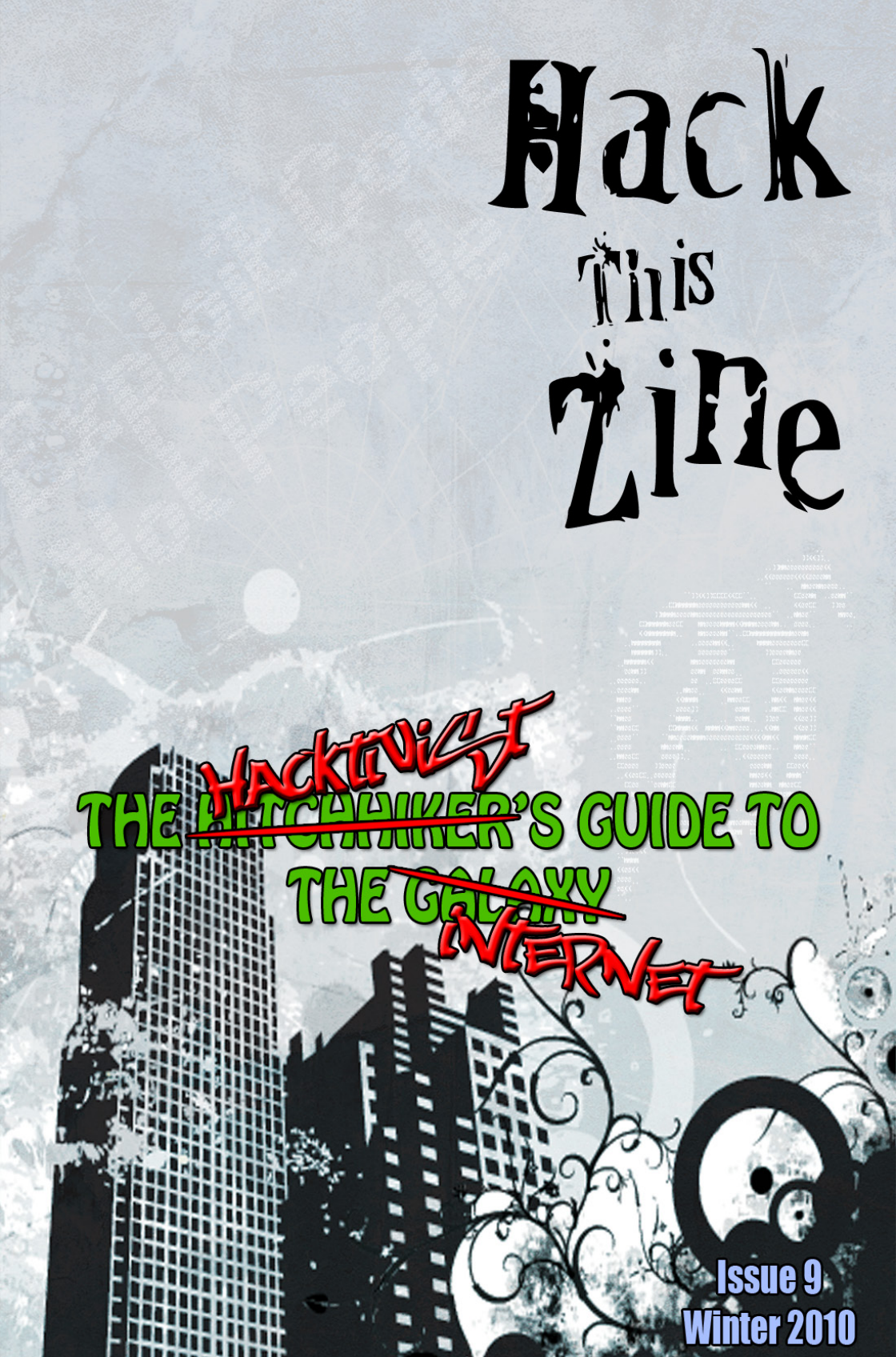
Hack This Zine



THE ~~HITCHHIKER~~ HACKTIVIST'S GUIDE TO THE ~~GALAXY~~ INTERNET

Issue 9
Winter 2010

==========

THE HACKTIVIST'S GUIDE TO THE INTERNET

(HackThisZine #9, Winter 2010)

==========

Table of DISContents

****

****

Introduction

Things have been busy around the HB network up-links recently mostly in preparation for the SF @ bookfair / 8 days of anarchy / BASTARD conference.

While HB has had a presence at the bookfair for at least the past 4 years it has mostly been in the free table section outside where various members could be seen milling around handing out copies of the zine and sharing lock picking techniques and tools.

We started talking about having a more established presence after last years bookfair with a table inside, a scheduled presentation of sorts, and a new issue of the zine. We are excited to bring you the ninth issue of HTZ, see you at the "Digital security for and by Anti-Authoritarians" workshop at Noisebridge, and catch up with you at the bookfair.

From my perspective the drive for this change in presentation is a result of change of focus with in the group and our desire to collaborate and be accountable to a larger community of anarchists. We have spent the past year working on the zine, building our skill-sets, writing communications tools, and attempting to improve the availability of our online presence and tools.

This recent drive and work has resulted in some new relationships, questions about future plans, and fair amount of meeting time spent talking about our role in the anarchist community. The articles of issue 9 reflect this work with the exception of an article regarding our participation in a community remediation process with Jeremy Hammond. While we were not able to get this article in for this issue we hope to have it for you by next issue and would like to point out that Jeremy has not been involved with HB since his sentencing a number of years ago.

As always we want to hear from those of you reading this zine online or in print, those of you crushing on us, drawing the HB logo in your notebooks with hearts around it, and those of you hating on us starting flame threads on the Internet. We are always accepting articles for the next issue, looking for new projects to give exposure to, and can always use letters to publish that do not involve requests to hack your ex's facebook account, or offers on deals for medicine to make us better lovers or tools to make us more attractive.

With monitor tan, love, and solidarity!

The Hackbloc Collective
<staff@hackbloc.org>
PGP: https://hackbloc.org/etc/hbStaffPubkey.txt

NEWS AND EVENTS

Pirate Bay Launches Private Proxy (VPN) Services, Promised Logless, Encrypted Privacy

Submitted by Anonymous on 01/21/2010

According to TorrentFreak, The Pirate Bay has finally launched its public VPN service and allowed anybody to get an account. This allows citizens around the world high-speed "anonymous" internet access for only $7 a month.

The way it works is that your computer establishes an encrypted connection to their VPN service (in Sweden) and then your web traffic, BitTorrent, etc. are sent from there. Anybody looking to find out your real identity will be stopped once they realize it's coming from an IPREDATOR server which doesn't keep logs. As an added benefit of the encrypted connection, your employer, people on your wireless network, and your internet service provider won't be able to see what you're doing online, only that you're connecting to this proxy service. Since Sweden's laws are more supportive of privacy and free speech than those in most countries including the USA, having internet access from there can be very useful. If you leak files or do journalistic work through IPREDATOR, you gain extra protection under Sweden's source-protection laws which make it illegal to investigate the source of a leaked document used for journalistic purposes.

This is one of the many layers of defense that organizations like Wikileaks provide. If you are looking for a different VPN service, check out Relakks.

For only 149 SEK (that's about 15 EUR / 21 USD) per 3 months you will get safe, encrypted communication between you and the internet, with no logging of the data transferred. It's of our utmost concern that you can use the network without anyone deciding what you're can communicate about.

Ipredator is not only another VPN-service. It's also a statement. Right now we're developing a new tool to make it harder (or impossible) for the government of Sweden to tap into their citizens traffic. Our goal is making people have the ability to use their democratic rights, without a fear of repression.

So, the more people that actually use the service, the better. We will get funds to build more tools and at the same time the users clearly show that they want to be anonymous. It sends a very clear message to the politicans!

Please invite your friends if they need a service like Ipredator, and tell people about the reasons why they should be allowed to communicate without a third party listening to their conversations... The most important thing is to actually make people aware of the situation.

Hate Social Networking? Commit Suicide.

Submitted by Anonymous on 01/14/2010

Hate your online social networks? Sick of acquaintances who barely know you eating up hours of your time and rating how attractive you are compared to others? Want to get to know real people? Want to kick the habit? Kill yourself... online that is!

Since the launch of the Web 2.0 Suicide Machine, over 800 people have cathartically killed their online identities, de-friended over 50,000 friends, and removed over 200,000 tweets. Even Facebook got in on the action, sending a baseless legal threat to the group which was posted to the whistleblower site Cryptome.

The site will quickly delete all of the content on your accounts at Facebook, Twitter, LinkedIn, and MySpace. Better yet, you can watch it do this live and enjoy watching your online demise which is as close as you'll get to an out of body experience without risking your health by fasting or taking drugs.

Why stop there though? These sites make money using their user's information (which is never really deleted anyways) to sell advertising. Give them something they'll love: more information for their hungry databases. Fill it with junk, join random groups, send meaningless messages, and friend request people you'd never even be remotely interested in back when you had your online identity. Poison the machine!

<http://suicidemachine.org/>

UPDATE: Facebook excommunicates WORM because of the Web 2.0 Suicide Machine, Rotterdam, 18th of February 2010

It is with great sorrow that we announce that Facebook Inc. has decided that WORM, the producer of the Web 2.0 Suicide Machine, will be excommunicated from Facebook. The initiative to build the Web 2.0 Suicide Machine came from Moddr_, WORM's media lab. By threatening WORM, Facebook is trying to take down the Suicide Machine.

The Web 2.0 Suicide Machine allows users of - among others - Facebook to commit 'social network suicide'. Facebook threatens WORM with further legal action if WORM doesn't stop targeting the FaceBook platform via the SuicideMachine. In addition, it has now also demanded that WORM immediately deletes its own Facebook profile (WORM_Rotterdam). According to Facebook and its lawyer, the Web 2.0 Suicide Machine has violated Facebook's Terms of Service and with that WORM has forfeited it's right to keep using the platform. WORM does not want to engage in a fight over this matter with Facebook. The idea behind the Web 2.0 Suicide Machine was to be able to 'unfriend' in an automated fashion and to make users of social networks aware that they should always be in control of their own data. Facebook won't allow for this control and is also not willing to enter into this debate. We are pretty much done with that and are left with no other choice than to commit online suicide ourselves. The conditions and attitude of Facebook leave no other option as far as WORM is concerned.

