they can get input data to these services that will wipe you out and there is nothing you can do; there is no way to know if they data really came from you, an attacker or a mistake. When you fill out that apartment credit application, you just handed these guys a knife to stab you in the heart with.

What are you going to do about it?

Make it a FELONY for ANY data mining operation to NOT let you see EVERY single bit of data they have on you and correct OR DELETE IT!?

How Spy Agencies Destroy Members of The Public That Politicians Put Hits On!

Did you piss off a corrupt Senator, The President's press secretary or the head of a federal agency by speaking out or reporting corruption?

Then you get a "hit job"

Got some dating site profiles? Suddenly very pretty girls will contact you, on your dating sites, but they will harrass, disparage and harangue you in an attempt to give you low self-esteem and demoralize you so you don't feel motivated. Those girls aren't actually girls, though, they are intelligence interns in a warehouse in Virginia. Those OK CUPID, Plenty of Fish and Match.com hotties may just be some nerd named Norman with a neck beard and six computer screens outside of DC.

Have you heard of the term: "Honey Trap" websearch that term and then try searching the term: "Snowden Honey Trap". Read about that. The hot girls they send to manipulate you are hot coed undergrads from Stanford and Yale, with a hankering for the spy business.

Did you just get fired after your boss got a phone call from a helpful party who wanted to "share some important information about you.." That was a slander job by those boys in Virginia.

Are you suddenly finding it hard to get an interview? Is it strange that recruiters and interviewers suddenly stop talking to you after the first contact? Those potential hirers have databases, that you can't see, and your enemies have put code phrases in your employment profile that makes you un-hireable.

Did your company get a bad review on Yelp or Google? Did it suddenly get frozen into the top position on every Google search. Yes, the CIA-Funded Google does have the power to destroy your life on-command.

All that surveillance for "Your protection" ...it's being used to monitor your actions and figure out how to put roadblocks in front of you, as punishment for pissing of that Senator.

It is called a "Q Request Filing". Q Requests are not even supposed to exist, but they do. Q Request processors are experts in psychological warfare, mood manipulation, brand damage, character assassination and personal attacks.

So, how do you counter-measure such political and business attacks?

- Hire private investigators to track down the attackers.
- Sue them in Civil court, the U.S. Court of Claims and small claims court
- Engage in massive press outreach to expose the attackers
- Expose the funding sources and investments of the attackers
- File complaints with every relevant regulatory and law enforcement agencu and make sure the media tracks the status of those complaint investigations

----

We live in a whole new world!

How many tens of millions of dollars have you spent on your personal web security?

What’s that, you didn’t spend tens of millions of dollars on your personal web security?

Sony Pictures did, Target did, Home Depot did, JP Morgan did, The White House did, PF Chiang did.. and they all got hacked!

What do we learn from this? You are more at risk than you realize!

There are a few problems that have caused all this:

First there are the “backdoors”. Spy agencies had companies like Cisco, Intel, Juniper and others, put hardware and software backdoors in all of their network equipment so that spies, and law enforcement, can get inside any network if there are “bad-guys” on it. The hackers got ahold of the keys to many of those backdoors. In many cases, they only need to get past one door to be inside your whole network. The problem is, many of the backdoors are in the hardware of the devices and those devices are distributed all over the Earth. None of these companies want to shoulder the cost of pulling out and upgrading all of those devices. Many users believe the companies should be liable for any break-ins via their backdoors. There is a big legal discussion around all of that.

Next we have bad IT. If you, or your network provider, are using funky, simple, passwords; then the hackers are auto-testing all of the ports and will eventually get in via computerized trial-and-error. They will just point $35.00 worth of software, that they downloaded off some Russian site, at your IP address and let it run for a few weeks until it gets in and texts them that they can now scrounge through your life. Some of these hackers are just bored teenagers in Thailand, the Ukraine or other impoverished areas where they can’t find work. They have plenty of time on their hands. Other’s are state agencies with $100M budgets and orders to “get as much as they can find” from the competing nations.

Third we have non-distributed networks. Networks are just too big. There are wide open football sized file repositories that should only be ping-pong table sized.

Fourth we have a glut of Silicon Valley companies who made their business model revolve around harvesting and manipulating your activities and personal information. Not only do they make billions doing this, they also get paid by federal and third party marketing groups to do it. They have every incentive to do it and no incentive to not do it.

“Internet security” means keeping your assets from getting stolen or abused. What are your “assets”?