WORM deeply regrets the current situation. The web 2.0 Suicide Machine was never intended to target Facebook as such, but meant as a tool for people who, for whatever reason, are tired of their online life. Facebook wants all access to their service, personal data of their users included, to run via their own 'connect' platform. In this way, Facebook can set, interpret and change its own rules as it sees fit...

The excommunication of WORM illustrates that data freedom and net neutrality of users is merely an illusion on many social network sites. Not only is it not allowed for people to unfriend (in an automated manner), but companies also have the power to expel users they do not like. Facebook shows that a user only has the rights that Facebook grants it.

Facebook claims all rights. WORM does not want to continue living in this 2.0 world. Which is why we say goodbye to all our friends. We wish you all the best.

No flowers, no speeches. [moddr_labs, WORM, Rotter, damworm.org, moddr.net, suicidemachine.org]

German 'Fleshmob' Takes on Full-Body Airport Scanners

Submitted by Anonymous on 01/13/2010

A 'fleshmob' of Pirate Party sympathizers in Germany confronted the new full-body scanning devices at the Berlin-Tegel in Germany. This new scanning technology allows scanner operators to see beneath the clothes of people walking through them, providing great opportunities for voyeuristic pleasure. In a study at Hull University, researchers found that one in ten women were targeted for such purposes by surveillance camera operators.

Anonymous Pwns Australian Government in Operation Titstorm

Submitted by Anonymous on 02/12/2010

Update Feb 13th 2010: List of websites taken offline: Australian Parliament + Stephen Conroy (http://www.australia.gov.au/, http://www.aph.gov.au/, . They have been down for two days now and anonymous said the attack could continue "for months". Interview with "spokesperson" for anonymous at http://delimiter.com.au/2010/02/12/anonymous-attacks-better-than-signing...

The hacktivist group Anonymous has launched a wave of successful attacks against websites of the Australian government. As many hackers are aware, Australia has proposed mandatory internet filtering at the isp level for all citizens. During the trial runs where the effectiveness of such a hypothetical system was measured, several whistleblowing, commercial, and otherwise "normal" or political sites were blocked.

According to a member of anonymous, "No government should have the right to refuse its citizens access to information solely because they perceive it to be unwanted". The website of the Australian Parliament was getting 7.5 million hits a second. Government offices involved were also hit with "a shitstorm of porn e-mail, fax spam, black faxes and prank phone calls to government offices." The porn consisted mainly of "extreme" porn and female ejaculation, both of which are proposed to be banned.

Based on reports, the main wave of attacks is through but low-intensity fighting continues. If the past actions of anonymous are anything to go by, another wave or two of attacks are expected in the next month. It's worth noting that Anonymous declared war on Australia several months ago.

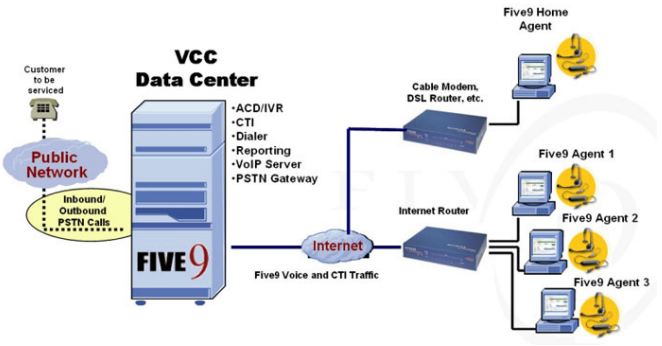
Fugitive VoIP Hacker Pleads Guilty to Stealing 10 Million Minutes

Submitted by Anonymous on 02/04/2010

Edwin Andrew Pena, a hacker who stole over 10 million VoIP minutes by routing them through a botnet, has pled guilty to several felony charges, facing up to 25 years in prison.

After posting bond, he fled to Mexico to avoid charges but it looks like he's in the clutch of the law once again.

He allegedly banked over a million dollars over the course of two years selling VoIP minutes at almost a quarter of their original price. All of this was done from one cable connection where he spent most of his bandwidth scanning for new botnet additions.



More Info on this can be found at:

www.theregister.co.uk

Original article was published February 3rd, 2010.

Manchester Police Computer Systems Shut Down by... Conficker

Submitted by Anonymous on 02/04/2010

In an epic security fail, the Manchester Police's criminal lookup system was disabled when it was discovered it had been infected with conficker. Their computer network had to be isolated from other police departments to stop its spread. Apparently somebody doesn't run basic anti-virus... or hasn't updated it in a few years.

One has to wonder what lax security like this means. Some script kiddie with a exe patcher could probably do a big rm -f * on everything.

Even if you clear your private data, how trackable is your browser?

Submitted by david on /01/29/2010

Even if you disable cookies and clear the private data on your browser, you still might be just as trackable. Why? Browsers give lots of information to the sites you visit including the browser version (called the user agent), what type of information it can view (flash, videos, audio, etc.), the ability to store flash cookies, your screen/window size, your color depth, and much much more. In fact, by changing only one aspect of your browser's information to protect your privacy such as a user agent, you might be making your browser easier to track. In some cases, your browser's "fingerprint", which is all the data it gives every website it views, may be completely unique.

The Electronic Frontier Foundation has released a tool called Panopticclick which compares your browser's fingerprint to thousands of others and tells you how "unique" yours is in addition to what makes it unique. It is worth mentioning that TorButton, which is commonly bundled with the Tor software has protected against this type of tracking for years. There's a post at their blog for those looking for more on these attacks.

[http://blog.torproject.org/blog/effs-panopticlick-and-torbutton]

ELECTRONIC FRONTIER FOUNDATION

See You in the Bay!

Submitted by Hackbloc.org on 02/12/2010

A grip of us from Hackbloc will be in the San Francisco Bay Area enjoying 8 days of anarchy, the BASTARD conference, and the sf anarchist bookfair. We are helping organize a workshop Friday March 12th from 6pm - 9pm called Digital Security and Tactics For (and By) Anti Authoritarians at Noisebridge, the local hacker space. Hope to see you there, it'll be a blast!

Think...

I was born as a thinker. I've spent much of my life thinking about things. Thinking about myself, thinking about others, even thinking about thinking. This is not to say I always think the right things, or that what I think about is always of any use to anyone. My brain isn't the best brain, and I don't have a great deal of conventional education.

Nonetheless, I sit and I think. Since an early age, my thoughts led me to believe that there was something funny about the world in which I was living. I started out as a child, interacting with my family, learning from their behavior, thinking about the things they do, the things they say. Garnering from it my basic beliefs about love, kinship, respect, and the value of life.

As my world grew beyond the borders of my immediate family, I began to learn about selfishness, greed, hate. I recognized these things as alien to what I believed "humanity" represented. I had theorized that the only reason human beings had grown beyond the animal world was because of our capacity for great things - Community, peace, love, tolerance. I still firmly believe that these are the foundations for a solid community, and a happy, prosperous life within that group.

When you are born, you are helpless. Unable to perceive the world around you, unable to rectify the situation you're in. You have fear, but it is mitigated by the fact that you have a loving family to nurture and protect you. Fear and Love. These are the basic emotions we are born with. To simplify it further, even though you don't understand the feelings you have, the only thing you have the capacity to be afraid of is NOT being loved. You do not KNOW this, but your biology has hard-wired you this way. Had you not been loved and cared for, you would have died. When you cry, you are calling out to the ones who love you. What I'm saying is that we are designed to love each other. Without this basic, primal desire for love, we would not have humanity. We would not have a culture at all.

From love comes empathy - The ability to see and feel the emotions of other human beings around you. From empathy sprouts understanding and tolerance. From these, a community can foster peace and tranquility. This, in my humble opinion, is how humanity has achieved great things. How we, as a whole, have risen up to be the stewards of our world. Not mere beasts roaming the plains, but the overseers who work the fields, care for God's creatures, and nurture all life on this small planet. It is the peace that allowed us to take time to think. With our thoughts, we discover new ways to improve our lives and the lives of those we share our space with.

A child does not know hatred. When you were born, you did not hate. You did not discriminate based on skin colour, class, religion, or culture. You weren't selfish, as you were not even self-aware. These are unnatural feelings, things you did not consider. That is, until you were taught by someone how to hate. We are born with the capacity for great things, and unfortunately that capacity includes the potential for these negative emotions. They are counter-intuitive to the things that make us great. Selfishness breeds ego. Ego gives us the capacity for materialism and hatred. Materialism because our ego desires the false admiration of others. Hatred comes from the fear that someone else has threatened our ego. These are things you did not know as a child.

I've spent my life being confused and conflicted. With all these things planted firmly in my mind - Things I believe to be obvious Truths - I watch the world around me in total chaos. Chaos that seems to be accelerating. This is not to say I live as a Saint, but as I said before, I spend a lot of time thinking. Most of these thoughts are dedicated to how I can raise up the ones I love. To making their lives better, thereby improving my own life with theirs. With that statement, I would also like to clarify that I'm not trying to be selfish, but simply that being part of and nurturing a peaceful, loving community will give you a more peaceful and loving life. This is inevitable.

This, unfortunately, also works with the negative, learned emotions and actions. Even more unfortunately, it seems as though there is a trend in our world pushing us towards these negative, unnatural ways. It seems popular to have the nicest car, the most sexual partners, the biggest house. These things do not provide love or peace. The desire to achieve these things displaces the natural, pushes away love and fosters selfishness. For if you are to HAVE, others must NOT. This creates an imbalance, causes others suffering, creates social classes, distrust, hatred.

There is a great inequality that pervades our society. Instead of caring for one another, we are taught one-upmanship and greed. This allows for us to be taken advantage of. As we grow and are taught, indoctrinated to believe in inequality, in distrust, in competition rather than cooperation, we cry out for someone to care for us. We beg, like children, for someone to give us stability. Those who teach us greed and hatred are the ones who come forward, offering us a solution. "Be with us," they say. "We will take care of you." In exchange, we give our labor, loyalty, and servitude. Yet, I know I still feel as though I'm not safe. I'm not living a life of peace by being a member of this invented culture of hate.

Now, after several generations, the "protections" provided to us and the exchange of servitude are enacted upon us when we are born, by default. Do we not get a choice? Could we not solve our problems by being loving and peaceful?

I think we can and will. What do you think?


THEORY

Most people who live in communities that are targeted for harassment and persecution by the powers that be adapt to fight that targeting. Every group has a different reaction, but the most common and effective one is adopting a culture of non-cooperation. In hood culture, where people see their families torn up by unequal crack/cocaine laws, tainted evidence, racist juries, and targeted police patrols, there's the 'stop snitching' movement. Traditionally, the phrase 'snitches get stitches' describes the situation pretty accurately. In activist culture, the policy of non-cooperation works similarly where those who assist police are immediately outed publicly and exiled from the community forever. Snitching is the ultimate betrayal, attempting to trade your friend's freedom for yours.

Hackers are another targeted community. We've even got ideology on our side. Hackers, in general, determine rules by ourselves. We bend them, break them, and when we get caught? We laugh because it took them so long. We're against state surveillance, the police state, and government control over our lives. We're against censorship, for free speech, and staunch advocates for privacy. The Streisand effect[1] is made possible on our connections and piracy is rampant because we seed till we bleed. We dumpster dive, snoop on open wireless, and social engineer our way into locked-down corporate offices. We support whistle-blowers, truth in media, and the inherent political statements in the Wikileaks experiment, Freenet, and the Tor project. We're educators, happy to share our knowledge with others even when it's inconvenient to some big corporation or government agency. Even when it could

mean our freedom.

When we get caught, we really get thrown in the shithole. The FBI and the Secret Service knock down our doors and confiscate everything that uses electricity. We're denied bail for fear of what we might do if we get out. We're so dangerous that some of us are banned from using computers, even those that aren't connected to the internet. We're thrown in jail on charges like 'fraud', 'conspiracy', and other charges - many of which stem from the idea that thinking about committing a crime or talking about its possibility is the same thing as committing it.

So why then, has our reaction as a community been anything but complete resistance to the current system? When the police come knocking, most hackers just roll over. Why do we tolerate cooperating in our communities? Why is it that when Jeff Moss [2] works for the Department of Homeland Security, we all look at him as helping out society instead of what the reality of the situation is: he's working for a section of a government that is responsible for tearing apart families because somebody along the line broke immigration law, operating a national surveillance network that watches hackers, journalists, and activists, and is constantly pushing the idea of a surveillance state. He's fixing their security problems so they can do their work with less interruptions. Jeff Moss is an ally of those who we despise and everything we despise; of those who try and frame people on the basis that they were using encryption and must have been 'trying to hide something'.

While I couldn't see many of the folks who read this zine specifically engaging in these acts, I can see the rest of 'the community' doing it and I can see our readers tolerating it. I know Emmanuel Goldstein [3] would never turn anybody in, even if he had some type of personal vendetta against them. Neither would Julian Assange, [4] The Mentor [5], Bernie S. [6], Peter Sunde [7], or any of the other hackers I look up to. Whatever we think about the acts of another, we can all agree that putting them in a cell isn't going to solve or change much of anything. The antithesis of the hacker is the white-hat, a corporate sell-out who never breaks the law , wants to make sure the corporations and govern

ments stay one step ahead of even your run of the mill cypherpunk, and who thinks that the movie Hackers was a portrayal of wayward teens who committed irresponsible acts. I know many of you are reading this, shaking your heads. I know some of you are doing this because you're down - you're down with most of what I'm saying and you don't think hackers are like this. The rest of you are probably white hats or maybe you're a real hacker too, but you've started to get sucked into the mainstream rhetoric that encourages you to abandon the hacker ethic and your friends.

This world isn't what it used to be. Everything is connected to everything and the choke point is the wire. When the wire breaks, when the server goes down, when the digital infrastructure doesn't work it takes more than a repairman to fix it. We hold the power to make some real change, to strike at the heart of a beast. To directly stop 'them', whoever that might be.

So here's my proposal, follow it if you want or not. Publicly out all those who cooperate with the state or inform on hackers or pirates, support those who don't and ostracize all that do. When you out them, do it right -- pictures, phone numbers, personal histories, everything. And when our friends get locked up, like when Bernie did, we need to stand by them in unconditional solidarity -- not because they're hackers or we agree with that they did or are accused of, but because they're being targeted by the state - an evil beast that is targeting us all. If you like what I wrote, here are some potential sites you may enjoy: snitchwire.blogspot.com, hackthissite.org, hackbloc.org, crimethinc.com/texts/atoz/security.php, crimethinc.com/texts/atoz/fuckpolice.php, crimethinc.com/tools/downloads/pdfs/dont_talk_to.pdf. https://secure.wikileaks.org, https://torproject.org

References:

[1] The Streisand effect is a primarily online phenomenon in which an attempt to censor or remove a piece of information has the unintended consequence of causing the information to be publicized widely and to a greater extent than would have occurred if no censorship had been attempted. http://en.wikipedia.org/wiki/Streisand_effect

[2] Jeff Moss, also known as Dark Tangent, is the founder of the Black Hat and DEF CON computer hacker conferences. http://en.wikipedia.org/wiki/Jeff_Moss_(hacker)

[3] Emmanuel Goldstein, pen name of Eric Gorden Corley, editor of the hacker magazine 2600: The Hacker Quarterly. http://en.wikipedia.org/wiki/Eric_Gorden_Corley

[4] Julian Assange is a public spokesman of Wikileaks, an internet based whistle-blowers site, from Australia. While often being refered to as founder of Wikileaks, he himself denied that. http://en.wikipedia.org/wiki/Julian_Assange

[5] Loyd Blankenship (a.k.a. The Mentor) (born 1965) has been a well-known American computer hacker and writer since the 1980s, when he was a member of the hacker groups Extasyy Elite and Legion of Doom. http://en.wikipedia.org/wiki/The_Mentor

[6] Bernie S, real name Ed Cummings, is a computer hacker living in Philadelphia, Pennsylvania. He participates in the WBAI show Off the Hook with Emmanuel Goldstein from 2600 Magazine. http://en.wikipedia.org/wiki/Bernie_S

[7] Peter Sunde Kolmisoppi (alias brokep) is best known for co-founding The Pirate Bay. http://en.wikipedia.org/wiki/Peter_Sunde

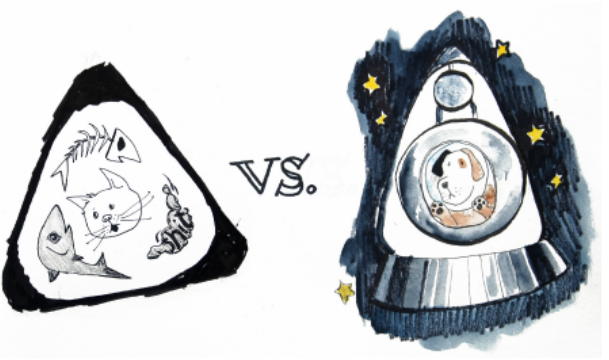
Food Not Bombs shares free vegan and vegetarian meals with the hungry in over 1,000 cities around the world every week to protest war, poverty and the destruction of the environment.

With over a billion people going hungry each day how can we spend billions on war?

<www.foodnotbombs.net>

autonomy and a new high tech

-by cloacina

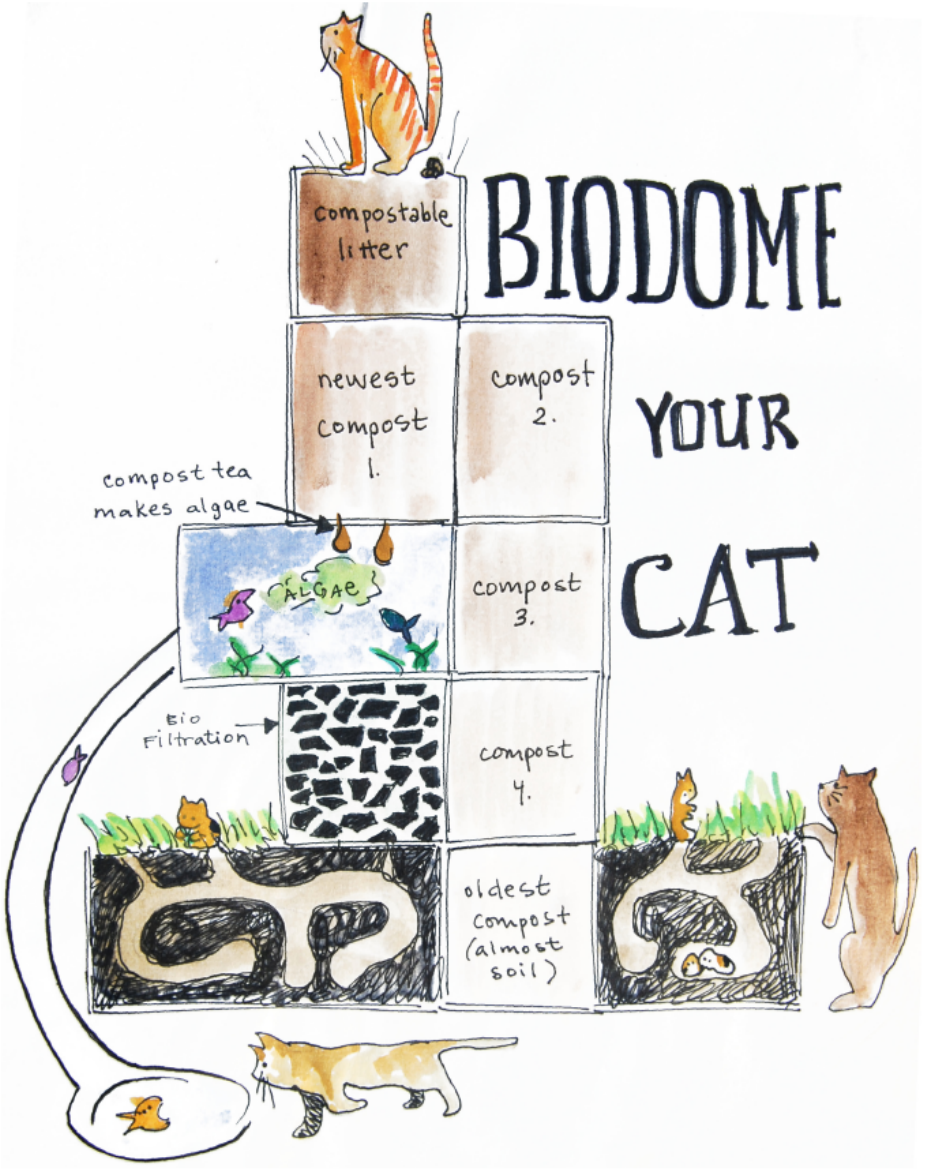


The Russians launched dogs into space because dogs are gullible. Laika was a model Soviet: a liberated female taking a leading role, subverting her own interest to that of the State. Obedient, loyal and unquestioning, she was asphyxiated, dying hungry and alone in a windowless steel can mounted atop a ballistic missile. Her true mission was naive deception, a scientific veneer over the technics of atomic apocalypse. Spacecraft now carry more luxuries for their crews -food, air, water, and re-entry systems- but the safe return of human beings does not mean that the forms of spacecraft have changed. They are still repurposed weapons systems first and human habitats second. Going to space has been an aesthetic and muscular display of energy concentration and a proving ground for power fantasies. Our contemporary technology owes much to the rigor harsh space environments place on machines.