They are:

Your money

Your credit

Your identity

Your privacy

Your intentions (ie: what you might do online and how to trick you into doing specific things)

Your activity history

Your time

Your brand

All of these things have monetary value. They are worth money to someone. Other’s can make money off of these things that you own.

You may not be an evil bad guy with dark intentions, but to marketing companies, you are going to get tracked, monitored and manipulated just as much, if not more. The thought that you “have nothing to hide” is the biggest falsity on the internet. You have everything to hide from the hackers and harvesters.

All of these companies, (most you probably never heard of), are panning for digital gold in your private records: White Pages: Address.com; Google; Spokeo; Marketo; Been Verified; Facebook; Peek You; Intellius; ZabaSearch; US Search; inBloom; Salesforce.com; IBM Data Services; People Finders; TWITTER; Veromi; US People Search; Private Eye; Public Records Now; Addresses.com; People Smart; Advanced Background Checks; People Lookup; TalentShield; BeenVerified; GIS BackGround Checks; CVCertify; Conair; Social Intelligence; Dun And Bradstreet; EquiFax; Infortal; Kroll Backgrounds; Onesource; Checkpeople. Most consumers would not recognize the names of the large data brokers that constantly collect detailed information on their finances, medical, legal, sexual and other personal information. It’s safe to say most people probably have no idea this is happening at all. Those who are aware should be shocked by the extent to which their online and offline behaviors are being sifted through for profit. Axciom openly stated that they sell your information to government agencies. They got in trouble for selling your sexual, drinking, STD, abuse and mental issues to third parties.

In 2013 Sen. Jay Rockefeller (D-W.Va.) issued a scathing report about the role and unchecked power of data brokers. Said Federal Trade Commissioner Julie Brill: “Your smartphones are basically mini tracking devices that supply the kind of information that really talks about who you are on a day-to-day basis.”

There are a group of Data Mining, privacy harvesting companies that can: find your kids for any stalker, kill off any chance you have of ever getting a job, destroy your credit, destroy your chances of getting a home, anticipate what you might do tomorrow, make you buy things you would not have otherwise bought, tell spammers and junk phone callers where and when to find you, tell everyone what your political affiliations are, and millions of other things that you never thought you were actually showing to the internet.

They grab every mouse move, hand twitch, the direction of your mouse travel, every word, password, page and link that you engage in. They know how long you looked at something, when you back-spaced, how many stories about sex you looked at and in what order.

OR… do YOU have an opinion that conflicts with certain politicians? BANG! Push a button and you are TOAST via a “data burn”! You saw what happened to the character Michael on the “BURN NOTICE” TV series, Right?

If someone does not like you, they can get input data to these services that will wipe you out and there is nothing you can do; there is no way to know if they data really came from you, an attacker or a mistake. When you fill out that apartment

So you wonder: “hmmm, If all network devices are now hacked! How can I have a NETWORK-FREE LIFE!

Touching any device connected to a network is the same as asking the Russian mob to “keep an eye on your stuff while you run to the store”:

You might as well leave your unlocked safe deposit box at the curb of your nearest ghetto.

Do you ever take off your clothes? That camera on your cell phone, tablet, PC or appliance is recording you in secret. All those nude photos of all of the starlets that are online from “The Fappening”...you could be next…

Hundreds of millions of consumers are having their personal data hacked from most big retailers.

The White House, NASA, The CIA and all those other sites you thought were super secure.. nope..not so much: Hacked!

The Snowden, Assange and Manning leaks, along with the CIA Torture report, show, more than anything else, that all nation states lie to each other and they have played a one-ups-man-ship game of you-hack-me-I’ll-hack you, that now every single network has been broken into hundreds of times.

CBS news revealed that the U.S. and Israel built the STUXNET virus to take out Iran’s nukes but Iran got ahold of it, and has passed derivatives of it to every anti-U.S. group.

Now nation-state-class regenerative virus attacks are running daily against U.S. corporations with complex viruses that self-mutate like the T3 Terminator in the famous sci-fi film franchise.

Want to see all of Hollywood’s secret movie contracts and all of the movie star’s social security numbers? Say hello to “Sony-Pocalypse”! The Koreans appear to have gutted all of the personal records and private communications of the whole studio system. Now we know that Sony’s own staff think that Adam Sandler is a Dick!

The USB connector, on all USB devices, has high odds of having a hacking virus built into the USB connection itself.