We live in the space age: everything is designed to exist in an eternal vacuum, with no thought to objects' beginnings or endings. Zipping planetesimals formed the planets, and our collapsing consumer devices are crushing the earth. But space can be a wonderful goal: living in space means self-sufficiency, whole systems thinking, and closed resource cycles. Even in a low energy future, space is still the place to test our concepts, and the narrative of space a framework for re-imagining our world.

So we'd like to outline what a low energy space program would be about. A space program about soft, slow, objects teaming with life. By adopting the professed goals of military-industrial air-superiority and subverting the iconography of force projection, we can redefine technological progress from power and industry to biology and information.

Lichens may have been the dry earth's first colonists; tiny efficient guilds of interrelated organisms mixing fungi, algae, and bacteria. Lichens construct themselves mostly out of atmospheric gasses, efficiently replicating the structures necessary to their own survival. They are a small example of autopoiesis, autonomous self-sustenance and



We need a small astronaut to practice autopoiesis. Building and testing small-scale ecosystems focuses attention on the information systems and techniques of resource cycling . Dogs are followers, but cats try to maintain autonomy and judgement. We often assume they have better taste than us. When a house cat seems happy, clean, and odorless we feel at home. Cats judge comfort, and we believe them. A closed-loop ecosystem that meets a cat's criteria for comfort is a reasonable model of autonomy, and a cat needs only 1/10th the calories a person does. We're working on such a system beginning with high-temperature composting of cat crap.

(1) *ecosystems' access to energy and nutrients is stabilized through physical mass, redundancy, diversity, and secession* **(2)** *in regenerative human systems, information and informed action replace mass* **(3)** *the pursuit of lightness drives ecosystemic knowledge, informing the remediation of earth*

replication. These symbiotic organisms attain efficiencies far beyond our own creations; algae's solar efficiency is greater than 80%, more than twice the best human-made solar cells. Our solar cells require high energy and rare-earth minerals- Lichens absorb their materials from the atmosphere and uses a quantum-mechanical system to absorb sunlight, all at room temperature. Evaluated on performance criteria, our creations aren't nearly as high-tech as lichen.

The autopoiesis of lichen offers a model of freedom. True autonomy can come only through the knowledge that one can grow and be sustained on one's own resources. Despite the difficulty of complete autopoiesis (even lichens need the atmosphere) all who hold autonomy maximizing ideologies aught to seek support systems approaching autopoiesis.

Like Laika, we are all locked into an industrial support system, dependent on supply rockets whose schedule we can't control. autopoiesis is the only way out.

Each part of the lichen system supports the others; bacteria fix nitrogen, algae fix solar energy to carbohydrates, and fungi construct a environment for both

while supplying algae with CO_2. Experiments with integrated greenhouse aquaponics mirror this approach, with animals and plants held in equilibrium through human action.

But collecting information about the environment and transforming it into actions has traditionally taken massive inputs of expert observation and effort. Computerized information systems present an opportunity for significant labor-savings and performance improvement in constructed autopoietic food systems. Mutual aid and information exchange between autopoietic groups can shift expertese away from technical specialists and towards a network of autonomous communities. Keeping the harsh limits of life in space focuses lightness, efficiency, and escape from industrial dependence.

State-of-the art near-space craft are materially identical to plastic greenhouses, constructed from the same thin film plastics, PET & LLDPE. NASA floats multi-ton payloads over the north and south poles, suspended beneath superpressure balloons for months, holding steady 20 miles up. Autopoietic habitats on earth create the skill base for space.

If greenhouses are our lichen, balloons can be our spores.

Balloons, loping and directionless, huge and soft, are not a physical threat to the state the way missiles are. They are the spore of the idea that the state can be escaped, proof that high-energy industrialization has lost its edge. Sending fairly autonomous ecosystems into long-duration missions around the earth challenges state power in its own environment, on its terms of supremacy. It is a symbolic expression of statelessness and freedom, claiming the high ground for biology and information systems.

follow us at cloacina.org

How can we know what is going on and fast when we take to the streets? An effective communication system is the life-blood of any skirmish, uprising or revolution. Timely information can provide nourishment and animation to all other aspects of a resistance project. Without the ability to communicate with our comrades we would become isolated and will not be able to effect real or substantial change. In this essay we will look at the sociological and technological underpinnings of various communications systems that have been used when we gather to take our resistance to the streets. We will examine the shortcomings of previous models and see how they can be improved upon to create a system that allows us to employ fully the passion of our dreams and resistance.

In the anti-globalization era, the radical dissent movement used to be at the forefront of communication and technology innovation. Many of us remember the early days of Indymedia, and the huge impact its model had both within our movement, and as an important meme breaking down the barriers and professionalization of information gathering and broadcasting. Today the type of "journalism" or open participation in media production that was the foundation of Indymedia is ubiquitous in all sorts of mainstream sites, blogs, etc. while Indymedia itself has actually declined as a source and locus for sharing ideas and news. The sharing of information in general has sped up tremendously in recent years and real-time communication is the name of the game. It seems that our creativity and knack for innovation has abandoned us lately, and we still cling to old, tested and failed models of both organizing and communicating. In mass mobilizations, many still rely on old school radio/walkie-talkie communications, cell phones, or just word of mouth, when there are so many tools out there we could be adapting and using to better effect. Today, when communications are even discussed in mass mobilizations, the conversations revolve around the technical aspects, or the means of communications to be used (should it be radio, walkie-talkie, SMS text, phones, etc.) while the end or principles of communication are most often overlooked or taken for granted. We believe that a closer look at the principles or goals of communication is the first step to innovation that can keep us ahead of the curve and the forces of oppression.

Ten principles of communications we think are fundamental when developing an effective street-based communication network for radicals. These principles could be used to guide us in creating new forms of communication, and new technical tools that can enhance our effectiveness while keeping us safe on and off the street.

1.Speed of Information is a primary goal of any useful street communication network. Law enforcement has spent billions of dollars on dispatch systems, radios and city-mapping software to maximize its ability to respond to events in real-time and so must we. Anyone who has been to a protest knows that seconds matter. Information is only useful if it is timely. We have become accustomed to the power of nearly instantaneous information sharing from instant messenger to texts from cell-phones to e-mail. Any communication network needs to replicate this speed of transmission to be a truly effective

tool on the street. Nothing ages as poorly as information. Our contemporary communications systems have adhered to this principle well. Using hand held walkie-talkies, Nextels, and even bull-horns has allowed information to be updated quickly providing contemporary information. Any new system would have to be equally as fast in its information distribution and hopefully more sophisticated.

2.Truthfulness is another principle that directly impacts the effectiveness of the overall information network. Accurate and understandable information is at the foundation of effective action and informed autonomous decision-making. Too much information on the street is not much better than too little. During the last two National Republican Conventions we have seen that the amount of text messages sent overwhelmed users to the point they often stopped reading them. We also have seen how inaccurate information and rumors can poison tactics disarming our resistance and in some cases putting us in peril. We have all heard about mass arrests only to later find out such reports were false, while the rumor has dampen or even ended a vibrant action. It is difficult to judge the veracity of any piece of information one hears while on the streets and thus we sometimes have to make decisions about the truthfulness of anonymous sources of perhaps crucial data. Any usable system needs to find a way to verify information to ensure its trustworthiness and that will allow people on the street, over time, to build trust in the message because they messenger.

3.Security of information is also an important factor. While most communications in a mobilization will have to be open, in order to allow for senders and receivers to participate, we obviously do not want to expose participants to more risk than they already run by simply being on the street, and expressing dissent. This means that certain messages or pieces of information may be inappropriate to share, and the systems needs a way to filter such messages. Additionally, the personal safety of those receiving and sharing information is a consideration both on the ground and in later persecution. In fact, this type of accurate information could be used by people fighting bogus charges by the authorities similar to how video has been used in recent cases. The information can also provide a more objective global view for those wishing to analyze the event after the fact and not wishing to rely solely on first person accounts. Finally, system itself must be secured from sabotage by outside forces that may wish to disrupt the flow of information or send misinformation to users. Verification and other procedures could seriously limit reactionary forces from undermining a communications system thus limiting there damage by using self-correcting mechanisms.

4.Cost is a self-evident principle. Most radical groups and individuals have limited resources especially when compared to the State's bloated budgets for communications. We need to find do-it-yourself (DIY) ways to level the playing field and allow the best communication system our limited monetary resources can provide. At first it might seem absurdly naive to believe that a DIY decentralized system could ever out perform the zillion dollar gizmos of the authorities, but the world has changed in recent years. It is no longer simply a matter of who has the best hardware but more who has the best system for delivering and filtering information. Open source collaborative communities have for decades shown that their shoestring (or no) budget programs are just as good , if not better, than those developed by big governments or multi-nationals. So it will not be easy and will require a lot of sweat but it is not out of the realm of possibility. Cost considerations are not just for those setting up the system but for end users. Most likely we will continue to use already ubiquitous technologies out there like radios

and cell-phones.