The sad thing is that there are hundreds of ways to solve the problem but those ways involve making networks hacker-proof and the spy agencies won’t allow that.

A large group of public organizations and consumer companies, who have brought hardware and software forward that is actually hacker proof, have been attacked for doing so.

Even famous companies: Apple and Google were just attacked by the FBI for adding a slightly stronger encryption to their phones.

Think you are a boring, non-attractive target? Think again! Ever take your clothes off? ..have sex? ..Buy stuff? Got a credit card?

Technology can absolutely fix the problem. Technologists are being blockaded from fixing the problem because of certain person’s over-whelming need for “control”. Where will it end?

How can you survive as a company, agency or individual in the mean-time? Since the “mean-time” could last for the next 20 years, at the “pace-of-politics”, you need to be ready to make a big commitment:

To be truly NETWORK FREE:

– You cannot own anything with a built-in hard drive. Boot any device from an external drive and try to never connect the drive when the device is on a network. Have a USB nub to put things on when you need to email or go online. Disconnect the main external hard-drive when you must go online. Use the external operating system on a USB drive called: TAILS from the people who brought you TOR.

– Consider having a tablet that is only for surfing the web. Set up ALL accounts on it with the universal login that all web users default to: John Doe. 1 Main Street, Anytown, USA, 91111. Never take any download off of it and never connect it to your home network or any other device.

– Buy old typewriters, paper file cabinets and 1990’s flip phones. Use pre-hack technology. The Russian’s have now switched to this.

– Don’t write anything on a social network.

Companies now realize that sending their design plans, CAD, campaign plans and electronic layouts by email, or FTP, is the same as handing them directly to Chinese and Korean copycat factories. Hackers can get into anything on-line with two mouse clicks, these days. Your personal assets are just as valuable to the hackers.

YAHOO

Stay safe. Be Aware. Once you adopt security techniques they will, eventually, become second nature.

When a technology company hires "opposition researchers" to spy on you, this is what they do to "build an interdiction file on you":

- Acquisition and tracking of your Comcast, Netflix, Hulu and related media uses for the last 10 years.

- Acquisition and tracking of your PG&E bills and usage curves for the last 10 years.

- Live feed observation from all cameras on your mobile devices, computers, smart devices and nearby surveillance cameras, even though those devices appear to be turned off.

- Acquisition and tracking of every keystroke on your devices via a delayed buffer file that remotely sends itself to surveillance servers when you believe your devices are turned off.

- Acquisition and tracking of all of your Paypal, credit card, debit card, club card and service card transactions for the last 10 years.

- "Stingray" device deployment in your neighborhood to spoof all of your wireless devices and create a archived database of all phone calls, text messages, voicemails and web search URLS.

- Routing your computer to spoofed URLS for Facebook, LinkedIn, Twitter and other sites that appear to be authentic but are actually monitoring sites.

- Acquisition, tracking and archiving of all third party business surveillance camera feeds on your daily routes of travel and any off-route deviations you may take.

- Identification and file creation for all investors, family members and associated partners who may have stock holdings or revenue access to your companies.

- Acquisition and tracking of all of your bank accounts, trust funds, shell corporations and any professional financial services people identified in the international databases for the last 20 years.

- Acquisition and tracking of the RFID circuits in your car and the radio system in your car.

- Wifi and Laser inteferomtry observance of speech surface vibrations and air space disruptions, which, essentially, mean that they can see inside buildings and hear speech without bugging anything by listening to the vibrations of nearby windows, ceramics, plastics or other objects.

- Computerized cross matrix comparison of all IRS and State tax filings compared with all revenue streams from the last 15 years.

- Computerized Cross matrix studies on you and your psychological state via the surveillance databases of Palantir, LucidWorks, Epic, PINWALE, XKeyScore, Stormwatch and others.

- Use of nearby Zone satellite array transponders for signal-specific targeting of your activities.