5.Accessibility is a key component to any system that hopes to be used by a diverse group, common at large demonstrations. Any communications system needs to be easy to use and have a very short learning curve because unlike in the anti-globalization days, today people spend very little time in preparatory skill-shares and workshops at large mobilizations. Now most people tend to arrive the day before a protest for better or worse so the system must be learned (or preferably be already self-evident) in a very short time or before the protest using web-sites, zines, etc. This has more to do with the users end but also could apply to the operator/developers end. During the Republican Convention in New York (2004) textmob (a version of sms sharing predating Twitter) was introduced but because it was unfamiliar and required some mastery of simple commands many people who had applicable cell-phones still did not use it. In fact less than eighty people used textmob during the week-long protests that drew tens of thousands. Indymedia on the other hand was so easy and replicated on many other internet sites that it was almost instantly used by thousands in the first week of its launch.

6.One overlooked component of an effective communications system is how it filters data not just for veracity (see point 2) but allow for effective pattern recognition. Textmob and live streaming of police scanners suffer from providing the user so much information that it can quickly become distracting noise. The difference between noise and useful information is usually a problem of filtering. A communications network, if it is receiving data from a large number of sources must find a reliable way to provide information in sizes that people can digest. Ideally the patterns revealed would allow users to have a more global picture of what is going on and be able to make decisions about their actions based on this understanding. Traditionally we use linguistic models (verbal or text) for transmitting information into communication but there may be other useful models for doing this. The visual recognition areas of the human brain are 13 times larger than the language centers and are some of the most developed aspects in the brain. By using pictures, symbols or similar visual representations it is possible to take large sets of data and turn them into usable patterns. By moving away from strictly language based systems a communications system can be used by a more diverse groups and in different geographic locations.

7.Virulence of both the system and the users is a necessary aspect of a sound communications network. The effort that goes into outreach/training is often underestimated. It is quite time-consuming and difficult to get people to adopt new ways of doing things especially if they are complicated or poorly understood. Viral growth allows peoples' natural networks to take on the bulk of this work and do it more effectively than any outreach working group could achieve on its own. The system used has to be easily implemented and shared by others. The best way of achieving this is by allowing a great deal of adaptability in the system. Indymedia started out as a way to report on the Seattle protests but was quickly adapted to other purposes including event announcements, sharing theoretical writings and even organizing protests. The actual implementation of the software was more complicated and relied on a small group of Johnny Appleseeds that went from city to city and country to country to set up Indymedia nodes. By 2001 the software and hardware had become stream-lined enough to allow anyone with some computer skills and access to moderate priced equipment to set up their own Indymedia site. Most of the communication systems used during protests are created on a disposable

model, meaning they are used just once. This one-time use interferes with the virulence of the system because it needs to be rebuilt and often relearned with each new event. Ideally a system would be developed that could be use and expanded upon by anyone and spread by existing social networks.

8.It should be clear from the previous principles that flexibility is a highly desirable characteristic of an effective communications system. By flexibility we mean a system that can easily function at various scales of both geography and size. A communications system should be able to tell us what is going on around the corner or across town while at the same time letting us connect with thousands or just our affinity group. The network should work equally well in Boston, Bogota and Beijing. It should allow the user to customize it so they can get and share the information they want at a particular time and place. This type of flexibility will dramatically improve the value of a communications system.

9.As anarchists we seek to create a communication system that is non-authoritarian. That means that the information is controlled by the users on both ends, and doesn't rely or allow some self- or otherwise selected "cadre" to use information in order to manipulate or direct participants without their active agreement. A horizontal, non-authoritarian system is also much more powerful and protected from oppression, arrests, or sabotage. We also believe that non-authoritarian systems require more participation and thus draw on the strength of many making it a more powerful tool that reflects our politics.

10.Seeking to create a sustainable system, we are looking to a model that will not become obsolete by next year or next month for that matter, a model that is flexible enough to grow and evolve as new needs, ideas, and technologies arise. Another aspect of sustainability is the need to develop a model that can easily be replicated and doesn't depend on a small group of highly specialized people for its functioning. Food Not Bombs is a good example of a sustainable model, while a small group of people can make an effective FNB anywhere in the world, the actual participants can easily change while the project continues to exist.

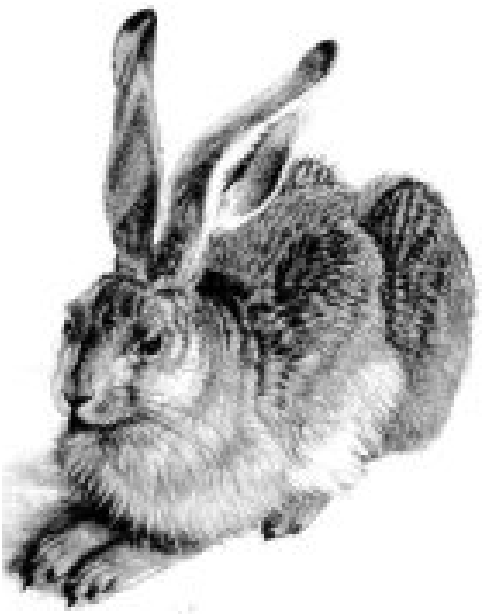
There are of course other attributes that go into making an affective communications network but these ten principles create a foundation for thinking about and developing any such network. We feel that an effective and radical communications network for mobilizations and protests can provide an important tool in the overall radical project.

A system that maximizes the ten principles can create a new model for our resistance on the streets. Our hope is that such a communications system would allow a real-time emergence of collective action, shared knowledge and intelligence that could counteract the State's ability to contain resistance and oppress us. The tired old chant of "the people united can never be defeated" might become a reality if tens of thousands of people have the ability to draw upon not only the "wisdom of the crowd" but also its passion. The courage, skills, intelligence, desire and commitment of the participants in our mobilizations is not in doubt; the goal is to create an information-sharing system that encourages all of these diverse people to act in concert without relying on some centralized decision-making body and soul crushing discipline. Flash mobs, internet organizing, political prisoner support web pages, etc.

have all suggested that technologies can be harnessed to multiply our strength. Imagine if we could create a communications network that encouraged all the passions on the streets to emerge naturally into a tidal wave of real and radical change. If we could build a system that unites us while keeping our individual autonomy of action intact then we would truly be unbeatable.

March Hare Communications Collective, Inc. (MHCC) is a volunteer mutual benefit corporation that is dedicated to promoting emerging communications technology for the use of public organizing of grass-roots groups and non-governmental organizations. The focus of the March Hare Communications Collective, Inc. is to develop new, secure and open software to be used with existing technologies that will aid community and grass-roots coordination, social networking and organization specifically using mobile technologies. In addition March Hare Communications Collective, Inc. seeks to provide educational materials and trainings on how to use mobile technologies in a safe and effective manner that meets the needs of the user groups. March Hare Communications Collective, Inc. seeks to be a repository of both technologies and information regarding the innovative use of mobile technologies to promote social justice in the US and internationally by grass-root/community groups.

As of March 2009 MHCC is still pulling its self up from the bootstraps. Some of the initial research the collective will be doing is looking into contributing to an extending the Ushaidi project [1], and repurposing the Tapatio project. To keep up to date with progress of the group and it's projects visit http://march-hare.org.



References:

[1] The Ushahidi Engine is a platform that allows anyone to gather distributed data via SMS, email or web and visualize it on a map or timeline. Their goal is to create the simplest way of aggregating information from the public for use in crisis response. This is very similar to the goals of the Tapatio project but managed to get a larger development team off the ground and was able to make due with out using twitter on the backend by leveraging Font Line SMS (http://www.frontlinesms.com/), and hardwired cell phones. http://www.ushahidi.com/

[2] Tapatio is intended to be a communications resource for the radical anti-authoritarian community. They have developed a system that can be used in mass direct action scenarios to gather tactical information, categorize that information based on type and urgency, rate the information for reliability, and then dispatch reliable information to individuals in the streets based on the criteria they request (for example, maybe the user only wants information about legal updates, or maybe they want to hear about police mobilizations and medical information). http://comms.hackbloc.org

comcastwatch

- FCC rules Comcast guilty of throttling P2P traffic in Class Action Lawsuit victory

---

December 25th 2009: Comcast has settled to pay up to $16 million dollars to eligible class members not exceeding $16.00 each. You can apply online at or read the text of the agreement at http://www.p2pcongestionsettlement.com. Comcast has since filed a legal appeal.

Comcast is using Sandvine, commercially available traffic shaping services - controversial because it designed to violate Net Neutrality principles.

The FCC is demanding that Comcast "ensure compliance with a proscribed plan to bring Comcast's discriminatory conduct to an end" and within 30 days of release of the Order Comcast must "disclose the details of its discriminatory network management practices to the Commission, submit a compliance plan describing how it intends to stop these discriminatory management practices by the end of the year, and disclose to customers and the Commission the network management practices that will replace current practices"

An open source project called Glasnost was put together to gather data on various ISPs to demonstrate BitTorrent traffic shaping patterns and have published their results at http://broadband.mpi-sws.org/transparency/results/. Amongst their findings was that Comcast (also Cox and StarHub) was blocking bit torrent upstream traffic.

- Comcast, General Electric and NBC

December 3rd, 2009: Comcast has purchased a controlling majority of NBC Universal (NBCU) further positioning itself as a media monopoly. Comcast will take a controlling 51% stake in the joint venture, and GE will control 49%.

According to the Wall Street Journal, the $30 billion merger "represents the first significant merger review for the Obama administration, and regulators are expected to undertake an exhaustive review." As of January 6th the Department of Justice antitrust division and the Federal Communications Commission are currently reviewing the merger.

Digital rights and free speech advocates who claim that the merger would consolidate too much media power into the hands of the nation's biggest cable company and ISP.

"How the FCC might stop the Comcast-NBC merger"
http://arstechnica.com/tech-policy/news/2009/12/how-the-fcc-might-stop-the-comcastnbc-merger.ars

"Justice Dept. will join FCC in review of Comcast-NBC Universal deal"
http://latimesblogs.latimes.com/entertainmentnewsbuzz/2010/01/dept-of-justice-will-probe-comcastnbc-universal-deal.html

If you work at Comcast consider joining or starting a Union: http://www.comcastworkers.com http://www.comcastworkersunited.com http://comcastworkersfightback.blogspot.com

- Ryan Harris busted by FBI for selling hacked cable modems

Ryan Harris("DerEngel") was indicted by the grand jury on August 16th 2009 for conspiracy, wire fraud and computer fraud but was not arrested until late October. Harris founded TCNISO which according to the indictment "develop, distribute and sell cable modem hacking software and hardware products." In November 2008, FBI agents purchased via TCNISO's website pre-hacked cable modems and the book "Hacking the Cable Modem" written by Harris.

The indictment also involved three additional unindicted co-conspirators: a software developer for TCNISO who lived in Kentucky, the vice president of TCNISO who lived in California, and "DShocker" who lived in Massachusetts(According to Wired, DShocker was previously busted for DDos and Swatting attacks and received an 11 month sentence).

The dangerous precedent being set with this case is that the FBI is not alleging that Harris personally used hacked cable modem to illegally steal internet access, but that TCNISO sold technology that possibly could be used by others to do so.

"Feds Charge Cable Modem Modder With ˜Aiding Computer Intrusion"
http://www.wired.com/threatlevel/2009/11/derengel/

Ryan Harris indictment
http://www.scribd.com/doc/22076368/Ryan-Harris-DerEngel-Indictment

Thomas Swingler was busted for nearly the same thing in January 2009 for running the website cablehack.net (http://www.wired.com/images_blogs/threatlevel/files/swingler_complaint.pdf).

- Three Charged for Hacking Comcast.net DNS Account

November 19, 2009: Three were charged in federal court for the May 28th, 2008 hijacking of Comcast.net's DNS account at NetworkSolutions.com, temporarily sending Comcast visitors to their own page which read "KRYOGENIKS Defiant and EBB RoXed COMCAST sHouTz to VIRUS Warlock elul21 coll1er seven."

Christopher Allen Lewis (EBK), James Robert Black, Jr. (Defiant), and Michael Paul Nebel (Slacker) are being charged with conspiracy to commit computer fraud Title 18 Section 1030. The indictment explains that they had gained access to Comcast's account through a series of phone calls and social engineering. Comcast claims that the website was down for more than five hours allegedly costing the company over $128,000 in damages

Some reports have speculated that the hackers were retaliating for Comcast's recent sabotage of BitTorrent traffic; Defiant and EBK say that's false: they just hate Com

cast in general. “I’m sure they hate us too,” says Defiant. “Comcast is just a huge corporation, and we wanted to take them out, and we did,” he says.

“I was trying to say we shouldn’t do this the whole damn time,” said Defiant last year. “But once we were in,” added EBK, “it was, like, fuck it.”

“Feds Charge 3 With Comcast.net Hijacking”
http://www.wired.com/threatlevel/2009/11/comcast-hack/

FIGHTING THE FASCISTS USING DIRECT ACTION HACKTIVISM

by tHoughTCRiimE

The past few months have manifested a number of internet attacks on white supremacist organizations ranging from destroying websites to releasing internal communications. Let’s analyze what happened to further discuss what tactics are appropriate and effective in our movements.

The most recent incident in December involved the release of mysql database dumps for ten neo-nazi websites and forums including private messages, emails, password hashes, everything. For anti-racist activists and researchers, there is a bottomless goldmine of information available in these databases.

You may find information such as pictures, phone numbers and home addresses for affiliated white supremacists in your area who would probably very upset if you make and distribute posters in their neighborhood. You may also find that some are involved with more mainstream conservative organizations such as the Republican Party or the Tea Party Patriots who would also be very upset having their Nazi affiliations exposed. You may also find out when and where white power groups are organizing meetings, and pass that along to anti-racist groups who could shut the event down and/or get the jump on em.

(Example: A quick look at the database dump for volksfrontinternational.com reveals that Andrew Yeoman of the Bay Area National “Anarchists” attended the Althing white power gathering in Missouri - and that his phone number is 415.309.7863. Give him a ring!)

Our only criticism is that the scope of these recent attacks seems rather narrow in only attacking white supremacists when there are other perfectly suitable targets such as anti-immigrant vigilante groups like the Minutemen(see swarm.mahost.org), Third Position nationalists, or groups like the Tea Party.

Furthermore there are other tools that can be utilized and some of the best are not surprisingly developed by the government. From the 60s to today, counter-intelligence programs attempt to identify and exploit weaknesses and divisions in progressive movements by infiltrating organizations and/or making false accusations about movement leaders. We could be using similar tactics to dismantle white supremacist movements by creating fake profiles on nazi forums to gather information or set up nazis to fight

against each other.

Free Speech for Who?

While these attacks are very disruptive and embarassing to fascists, some white hat "hackers", right wingers and even some rich liberal types are often quick to criticize such actions in that they violate "free speech". (Nevermind the fact that everywhere the Nazis go the police are there to protect them while cracking down on the leftists). The oppressors already have their stage; the mainstream media bombards us with racism and sexism every day, creating space for more blatent neo-nazi groups who if they are not exposed and confronted with militant action they will continue to grow and thrive. The tactics used by Anti-Racist Action have proven to be effective in driving out white supremacist and other racist organizations and individuals. The ARA Network has this to say about free speech:

"We think that hate speech, turning people into scapegoats and targets for hateful action, is an abuse of free speech and that people's lives are more important than the right of someone to publicly encourage others to target certain groups for a campaign of murder, rape, assault, genocide, ethnic cleansing and terror. A cross burning, for example, is not free speech or the free exercise of religion -- it is an act of racist terror and intimidation."
(http://www.antiracistaction.org)

The purpose of these actions is not to defend the free speech rights of racist scum - it is to disrupt and dismantle white supremacist organizations. The idea of direct action itself is not about appealing to politicians or police to solve our problems or to attempt to win any sort of ideological battle - it's about taking matters into our own hands and wrecking what wrecks us. By breaking into their computer systems, exposing their correspondence, and shutting down their communication systems we hope to make it more difficult to spread their hate, recruit new members, or organize on the internet at all.

Direct Action Hacktivism

Bashing the Fash on the internet is one campaign that we can draw some lessons from and apply it to other struggles. Let's suppose the goal of direct action hacktivism is to cause the target organization enough stress and damage that they can no longer perform their services, individual members will quit and/or turn against each other, and even collapse entirely. What kinds of tactics are most effective, and why? Here are some points to measure how effective an action is:

* Creating a financial burden for the target - making it costly in terms of money and labor to return services to normal (such as having to buy a new server, or having to put hundreds of hours in to rebuild)

* Causing loss of irreplacable data - the trashing of site content, databases, and backup files making it difficult if not impossible to ever restore services (such as deleting site content, customer records, research files, backups, etc)

* Bringing attention to the atrocities and injustices committed by the target - articulating your message clearly so as not to be dismissed as petty vandals or criminals, and ensuring that those reading about the action understand it and dig it

* Exposing harmful or embarassing information - uncovering internal documents that if released would turn the general public against the target and possibly be incriminating (such as posting personal email correspondence, internal policies or research, personal information such as phone # and addresses on individual members)

Following these points should help

ensure an action is significantly damaging to an organization and will hopefully cause it to collapse entirely. But it can all be for nothing if:

* The cost/benefit ratio isn't worth it - that it might bring legal heat down on you or other allied organizations, or (warning, some liberal bullshit right here) there is public backlash against your choice of tactics because it "makes you look as bad as them".

* The action is not in synchronicity with already existing campaigns and movements with well defined goals and demands. Hacktivism is not ever a substitute for on-the-ground community activism.

Recent Timeline of Internet Actions Targetting Fascist Organizations

Late 2008
Anti-fascist hackers calling themselves "Daten-Antifa" (data-antifa) broke into the nazi forum Blood & Honour and released complete database dumps of tens of thousands of members including names, emails, passwords, private messages and other internal information. The information was uploaded to a variety of torrent websites and was described by the hackers as a "laboriously prepared cloak-and-dagger operation".
http://de.indymedia.org/2008/08/225641.shtml

August 2009
Private emails belonging to a chapter of the National Socialist Movement(NSM) were released to WikiLeaks. The contents of these emails include personal correspondence, information on other accounts the user had access to, and the contents of the NSM's internal discussion email list.
http://wikileaks.org/wiki/US_National_Socialist_Movement_private_emails_,until_15_Aug_2009

November 2009
The websites of holocaust denier and Nazi sympathizer David Irving were defaced by "Anti-Fascist Hackers" who released private email correspondence, secret locations of his speaking tour, and detailed information on people attending his events which included members from various white supremacist organizations. This information was also posted to WikiLeaks.
http://www.wired.com/threatlevel/2009/11/david-irving/

December 2009
In possibly the best score yet, mysql database dumps of ten white supremacist and neo-nazi websites were released to WikiLeaks. The information is 54MB compressed and contains usernames, email addresses, password hashes, and private messages belonging to the following websites: volksfrontinternational.com(Volksfront International), hammerskins.net(Hammerskins Nation), aryanfront.com(Aryan Front), newp.org(North East White Pride), whiterevolution.com(White Revolution), finalstandrecords.com(Final Stand Records), enationalism.com(eNationalist), ecwu.org(East Coast White Unity), bloodandhonour.com(Blood & Honour, updated version!), and creativitymovement.net(Creativity Movement, formerly World Church of the Creator).

The filename is ten-neo-nazi-sites-plus-2009.tgz and is available on various torrent websites. Much work is needed by hackers to parse this information, crack giant password hash lists, and publish the information in human readable formats!