How an adversary will conduct a surveillance operation on you and how to trip them up:

#1 How you get targeted for surveillance:

- By being a human that owns, or is near, any device that can connect to a network

- By having any police record

- By having any tax record

- By making any public statement in social media, that is a political opinion

- By owning a business

- By doing anything that causes three or more people to regulary pay attention to you

- By shopping on line

- By using email

- By having a website or socal media page

- By being in a lawsuit

- By writing a complaint letter

- By signing a petition

#2. When you engage in any of these actions you are assigned a surveillance code. The more you do any of these things, above, the deeper your surveillance becomes

#4. Who surveils you:

- Your government
- Foreign governments
- Local police
- State police
- Federal intelligence agencies
- Democrat opposition researchers
- Republican opposition researchers
- Marketing companies
- Business competitors
- Lovers
- Ex-lovers
- Family members
- Your children
- Hackers
- Foreign organized crime groups
- Neighbors
- Bored teenage gangs
- Lobby groups
- Think tanks
- Political psychologists
- Consumer electronics companies
- Silicon Valley data harvesters
- the CIA
- the NSA
- the DIA
- the FBI
- NEST
- Senators
- the White House press office
- Gawker Media
- the Verge
- Unit 52 of the Chinese surveillance group
- Google
- Linked-in
- Amazon.com
- Experion
- or by "information services" who sell your data to the parties above

#5. Why do they target you:

- to acquire political advantage
- to manipulate political advantage
- to damage political efforts
- to trick you into buying things
- to determine if you might be causing trouble
- to determine if you might be about to cause trouble
- to sell your data assets without your knowledge
- to determine your voting intentions
- to manipulate your voting intentions
- to see if you are a threat to government
- to see if you are a financial threat to a competitor
- to determine the best ways to damage your effort if you are a threat to a competitor
- to get secret information in order to write news stories
- to put misleading information in front of you in order to steer you away from competing with something
- to find out who you are talking to in order to manipulate your contacts
- to trick you by putting manipulated information in front of you with missing pieces and watching how you fill in the missing parts, there-by exposing your thinking
- to trick you into thinking many other people are doing a certain thing and that you should "follow the crowd"
- to put certain words, or short phrases in front of you that candidates then repeat on tv so that you become programmed to accept those phrases
- to identify a city, or region, which might be about to unite under a common complaint, or goal
- to disinform
- to capture location, use and input data about you from your mobile device apps
- to secretly update the spyware already on your system
- to look at other spies that are spying on you and spy on them
- too turn off, or destroy, your device, remotely, iff you "cause trouble"
- to identify if you are exhbiting too much independent thinking and deepen your surveillance if you are

----

Deep dive into QUANTUM INSERT

http://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/

What is a QUANTUM INSERT attack on you?

QUANTUMINSERT is described as a ‘HTML Redirection’ attack by injecting malicious content into a specific TCP session. A session is selected for injection based on ‘selectors’[3], such as a persistent tracking cookie that identifies a user for a longer period of time.

The injection is done by observing HTTP requests by means of eavesdropping on network traffic. When an interesting target is observed, another device, the shooter, is tipped to send a spoofed TCP packet. In order to craft and spoof this packet into the existing session, information about this session has to be known by the shooter.

All the information required by the shooter is available in the TCP packet containing the HTTP request:
•Source & Destination IP address
•Source & Destination port
•Sequence & Acknowledge numbers

For the attack to succeed the packet injected by the shooter has to arrive at the target before the ‘real’ response of the webserver. By exploiting this speed difference or race condition, one can impersonate the webserver.

A video was posted online by The Intercept that shows the inner workings of QUANTUMHAND, which uses QUANTUMINSERT against targets visiting Facebook: https://vimeo.com/88822483.

Any nation state, or skilled hacker, could perform QUANTUM attacks as long as the traffic passes through their country or they possess other capabilities to get the required TCP session data.

QUANTUMINSERT could be used for lateral movement within internal networks.

Detection is possible by looking for duplicate TCP packets but with different payload and other anomalies in TCP streams.

The usage of HTTPS in combination with HSTS can reduce the effectiveness of QI. Also using a content delivery network (CDN) that offers low latency can make it very difficult for the QI packet to win the race with the real server.

Who is able to perform these attacks

Anyone who can passively or actively monitor a network and send spoofed packets can perform QUANTUM-like attacks. The NSA is allegedly able to perform this attack on a large scale on the internet and with a high success rate, which of course not everyone can simply do. This is because it requires the capability to listen in on potentially high volumes of internet traffic, which requires substantial resources and a fast infrastructure. This means that internet service providers (ISP) can potentially also perform these attacks.

A nation state could perform QUANTUM-like attacks when traffic passes through their country. An example of this is the recent research on China’s Great Cannon[4] by CitizenLab that confirms this.