While trying to answer the question, "What is the future of the Tapatio Project?", I ended up getting in touch with a number of different people who have worked on anti-authoritarian communications teams as well as a few who are actively developing the next generation comms tools. Nathan Frietas is working on the the Guardian project, an attempt to bring useful tools for political activists to mobile devices. The target platform is android and while there are a number of ambitios goals, progress is being made and more and more people from the community are taking note and getting involved. The general idea of the project is to create a suite of tools, each providing
a discreet feature that collectivly meet the requirements of a communications team with scouts, medics and their dispatchers, reporters and their publishers, all of whom may be deployed to a hostile environment.

The public description of the Guardian Project along with a plug for the android platform on the project site
(http://openideals.com/guardian/) is:

While mobile phones have been heralded as a powerful new tool for political activists, human rights advocates and public health initiatives around the globe, they are a step backwards when it comes to personal liberty, anonymity and safety. Google Android's open-source mobile telephony platform provides a foundation on which a new type of phone that cloaks its user and their data, both on the device itself and as it communicates around the world.

Nathan was kind enough to meet up with me and give me the low down on getting
involved with the project and agreed to talk a bit about the Guardian project
as part of an interview with HTZ.

evoltech: What tools / components of the Guardian project are currently ready for use?

Nathan: Orbot, the Tor port for Android, is where the initial bulk of our labor has been placed. Through this work, we've not only gotten Tor working, but have solved the basic problems of controlling the flow of all packets in and out of an Android device. Our goal with Orbot is that you can use it to blacklist or whitelist all network-enabled application, as well as select which ones you wish to route via Tor. In addition, Orbot can route all DNS queries through Tor, so that there is no leakage into the mobile network, at all, and you can be assured there is no targeted MITM attacks happening within the carrier network. With Orbot fully enabled on your device, every networked application is anonymized.

Beyond that, there a number of third-party open-source applications we have begun testing for inclusion on our distribution. One of this is SIPDroid, which is a SIP/VOIP client which can connect with an Asterisk server to provide IP-based voice communication over 3G or Wifi. We have tested SIPDroid over a VPN connection (PPTP or OpenVPN) and it works very well. With this configuration, if you have multiple users with Android phones and SIPDroid, you can have a secure voice communications network. This is the type of "telecommuter" configuration that corporations with Cisco-powered infrastructures have been running for ten years - we've just figured out how to do it with open-source and on Android phones.

Finally, Beem Project (XMPP chat with SSL), RemoteWipe (SMS-based remote device eraser), DroidTracker (SMS-based authorized GPS tracker) and DroidWall (iptables-based firewall) are some of the other applications we are working to optimize and integrate. Some version of this code is available either through the Android Market, or via their project pages and code repositories.

evoltech: Which of the Guardian tools is seeing active development right now?

Nathan: The big focus now is porting

GPG. K9Mail is the best open-source IMAP/POP client on Android, we'd love to provide integration with it to support all the features you need to sign and encrypt mail, as well as basic key management. The apps would end up looking very much like what you have on a desktop - Keychain Manager, GPGDropThing, and so on. We are using the same approach we did with Tor - native cross-compile of the GPG codebase, wrapped in Android Java code to provide the glue and user interface.

There are a few other side efforts going on around encrypted SMS and ZFone (Phil Zimmerman's end-to-end voice encryption), and I am trying to get those efforts linked in a bit better into Guardian.

We are also trying to get our first complete Android firmware MOD built, so that you can simply flash a rooted device, and have a complete secured distro. We are building our working up on the CyanogenMOD project, which has shown great success in providing an alternate firmware with enough ease-of-use that even mainstream users are switching to it.

evoltech: Can you describe were you see this project a year down the road?

Nathan: We have some pretty tangible goals:

- Availability of the core applications (Tor, GPG, in the Android Market and via direct download of the APK files in multiple languages/locales
- Availability of MOD firmware distribution with bundled apps with support for major devices on the market
- A small but vibrant developer community with the ability to respond to bugs and feature requests as they arise
- Direct sale (at cost) and conversion service of Guardian-enabled Android hardware
- An grant/donation-funded program "One Mobile Per Activist" to get devices into the hands of the groups that need them the most

evoltech: The communication team deploying tapatio 3 years ago at the RNC in Minneapolis had a difficult time teaching people how to use twitter from their phones. It was totally foreign to people. Less then a year later the service had become so ubiquitous that every one already knew how to use it. Right now to use some of the guardian project tools you have to have a hacked android phone which is probably out of reach for most activists. Can you speculate as to when the use of mobile applications like this will become accessible to activists? Do you think it is important for it to be accessible, or do you think that work should be focused on building tools that can installed, contributed to, and managed by a tech-capable crowd?

Nathan: When Orbot is available in the market (next week?!), you will see that it is very, very easy to use. Literally one-tap was our goal. We then want a number of applications (browsers, IM chat, photo upload, etc) to be marked as "Tor-enabled" or "Tor-certified" so that users can just install those and be on their way. The goal of Guardian is not so much new concepts or functionality, but trying to secure all of the existing activities that users do naturally on their mobile devices.

Ultimately, since the work on Guardian is open-source, I would hope that for specific events, mobilizations, campaigns or days of actions, a group could come together and build a custom app just for that effort. It might tie together different pieces of Guardian, while providing a very, simple set of functionality... a one-click picture + upload + GPS that is all done over a secure, anonymous channel, for instance.

I can also see specialized configurations of hardware and software deployed by the more serious teams. For instance, having Guardian phones preconfigured with voice networks, safe GPS tracking, remote wipe, etc. in the hands of a comms or media teams would allow them to do their job without compromising those around them.

evoltech: Can you describe some of the Guardian project tools that you imagine to be well suited for a comms team? How do you imagine these tools being used in a comms deployment?

One feature that is a bit controversial is GPS tracking. It is funny that this is one of the biggest paranoias of activists - that your position is being tracked, or that your phone could be controlled or activated remotely. However, this same capability could be very useful for a comms team. I have

been in many days of action where you spend half of your energy talking on radios trying to figure out exactly where everyone is located. The vision then, would be to allow an authorized, encrypted stream of your GPS to be sent our to just your team, while also giving you precise control to turn that on or off. I could also imagine this all flowing into a private Laconi.ca/Status.net server and having the GPS data map onto OpenStreetMaps... a complete, private, secure open-source social/location awareness stack.

In addition, the ability to erase a phone's call or messaging history remotely if you know a team member has been detained is also critical. I have heard a number of stories about activists being popped, then having their call log used to track down everyone they'd been in touch with. I also have direct experience with this happening with a group of media activists in China, where their texts and twitter messages to each other were used as evidence to hold them for a week.

The work on SIPDroid that I mentioned earlier would also provide a better way to call people (via names or x1234 style extension) as opposed to exposing their actual mobile phone number.

evoltech: On openideals.com/guardian/ you talk about being able to use this suite of tools on the windows mobile platform, is this currently possible?

Natahan: Not yet, but our work on porting Tor has already inspired similar efforts on the Nokia N900 and other Linux-based mobile platforms. Windows Mobile (and not Windows Phone 7) is such a completely different environment, that it will take a different set of skills that we currently have on board. The Crytophone product out of Germany is based on Windows Mobile 5/6 and we have begun discussing more collaboration with them. The problem is that with Windows Mobile, you really don't get to see inside of the OS, to truely understand what is happening beneath the application layer. Android, Maemo and now Symbian OS, all give you that insight and ability to patch at a very low-level.

In the end, we have to balance the practical value of Guardian-style features being available on every phone on the market, with our commitment to supporting true open-source platforms and tools.

evoltech Do you have any announcements or other things you want to say about the Guardian project in HTZ?

Nathan: First, I really appreciate your coverage of our work, and want to openly solicit feedback and criticism for your readers. We are of the transparency school when it comes to building great security software, fully realizing that while we are clear in our passion and ability, we would never claim to know everything or consider every possible vector of attack.

With that in mind, we are launching our new website (http://guardianproject.info) shortly, and that will include all the information you'll need to get in touch with us. We're building a knowledge base on general mobile security, and will be creating some webcasts, as well, documenting our work, and featuring some of the applications I mentioned earlier.

You can also join our mailing list there to keep abreast of developments. Our site and lists are hosted and managed on Mayfirst.org, a progressive, technology cooperative located in Brooklyn, NY. You can be assured that we will keep your information private.

LITTLE BROTHER
CORY DOCTOROW
A review

Warning: contains spoilers

The thesis of Little Brother is the feasibility of asymmetric digital resistance, a sort of "open-source insurgency". The novel portrays technology as a neutral medium, utilized by both the state and insurgents. While Little Brother is a story of a fight against the state, and is sympathetic to anarchism, it fails to reject the state and capitalism and ends on an explicitly statist note.

The novel opens with a "terrorist" attack on the Bay Bridge. In the immediate aftermath, the protagonist and his friends are arrested by agents of the Department of Homeland Security, black-bagged, and shipped off to the novel's Guantanamo stand-in, an island facility off the coast of San Francisco. The protagonist initially refuses to cooperate with interrogators, and they single him out for rough treatment, eventually breaking him and extracting passwords for his Pirate Party-provided email account and encrypted mobile storage. After he is released, the protagonist organizes a resistance movement based around the fictional anonymity network Xnet, and a psuedonym he builds up, 'M1k3y'. The insurgency is essentially online fight club - M1k3y posts blog entries detailing how to fight some surveillance technology, and his followers engage in actions based on the targets he singles out. Eventually this becomes a mass youth movement. Around this time, the protagonist decides to break his own anonymity and tell his story to a mainstream media reporter, abortively goes into hiding, begins ordering his insurgents to stand down, and gets captured by the DHS again. As he is being tortured, the cavalry arrives and rescues him, and the novel abruptly winds down with a call for reform, urging concerned citizens to dissent at the polls.

The insurgency of Little Brother uses anonymity networks based on wireless mesh networks to organize a decentralized fight against the state. Inexplicably, the novel includes few references to existing privacy-enhancing technologies - instead of using Pidgin[1] and OTR[2] for encrypted, authenticated instant-messaging, Doctorow invents "IMParanoid"; instead of using Freenet or GNUnet for anonymous, censorship-proof filesharing, the rebels use Xnet, a mesh-network powered by Microsoft XBoxes running a variant of GNU/Linux[3]. The novel does use OpenPGP as a central device, explains it comprehensively and in great detail, and spends the bulk of a chapter describing a key-generating and key-signing party. However, Doctorow abuses the notion of a web of trust, transforming it from a device used to verify the authenticity of a public-key into an expression of one person's trust in another. Since the novel is released under a Creative Commons license, these mistakes could be fixed, but since the license Doctorow chose prohibits commercial distribution, it's unlikely such a remix would ever exist in a printed form.

The structure of the insurgency is depressingly centralized. While actions are carried out by affinity groups with no formalized connections to any other groups, they take instruction from M1k3y. There seems to be no hub of revolution more important than M1k3y's blog, and ideas for new actions, news events, and everything else, is emailed to M1k3y and maybe blogged later. This is an artifact of the speculative fiction - if there

was no Supreme Leader, readers couldn't fantasize about being it.

Little Brother goes disappointingly halfway in its look at existing power structures. While it decries the surveillance state, it is not against states, and while it points out oppressive systems of race, gender, and age, it seems to mention these things only as an afterthought. The potent message of youth power expressed by the insurgency is undermined by the Deus Ex Machina intervention from adults at the close of the novel - indicating that revolution is a fun game, but just a game, and one that needs cleaning up. The novel fails to mention capitalism in any sort of negative light, although it does favorably mention anarchists, and to lesser extent, anarchism.

While possessed of an enjoyable story and some valuable technical information, as well as an interesting model for computer network-centric insurgency, Little Brother fails to stick to reality where it matters, and fails to question the elephants in the room.

[1] http://pidgin.im/
[2] http://cypherpunks.ca/otr
[3] http://trygnulinux.com/

"Badger hates Society, and invitations, and dinner, and all that sort of thing."
- Kenneth Grahame, The Wind in the Willows, Ch. 3

Last issue we gave a general review of ruby, Ronin, Ronin overlays, and released a WordPress password brute forcing tool. Since then, Ronin has started to under go some changes, and the word press brute force tool has been revised. In this article we will go over some of the changes happening with Ronin and the smart brute forcer.

Ronin is growing up

As the Ronin project is maturing design decisions are being made to simplify, standardize, increase accessibility, and improve internal integration.

Some code is getting completely cut from the code base such as the SQL DSL (Domain Specific language) for generating SQL in Ronin::Code::SQL [1].

The website ronin.rubyforge.org is getting re-written to make use of Jekyll [2], "a simple, blog aware, static site generator" as opposed to the custom xml based site. This is being done because the tool is getting a lot of use by other developers, it is being actively supported, it supports blog post generation, and handles markdown syntax [3] (being used by github.com, we.riseup.net, and nearly every other web application written in ruby) to aid user contribution to documentation. It also integrates nicely with ruby's WEBrick [4] for live testing. Another standardization project outside of Ronin, but also from postmodern and related to exploit development, is ruby-yasm [5], a ruby interface to the YASM assembler [6]. This will make it easy to generate shellcode for multiple different architectures file

formats on the fly while developing payloads.

The obvious downside for strong integration with other projects is when project maintainers become unresponsive. The upside, aside from having someone else maintain the dependency, is that it strengthens other projects through mutual aid and creates tangible human relationships within the software development community. As anyone who has worked on a campaign that has existed for more then a short period of time will tell you, sustainability depends on a shared feeling of community and belonging.

Integration is not just happening with external libraries but with internal ones as well. There are a few places in the Ronin code base where there is duplicated effort. The prime example here is the ronin-php library which provides access to rfi and lfi vulnerability testing which really belongs in ronin-exploits. There is also planned integration of ronin-scanners, the library for integrating with external tools like nmap [7], nikto [8], into ronin-int [9], the Ronin intelligence tool.

The Ronin intelligence gathering library is an exciting addition from the perspective of software based campaigns. Security being the ever morphing nightmare that it is can leave computers vulnerable to attacks one day and secure the next. A campaign, especially when being contributed to by multiple developers, will need a way to collect and share information and notes on all relevant assets of the campaign's targets. Metasploit uses sqllite (not easily shareable) and can possibly make use of other DBMSs but would require a bit of custom hacking, and CANVAS is totally inaccessible do to licensing price and it being closed source. Ronin-int has been around for a while, but will really become the red team Intranet blog in the next couple of months when it gets integrated with ronin-scanners. Contributions to the ronin-int database can be added by humans (comments on hosts or services, references to relevant propaganda, or individuals and contact information related to the campaign's targets) or can be programmed (the output of an nmap or wikto scan possibly from multiple sources to pin point location based filters). At a recent talk with postmodern there was a good deal of discussion about how centralizing this type of data is a liability as a single point of failure if the central source is deleted, lost, or stolen. To address this issue ronin-int could make use AMQP [10] (a messaging protocol like XMPP (think Jabber / Google Talk) with PubSub built in allowing notification of events (intelligence in this case) to all subscribed parties) [11].

The Ronin exploit library, ronin-exploits, has also been around for a while now but will have had a major overhaul by the time this goes to print.

Another postmodern creation, code name badger, roninRat, and libBERT, will provide a rpc interface to computers it runs on. This project will allow a standardized way to connect and add commands to Ronin instances running on a server. Badger is installed (dropped) on a server, will use ffi for arbitrary system library / file inclusion, can connect back, or listen locally. This component will handle running commands, and accessing the local FS (essentially remote shell) using BERT as the serialization mechanism.

Misc update and fails

There was a bit of work done to show off some of the exploit generation

functionality of Ronin, but it did not get finished in time for this issue so your just going to have to wait till the next issue. There was however a feature added to spidr, a ruby web spidring library, that now allows for spidering of sites being served as vhosts but without public DNS records. If you remember from last issues article we wrote a "smart" word press password brute forcing tool leveraging Ronin and a library call wordlist. Wordlist uses spidr on the backend. Another side effect of this is that we can spidr a server using the IP address and domain name without leaking dns requests through the spidr library. Run this all through privoxy and tor and you have a properly anonymous password auditing tool [12]:

```
smartBruteForceWP.rb -v -s
204.12.0.50 -hh test.com -px localhost:8118
```

References:

[1] Ronin SQL API reference - http://ronin.rubyforge.org/docs/ronin-sql/

[2] Jekyll is a simple, blog aware, static site generator - http://jekyllrb.com/

[3] Markdown syntax is a meta language for a meta language (HTML), but it is a bit simpler then HTML - http://daringfireball.net/projects/markdown/syntax

[4] Gnome's Guide to WEBrick. The best WEBrick documentation in existence, albiet with a few to many "So, <computer_programmer_explanation>" phrases. http://microjet.ath.cx/webrickguide/html/html_webrick.html

[5] A Ruby interface to YASM - http://ruby-yasm.rubyforge.org/

[6] YASM - http://www.tortall.net/projects/yasm/

[7] NMAP is a feature rich port scanner - http://nmap.org/

[8] Nikto is a web server vulnerability scanner - http://cirt.net/nikto2

[9] ronin-int - http://github.com/postmodern/ronin-int

[10] AMQP is an open Internet Protocol for Business Messaging http://www.amqp.org

[11] If you have ever had to program lisp and that last sentence just gave you flashbacks, Im sorry.

[12] smartBruteForceWP.rb - https://hackbloc.org/svn/htz/8/smartBruteForceWP.rb

Upcoming Cons and Events

* The Next HOPE (16 July 2010, 18 July 2010) *

HOPE (Hackers On Planet Earth) is a conference series sponsored by the hacker magazine 2600: The Hacker Quarterly. There have been seven conferences to date: HOPE, Beyond HOPE, H2K, H2K2, The Fifth HOPE, HOPE Number Six, and The Last HOPE.

The Next HOPE is scheduled for July 16-18, 2010 at the Hotel Pennsylvania in New York City.

* DefCon 18 (29 July 2010, 1 August 2010) *

DEF CON is generally in the last week of July or first week of August in Las Vegas. DEF CON 17 will be held July 31 - August 2 at the Riviera Hotel & Casino in Las Vegas. Many people arrive a day early, and many stay a day later.

* Burning Man 2010 (30 August 2010, 6 September 2010) *

Once a year, tens of thousands of participants gather in Nevada's Black Rock Desert to create Black Rock City, dedicated to community, art, self-expression, and self-reliance. They depart one week later, having left no trace whatsoever. Learn more about this incredible experience through our First Timers' Guide, our mission statement and Ten Principles.

Tumult and change, churning cycles of invention and destruction - these forces generate the pulse of urban life. Great cities are organic, spontaneous, heterogeneous, and untidy hubs of social interaction. In 2010, we will inspect the daily course of city life and the future prospect of civilization.

THE BACK PAGE...

If we didn't get a chance to use your submission now, we will get it into the next issue. We are always looking for more content, and we thank everyone for helping with the zine, not just by submitting content, but by also giving of your time, we can use all the help that we can get! We couldn't do it without you!

Have you ever had a dream, that you were so sure was real? What if you were unable to wake from that dream? How would you know the difference between the dream world and the real world?

Hackbloc Staff:
alxCIAda
Doll
Evoltech
Flatline
Frenzy
Hexbomber
Impact
Kuroishi
Ringo
Sally
whooka

Zine Staff:
alxCIAda
Evoltech
Flatline
Frenzy
Hexbomber
Kuroishi
Ringo
Sally
whooka

Questions? Comments? Article Submissions? Get a hold of us at:
e-mail: staff [at] hackbloc [dot] org
our website: hackbloc.org/contact

--> GET COPIES OF THE ZINE! <--

Electronic copies of the zine are available for free online at the hackbloc website:
www.hackbloc.org/zine/

There are two versions of the zine: a full color graphical PDF version which is best for printing and also includes all sorts of extras, as well as a raw TXT version for a more readable and compatible format. Having the zine in your hands is still the best way to experience our zine. If you can't print your own(double sided 8.5x11) then you can order copies of this issue and all back issues online from Microcosm Publishing (microcosmpublishing.com) who are based out of Portland. If you live in The San Francisico Bay area, you can find us at the SF Anarchist Bookfair, March 13-14 2010. More info will be found on our site closer to the time of the event!

We are seeking translators to translate Hack This Zine into other languages, if you are interested send an email to staff [at] hackbloc [dot] org.

HACKTHISZINE