What are QUANTUM INSERTS used for

QUANTUM attacks are possible against various protocols and for different purposes. For both offensive and defensive capabilities as the following table shows:

QUANTUMINSERT: A man-on-the-side attack. Brief hijack of connection to redirect target to exploit server.
QUANTUMBOT: Capable of hijacking idle IRC bots and hijacking c2 communication from bots.
QUANTUMBISQUIT: Enhances QIs effectiveness against proxies and other hard to reach targets
QUANTUMDNS: DNS injection/redirection of A records. Targets single hosts or chaching name servers
QUANTUMHAND: Exploits the computers of Facebook users
QUANTUMSKY: Denies access to a webpage by injecting/spoofing RST packets.
QUANTUMCOPPER: File download/upload disruption and corruption.

Source: https://firstlook.org/theintercept/document/2014/03/12/one-way-quantum/

All of these programs attempt to race the response packet to the target before the response of the real server arrives.

NSA has QUANTUMINSERT capabilities since 2005. The first QUANTUM tool was QUANTUMSKY, realised in 2004. The most recent development, according to the slides was done in October of 2010.

Man-on-the-Side vs Man-in-the-Middle

The QUANTUM attacks described in the Snowden leaks are all man-on-the-side (MOTS) attacks, while China’s Great Cannon attack uses man-in-the-middle (MITM) capabilities. There is been some misinformation on the matter in write-ups. The difference between the two can be observed by looking at the network traffic of the attacks[4]. The Great Firewall of China (not to be confused with The Great Cannon), injects additional TCP reset (RST) packets, and the original real responses can be observed after these RST packets, but real responses can be observed after these RST packets. This is a sign of a MOTS attack, rather than a MITM attack. The network traffic related to the Great Cannon showed only modified packets and no original responses. In other words: the original packets were replaced. This is a sign of a MITM attack, rather than a MOTS attack. The CitizenLab report describes this in great detail.

Monitor and shooter locations

The attack can be done against remote networks on the internet, but also inside internal networks for lateral movement purposes. The closer the monitor and shooters are to the target, the higher the success rate.

Similar attacks

There has been work on injecting packet into TCP sessions. Some tools that perform a similar attack to QUANTUMINSERT are:
•The attack performed by Kevin Mitnick back in 1994 used the same principles as QUANTUMINSERT, though he predicted TCP sequence numbers rather than observing them[5].
•Hunt, a tool released in 1999 was able to spoof and hijack connections.
•TCP Session Hijacking by Cheese, an article released in 2009, describes the technique accompanied by source code showing how to do it[6].
•AirPwn[7], a framework for 802.11 (wireless) packet injection.

How we performed a QUANTUMINSERT attack

We used three virtual machines (VM) to simulate the monitor, client and shooter, as described in the leaked slides. In this controlled environment it was relatively easy to outrace the server response and inject a HTTP response into the TCP session of the web browser.

The monitoring VM received a copy of all the client traffic and was configured to search for a specific pattern in the HTTP request. When a matching packet was found, the monitor service would notify the shooter about the current IPs, ports, sequence and ACK numbers of the session. The shooter would then send a spoofed TCP packet containing the right values for the session and a not so malicious HTTP response to prove the insert was successful.

The monitor is a simple Python script that can read Tcpdump or Tshark output for the required sequence numbers, ACK numbers, IP addresses, TCP ports and optionally HTTP cookie values. The shooter is also written in Python using Scapy for crafting and sending the spoofed packets. We then tested this code over the internet in a controlled environment. One of the harder parts was finding a service provider that permitted source IP spoofing close to our office.

Detection of QUANTUM INSERT attacks

Among the leaked NSA documents was a slide from the Communications Security Establishment Canada describing how to detect QUANTUMINSERT attacks:

Detect QUANTUMINSERT CSEC
Source: https://www.eff.org/files/2015/01/23/20150117-speigel-csec_document_about_the_recognition_of_trojans_and_other_network_based_anomaly_.pdf

To clarify the above, the first content carrying packet is the first packet containing data received by the client from the server. If there are two packets received with the same sequence numbers but have a different payload, it is a possible QI attack.

Theoretically an insert can be done anywhere in the TCP session, for example in long lived HTTP/1.1 sessions. A redirect could also be performed that would have less than 10% difference with the real payload. For example by doing the QI on a similar domain name on a HTTP 302 redirect.

It is even possible to start 'shooting' before the client sends the HTTP request, resulting in a faster response than the real HTTP response. However, by doing so you will lose the ability to identify and target specific users. According to the leaked slides, NSA targeted clients with QUANTUMINSERT using selectors such as HTTP cookies.

So in practice we have to look for duplicate HTTP response packets with significant differences in their content.

In order to detect this using an IDS one would need to observe the network traffic between client and the internet.

Payload inconsistency

A client will receive duplicate TCP packets with the same sequence number but with a different payload. The first TCP packet will be the "inserted" one while the second is from the real server, but will be ignored by the client. Of course it could also be the other way around; if the QI failed because it lost the race with the real server response.

quantum_insert_wireshark
Example of duplicate sequence and ack numbers, but with different payload sizes.

Checking the first content carrying packet is probably the easiest way to detect a QI, but offers no guarantees, as an inject can be present later in the TCP session. Checking only the first content carry packet reduces the amount of false positives.

A retransmission with a different payload size will sometimes look like a QUANTUMINSERT, this can happen when a retransmission is cut short, for example during TCP window size changes.

TTL anomalies

The injected packets also show a difference in their Time To Live[9] (TTL) values. Because the QI packets are usually inserted closer to the target client, the TTL is relatively higher than that of the real responses, because they come from further away. While the initial TTL can be modified, it is difficult to exactly predict the correct TTL value.

Slight variations in TTL values are not unusual, due to route changes on the internet.

Other anomalies

Other anomalies can be seen if the spoofed packets are not carefully crafted. For example, the TCP Timestamp value is usually set if it was also set in the TCP SYN packet. However this could vary between operating systems.

Other values such as the Differentiated Services Code Point (DSCP) in the IP header can also be observed for anomalies.

Detection using IDS

We created a number of packet captures (pcaps) when performing the Quantum Insert attack, which can be found here: https://github.com/fox-it/quantuminsert/tree/master/pcaps

This helped us with developing detection for a number of Intrusion Detection Systems and we hope others find these pcaps useful for further analysis and research.

While we have released Snort signatures in the past, we realised that this was not going to be enough to detect Quantum Insert. The Fox-IT Security Research Team successfully made detection for Quantum Insert and released this proof of concept code into the public domain on our GitHub: https://github.com/fox-it/quantuminsert/tree/master/detection

Snort

We made custom patches to the Snort Stream pre-processor to be able to detect possible Quantum Inserts. We found this to be the most efficient way rather than creating our own pre-processor. When a possible QI is detected it will trigger an event and also try to log the payload of the other TCP packet that was inconsistent as extra data.

See the README.md for more technical details: https://github.com/fox-it/quantuminsert/tree/master/detection/snort

We hope these patches will eventually find its way upstream.

Bro

We made a Bro policy to check for inconsistencies in the first content carrying packet. Keeping track of multiple packets would be better, if this could be done in the core functionality of Bro. We attempted to use the rexmit_inconsistency event, but this did not seem to work. Others have also reported this on the mailing lists[10], however it never got much attention. It should be feasible to improve Bro so that it can also keep track of older TCP segments, in order to detect QI like attacks. There's even an official Bro ticket for this: BIT-1314[11].

See the README.md for additional technical details:https://github.com/fox-it/quantuminsert/tree/master/detection/bro

Suricata

We asked the lead developer of Suricata, Victor Julien, if he could verify Suricata's coverage for QI by supplying him a pcap. Victor explained that Suricata has an event called 'stream-event:reassembly_overlap_different_data' that can be alerted on when triggered using a default signature. We received an additional signature that detects HTTP 302 responses in possible QI payloads.

https://github.com/fox-it/quantuminsert/tree/master/detection/suricata

Evasion

Note that these detection methods are possibly not evasion proof, one could also easily spoof a FIN packet after the QI packet to close the session. This would stop tracking the TCP segments in most IDS systems. Later packets in this stream will not be matched with previous packets.

Other possibilities is to try to create a partial overlap of data, thus avoiding detection of duplicate sequence numbers.

Other work

The following blog post[12] describes how to perform QI containing Proof of Concept code to perform the attack: https://github.com/stealth/QI

HoneyBadger[13], is a comprehensive TCP stream analysis tool for detecting and recording TCP attacks written by David Stainton can most likely also detect this attack.

While writing this article a DoS attack on GitHub was going on and a analysis was posted by NETRESEC[8], we did not see duplicate packets in the screenshots that could indicate a QUANTUM (man on the side) attack. However, the difference in TTL values was noticeable.

The detection for this attack has been included in our Cyber Threat Management platform.

Additional sites where you can conduct your own research:

http://www.aclu.org

http://www.propublica.org